Monika Pfaffinger

Das Recht auf informationellen Systemschutz

Plädoyer für einen Paradigmenwechsel im Datenschutzrecht

Nomos

DIKE

https://doi.org/10.5771/9783748936046, am 11.09.2024, 22:39:47

Monika Pfaffinger

Das Recht auf informationellen Systemschutz

Plädoyer für einen Paradigmenwechsel im Datenschutzrecht

Nomos Verlagsgesellschaft

Monika Pfaffinger studierte Rechtswissenschaften an der Universität Zürich, wo sie 2007 auch promoviert wurde. Es folgten die Berufung zur Assistenzprofessorin für Privatrecht mit Schwerpunkt ZGB (non-tenured) an der Universität Luzern sowie die Bestellung als Vizepräsidentin der Eidgenössischen Koordinationskommission für Familienfragen in Bern. Parallel zur Etablierung einer Beratungspraxis sowie zur Tätigkeit als freischaffende Wissenschaftlerin engagierte sich Monika Pfaffinger ab 2019 als Universitätsrätin, später als Prorektorin an der Universität Liechtenstein. Seit 2019 lehrt sie an der Kalaidos Law School. Mit der vorliegenden Schrift wurde sie 2022 von der Universität Basel habilitiert, wobei ihr die Venia Legendi für Privatrecht, Informationsrecht sowie Recht und neue Technologien verliehen wurde.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

Zugl.: Basel, Univ., Habil., 2022

1. Auflage 2022

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

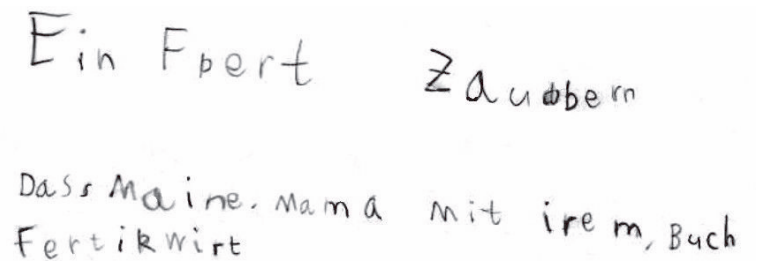
ISBN (Print): 978-3-7560-0025-8
ISBN (ePDF): 978-3-7489-3604-6

ISBN (Print): 978-3-03891-530-0 (Dike Verlag, Zürich/St. Gallen)

DOI: https://doi.org/10.5771/9783748936046

Das Buch wurde auf alterungsbeständigem Werkdruckpapier gedruckt und fadengeheftet.

Für Ella



(Ellas drei Wünsche im Dezember 2018)

Vorwort

Die vorliegende Studie wurde im Frühlingssemester 2022 von der Juristischen Fakultät der Universität Basel als Habilitationsschrift angenommen. In demselben Semester erfolgten das Habilitationskolloquium und die Verleihung der *Venia Legendi* für Privatrecht, Informationsrecht sowie Recht und neue Technologien durch die Regenz der Universität Basel.

Die Arbeiten zu dieser Schrift begannen vor mehr als zehn Jahren. Zu jener Zeit hatte das Datenschutzrecht in der Schweiz nicht die in Breite und Tiefe gebotene Aufmerksamkeit erfahren. Seither hat das Rechtsgebiet einen markanten Bedeutungswandel durchlaufen: Konfrontiert mit den technologischen und ökonomischen Realitäten ist eine Intensivierung und Professionalisierung in der Auseinandersetzung mit der Materie zu verzeichnen. Es wurden tiefgreifende Anpassungen des Datenschutzrechts erforderlich, die sich auf europäischer Ebene in Gestalt der DSGVO sowie in der Schweiz mit der Totalrevision des DSG manifestiert haben.

Da die Studie über den gesamten Zeitraum dieser in vielerlei Hinsicht revolutionären Entwicklungen hinweg entstand, werden in ihr alle relevanten Aspekte dieses grundlegenden Wandels erfasst, analysiert und bewertet. Die zentrale Erkenntnis der Untersuchung lautet, dass es – ungeachtet jeglicher Neuerungen – für das Datenschutzrecht der Zukunft dringend eines Paradigmenwechsels bedarf: weg vom inzwischen durch die Tatsachen überholten, aber in den Köpfen weiterhin bestehenden analogen Denken, in dem das Datenschutzrecht in den Kategorien von Subjekt und Objekt verhaftet bleibt, und hin zu einem kontextuellen Verständnis, demzufolge das Datenschutzrecht nicht länger nur auf das einzelne Subjekt bezogen werden kann, sondern als *Recht auf informationellen Systemschutz* gedacht werden muss. Denn Gegenstand des Datenschutzrechts sind seit jeher nicht isolierte Daten und Datensubjekte, sondern Datenflüsse in einer pluralistisch strukturierten Datentopografie: Neben dem Schutz des einzelnen Subjekts und dessen Daten besteht die zentrale Aufgabe des Datenschutzrechts vor allem darin, den *Transfer* von Daten zwischen verschiedenen gesellschaftlichen Bereichen zu regulieren, um deren Integrität zu garantieren. Nur ein Datenschutzrecht, das nicht exklusiv auf das Subjekt fokussiert, sondern systemrelativ konzipiert ist, kann seinem Schutzauftrag in unseren modernen und facettenreichen Gesellschaften gerecht werden.

Doch nicht nur bezogen auf den Forschungsgegenstand reifte die Untersuchung in einer Phase grosser Umbrüche heran. Auch persönlich betrachtet war die Zeit der Ausarbeitung dieses Werks von vielen Veränderungen geprägt, infolge derer ich mich in unterschiedlichen und gleichermassen faszinierenden wie herausfordernden Kontexten und Rollen wiederfand. Unter anderem hatte ich eine befristete Stelle als Assistenzprofessorin an der Universität Luzern inne und war

Vizepräsidentin der Eidgenössischen Koordinationskommission für Familienfragen. Mit der Geburt und Betreuung meiner Tochter eröffnete sich mir eine gänzlich neue Dimension, und auch beruflich gab es infolge eines Wechsels in die Privatwirtschaft sowie in die Selbständigkeit grosse Veränderungen. Nie verloren ging dabei jedoch meine Leidenschaft und mein kontinuierliches Engagement für die akademische Forschung und Lehre.

An die Menschen, die mich auf diesem Weg begleitet haben, möchte ich an dieser Stelle folgende Worte des Dankes richten: Mein besonderer Dank gebührt Prof. Dr. R. Fankhauser, der die Habilitationsschrift vom Anfang bis zum Schluss umsichtig betreut hat. Ebenso gilt mein Dank Prof. Dr. K. Pärli. Beide haben wertvolle Impulse gegeben und zeichnen gemeinsam für das Erstgutachten verantwortlich. Die externen Gutachten wurden dankenswerterweise von Prof. Dr. M. Gruber sowie Prof. Dr. F. Thouvenin verfasst. Für das sorgfältige Korrektorat und die engagierte Unterstützung im Zuge der Drucklegung danke ich Herrn Dr. T. Kronenberg, zudem den Verantwortlichen beim Nomos-Verlag für die effiziente sowie freundliche Zusammenarbeit.

Inniger Dank gilt meiner Schwester lic. phil. K. Ahr mit ihrer Familie, die mir stets unverrückbar, gleichwohl vielfältig zur Seite standen. Ebenso möchte ich RA Dr. N. Passadelis meinen Dank aussprechen, der die gemeinsame Verantwortung für unsere Tochter immer liebevoll sowie verlässlich übernommen hat, damit einen wichtigen Beitrag für meine persönliche wie akademische Entfaltung und entsprechend für die Entstehung dieser Arbeit geleistet hat. In meinen Dank schliesse ich zudem meine langjährigen Freundinnen und Freunde ein, die mich auf dem langen und anstrengenden Weg bis zur Fertigstellung dieser Schrift fortwährend ermutigt haben und mit denen ein sowohl emotional als auch intellektuell inspirierender Austausch möglich war: mein akademischer und persönlicher Freund Prof. Dr. V. Karavas, sodann Dr. P. Frey, Dr. K. Fischer, I. Reiss (CFA), R. Gresch, L. Roth, Diplom-Volkswirtin M. Kotz, Prof. assoc. M. Dougoud (MLaw) und viele weitere mehr. Vincent, der Mann an meiner Seite, stand mir ebenso an schwierigen Tagen mit seiner ausgeglichenen und sportlichen Art bei. Meinem Vater verdanke ich Disziplin und Beharrlichkeit – Eigenschaften, die für meinen Werdegang und die Vollendung dieser Analyse unverzichtbar waren. Zu guter Letzt adressiere ich meinen Dank auch an die Menschen, an deren Widerständen ich gewachsen bin.

Die Entwicklung dieser Schrift stand im Andenken an meine vor vielen Jahren jung verstorbene Mutter, selbst Juristin und Künstlerin.

Gewidmet ist dieses Buch meiner geliebten Tochter, deren vitale Lebensfreude mich mit Glück und Stolz erfüllt.

Zürich, im Dezember 2022 Monika Pfaffinger

Inhaltsverzeichnis

Abkürzungsverzeichnis

a	alt
a. A.	anderer Ansicht
a. a. O.	am angegebenen Ort
a. E.	am Ende
a. M.	anderer Meinung
AB	Amtliches Bulletin
Abs.	Absatz
AcP	Archiv für die civilistische Praxis
AfP	Zeitschrift für Medien- und Kommunikationsrecht
AJP/PJA	Aktuelle Juristische Praxis/Pratique Juridique Actuelle
Am. J. Comp. L.	American Journal of Comparative Law
ANAG	Bundesgesetz über die Ausländerinnen und Ausländer (Ausländergesetz, AuG) vom 16. Dezember 2005 (Stand am 1. Januar 2013), SR 142.20
Antitrust L.J.	Antitrust Law Journal
Anwaltsrevue	Das Praxismagazin des schweizerischen Anwaltsverbands
AöR	Archiv des öffentlichen Rechts
Art.	Artikel
AsylG	Asylgesetz vom 26. Juni 1998 (Stand am 1. September 2022), SR 142.31
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG) vom 6. Oktober 2000 (Stand am 1. Januar 2022), SR 830.1
Az.	Aktenzeichen
BankG	Bundesgesetz über die Banken und Sparkassen (Bankengesetz, BankG) vom 8. November 1934 (Stand am 1. Januar 2020), SR 952.0
BB	Betriebs-Berater
BBl	Bundesblatt
Bd.	Band
BDSG	Bundesdatenschutzgesetz
Berkeley Tech. L.J.	Berkeley Technology Law Journal

Berl J Soziol	Berliner Journal für Soziologie
BGE	Bundesgerichtsentscheid (Schweiz)
BGer	Bundesgericht
BGG	Bundesgesetz über das Bundesgericht (Bundesgerichtsgesetz, BGG) vom 17. Juni 2005 (Stand am 1. Juli 2022), SR 173.110
BGH	Bundesgerichtshof (Deutschland)
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsgesetz, BGÖ) vom 17. Dezember 2004 (Stand am 19. August 2014), SR 152.3
BJM	Basler Juristische Mitteilungen
BR	Bundesrat
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (Stand am 1. Januar 2021), SR 101
BVerfG	Bundesverfassungsgericht (Deutschland)
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (Deutschland)
BVGer	Bundesverwaltungsgericht (Schweiz)
Calif. L. Rev.	California Law Review
Case W. Res. L. Rev.	Case Western Reserve Law Review
CB	Compliance-Berater
CLSR	Computer Law and Security Review
CNIL	Commission Nationale de l'Informatique et des Libertés (Frankreich)
Colum. Sci. & Tech. L. Rev.	Columbia Science and Technology Law Review
Colum.-VLA J.L. & Arts	Columbia-VLA Journal of Law & the Arts
CR	Computer und Recht
CRM	Customer Relationship Management
d. h.	das heisst
DBG	Bundesgesetz über die direkte Bundessteuer (DBG) vom 14. Dezember 1990 (Stand am 1. Januar 2022), SR 642.11

Der Staat	Zeitschrift für Staatslehre und Verfassungsgeschichte, deutsches und europäisches öffentliches Recht
DGRI	Deutsche Gesellschaft für Recht und Informatik
digma	Zeitschrift für Datenrecht und Informationssicherheit
Diss.	Dissertation
DSG	Bundesgesetz über den Datenschutz, Eidgenössisches Datenschutzgesetz vom 19. Juni 1992 (Stand am 1. März 2019), SR 235.1
DSGVO	Datenschutz-Grundverordnung der EU, Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
DuD	Datenschutz und Datensicherheit
E	Erwägung
E-DSG	Entwurf eines totalrevidierten Datenschutzgesetzes
ed.	Edited/Editeur
EDB	Eidgenössischer Datenschutzbeauftragter
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDPD	European Data Protection Board
EGMR	Europäischer Gerichtshof für Menschenrechte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ELR	Entertainment Law Review
EMRK	Europäische Menschenrechtskonvention
ErwG	Erwägungsgrund
ESTV	Eidgenössische Steuerverwaltung
Ethics Inf. Technol.	Ethics and Information Technology
EU	Europäische Union
EuZA	Europäische Zeitschrift für Arbeitsrecht
ex/ante	Zeitschrift der juristischen Nachwuchsforschung
FamPra.ch	Die Praxis des Familienrechts
FAZ	Frankfurter Allgemeine Zeitung

FINMA	Eidgenössische Finanzmarktaufsicht
FMG	Fernmeldegesetz (FMG) vom 30. April 1997 (Stand am 1. Juli 2021), SR 784.10
Fn	Fussnote
Geo. L.J.	Georgetown Law Journal
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG) vom 8. Oktober 2004 (Stand am 1. Januar 2014), SR 810.12
h. L.	herrschende Lehre
Habil.	Habilitation/Habilitationsschrift
Harv. Envtl. L. Rev.	Harvard Environmental Law Review
Harv. J.L. & Pub. Pol'y	Harvard Journal of Law and Public Policy
Harv. J.L. & Tech.	Harvard Journal of Law & Technology
Harv. L. Rev.	Harvard Law Review
Hastings L.J.	Hastings Law Journal
HAVE	Haftung und Versicherung
HFG	Bundesgesetz über die Forschung am Menschen (Humanforschungsgesetz) vom 30. September 2011 (Stand am 1. Februar 2021), SR 810.30
HMD	Praxis der Wirtschaftsinformatik
HRRS	Online-Zeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht
i. c.	in casu
i. d. R.	in der Regel
i. e.	id est
i. e. S.	im engeren Sinne, im eigentlichen Sinne
i. K.	in Kraft
i. S.	im Sinne
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit

i. w. S.	im weiteren Sinne
IDG	Gesetz über die Information und den Datenschutz (IDG) vom 12. Februar 2007, Kanton Zürich 170.4
IJC	International Comparative Jurisprudence
insb.	insbesondere
Int. J. Commun.	International Journal of Communication
Int. J. Law Inf. Technol.	International Journal of Law and Information Technology
Int. Stud. Q.	International Studies Quarterly
InTeR	Zeitschrift zum Innovations- und Technikrecht
IPRG	Bundesgesetz über das Internationale Privatrecht
IRIE	International Review of Information Ethics
ITSL	Center for Information Technology, Society and Law
IV	Invaliditätsversicherung
IVG	Bundesgesetz über die Invalidenversicherung (IVG) vom 19. Juni 1959 (Stand am 1. Januar 2022), SR 831.20
J. Bus. Ethics	Journal of Business Ethics
J. Intell. Prop. L.	Journal of Intellectual Property Law
J. Priv. Confid.	Journal of Privacy and Confidentiality
JdT	Journal des Tribunaux
JZ	Juristenzeitung
K&R	Kommunikation & Recht
KG	Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (Kartellgesetz, KG) vom 6. Oktober 1995 (Stand am 1. Dezember 2014), SR 251
KritJ	Kritische Justiz
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
KVG	Bundesgesetz über die Krankenversicherung (KVG) vom 18. März 1994 (Stand am 1. Januar 2022), SR 832.10
LeGes	Mitteilungsblatt der Schweizerischen Gesellschaft für Gesetzgebung (SGG) und der Schweizerischen Evaluationsgesellschaft (SEVAL)

lit.	litera
m. E.	meines Erachtens
m. w. H.	mit weiteren Hinweisen
Md. L. Rev.	Maryland Law Review
medialex	Fachzeitschrift für Medien- und Kommunikationsrecht
MIT	Massachusetts Institute of Technology
Mittelweg 36	Zeitschrift des Hamburger Instituts für Sozialforschung
MMR	Multimedia und Recht
n	neu
N	Nummer/Note
N. Ill. U. L. Rev.	Northern Illinois University Law Review
nDSG	Neue Fassung des Bundesgesetzes über den Datenschutz, Eidgenössisches Datenschutzgesetz vom 25. September 2020, SR 235.1 (nach Totalrevision)
NJW	Neue Juristische Wochenzeitschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
NZZ	Neue Zürcher Zeitung
OBA	Online Behavior Advertisement
OGer	Obergericht
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (Stand am 1. Februar 2021), SR 220
Oxf. J. Leg. Stud.	Oxford Journal of Legal Studies
ÖZS	Österreichische Zeitschrift für Soziologie
PinG	Privacy in Germany
PUK	Parlamentarische Untersuchungskommission
recht	Zeitschrift für juristische Weiterbildung und Praxis
resp.	respektive
RR-CO	Recht relevant. für Compliance Officers
RR-VR	Recht relevant. für Verwaltungsräte
Rz	Randziffer

S.	Seite
S. Cal. L. Rev.	Southern California Law Review
SAEZ	Schweizerische Ärztezeitschrift
Santa Clara L. Rev.	Santa Clara Law Review
Sci. Eng. Ethics	Science and Engineering Ethics
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SJZ	Schweizerische Juristen-Zeitung
Soc. Res.	Social Research
sog.	sogenannt
SR	Systematische Rechtssammlung
SRIEL	Swiss Review of International and European Law (Schweizerische Zeitschrift für internationales und europäisches Recht)
Stan. L. Rev.	Stanford Law Review
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 1. Juni 2022), SR 311.0
successio	Zeitschrift für Erbrecht, Nachlassplanung und -abwicklung
SZG	Schweizerische Zeitschrift für Geschichte
SZS	Schweizerische Zeitschrift für Sozialversicherung und berufliche Vorsorge
SZW/RSDA	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht
TA-SWISS	Stiftung für Technologiefolgen-Abschätzung
u. a.	unter anderem
u. a. m.	und andere(s) mehr
U. Pa. L. Rev.	University of Pennsylvania Law Review
UC Davis L. Rev.	UC Davis Law Review
Urban Hist.	Urban History
URP	Umweltrecht in der Praxis
UVG	Bundesgesetz über die Unfallversicherung (UVG) vom 20. März 1981 (Stand am 1. Januar 2022), SR 832.20

UWG	Bundesgesetz gegen den unlauteren Wettbewerb (UWG) vom 19. Dezember 1986 (Stand am 1. Januar 2022), SR 241
Va. J.L. & Tech.	Virginia Journal of Law & Technology
VAG	Bundesgesetz betreffend die Aufsicht über Versicherungsunternehmen (Versicherungsaufsichtsgesetz, VAG) vom 17. Dezember 2004 (Stand am 1. Januar 2020), SR 961.01
Vand. L. Rev.	Vanderbilt Law Review
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (Stand am 16. Oktober 2012), SR 235.11
VE-DSG	Vorentwurf eines totalrevidierten Datenschutzgesetzes
VGG	Bundesgesetz über das Bundesverwaltungsgericht (Verwaltungsgerichtsgesetz) vom 17. Juni 2005 (Stand am 1. Januar 2019), SR 173.32
VwVG	Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG) vom 20. Dezember 1968 (Stand am 1. Januar 2021), SR 172.021
WestEnd	Neue Zeitschrift für Sozialforschung
Wis. L. Rev.	Wisconsin Law Review
wrp	Wettbewerb in Recht und Praxis
WSJ	The Wall Street Journal
WuR	Wirtschaftsverwaltungs- und Umweltrecht, Zeitschrift für Praxis und Wissenschaft
Yale L.J.	Yale Law Journal
z. B.	zum Beispiel
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZD	Zeitschrift für Datenschutz
ZEuP	Zeitschrift für Europäisches Privatrecht
ZfM	Zeitschrift für Medienwissenschaft
ZfPW	Zeitschrift für die gesamte Privatrechtswissenschaft
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (Stand am 1. Januar 2021), SR 210

ZHR	Zeitschrift für das gesamte Handels- und Wirtschaftsrecht
Ziff.	Ziffer
ZIK	Zentrum für Information und Kommunikation
zit.	zitiert
ZNR	Zeitschrift für neuere Rechtsgeschichte
ZPO	Schweizerische Zivilprozessordnung (Zivilprozessordnung, ZPO) vom 19. Dezember 2008 (Stand am 1. Juli 2022), SR 272
ZRP	Zeitschrift für Rechtspolitik
zsis	Zentrum für Schweizerisches und Internationales Steuerrecht
ZSR/RDS	Zeitschrift für Schweizerisches Recht/Revue de droit suisse
ZUM	Zeitschrift für Urheber- und Medienrecht

Einleitung

«Wieder versuchen. Wieder scheitern. Besser scheitern.»[1]

Eine wissenschaftliche Auseinandersetzung mit dem Schutz des Privaten – Schirmbegriff für datenschutzrechtliche Anliegen – gleicht einem Blick in ein Kaleidoskop, dem Gang durch ein Labyrinth. Das Private, paradoxerweise mit dem bestimmten Artikel versehen, ist nicht nur in der juristischen Disziplin über Jahrzehnte, ja Jahrhunderte, auffallend unbestimmt, nahezu diffus geblieben. 1

Das Schweizer Datenschutzgesetz besagt in Art. 1 DSG (vor wie nach Totalrevision) schlicht und einfach, fast elegant: «Dieses Gesetz verbürgt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.» Dieser einleitende Zweckartikel lässt nichts von den heterogenen wie tiefgreifenden Herausforderungen erahnen, denen das Datenschutzrecht seit jeher ausgesetzt ist. Das DSG steht, sowohl was die Erfassung seines Schutzzweckes als auch was die Fixierung von Regelungsmechanismen sowie -instrumenten angeht, bis auf den heutigen Tag auf dem Prüfstand. Insofern ist ebenso relevant, dass die faktische Einhaltung des geltenden Rechts in der Realität defizitär bleibt. Gewiss, die Totalrevision des DSG, die im Zuge der Neuerungen gemäss DSGVO verabschiedet wurde, liefert bedeutsame und effektive neue Ansatzpunkte. Gleichwohl greift es zu kurz, in dieser jüngsten Revisionswelle einen datenschutzrechtlichen Schlusspunkt zu sehen oder sich auf eine rein dogmatische Durchdringung der neuen Regelungen *de lege lata* zu beschränken. 2

Diese Studie leistet einen Beitrag dazu, das Datenschutzrecht – ungeachtet markanter Veränderungen, die das Rechtsgebiet neuerdings erfährt – in die fernere Zukunft zu führen. Wie bereits der Titel verrät, geht sie von der Erkenntnis aus: Der Weg zu einem wirksamen Datenschutzrecht der Zukunft führt über die Anerkennung, wonach der Datenschutz – über die Person und ihre individuellen Rechte hinaus – *diversifizierte Schutzdimensionen* zu erfüllen hat. 3

Entwickelt wird ein *neues datenschutzrechtliches Paradigma*. Seine Herleitung setzt das Hinterfragen einiger Kernannahmen des aktuellen Datenschutzrechts voraus. Ein *Recht auf informationellen Systemschutz* überwindet sowohl die Dualismen von öffentlich versus privat, Subjekt versus Objekt, online versus offline als auch den monistischen Ansatz. Beide Konzepte finden sich in den zeitgenössischen Datenschutzerlassen Kontinentaleuropas. Der in dieser Untersuchung vorgeschlagene Perspektivenwechsel möchte das Datenschutzrecht, das bis heute im Recht der analogen Welt verhaftet ist, auf den Weg hin zu einem wirksamen Datenschutzrecht der digitalen Welt führen – zu einem Datenschutzrecht 4

1 Samuel Beckett.

de lege ferenda, das in den technologisch netzwerkartigen sowie gesellschaftlich diversifizierten Systemen funktionstüchtig wird.

5 Unbestritten: Dem Datenschutzrecht obliegt der Schutz des Menschen, der Person resp. Persönlichkeit. Allerdings: Hierin erschöpft sich seine Garantenstellung nicht. Vielmehr hat das Datenschutzrecht – so die hier vertretene These – in elementarer Weise dem *Schutz der Robustheit sowie Integrität* von strukturierten und strukturierenden *gesellschaftlichen Kontexten zu dienen.*

6 Beim *Recht auf informationellen Systemschutz* handelt es sich nicht um ein weiteres subjektives Recht, sondern um einen konzeptionell neuen Lösungsansatz. Er zielt darauf ab, angemessene Regelungen in Gestalt von Transmissionsprinzipien für Personendatenflüsse innerhalb und zwischen pluralen gesellschaftlichen Bereichen zu definieren. Wie Personendatenflüsse datenschutzrechtlich adäquat gestaltet werden und welche Instrumente dafür gewählt werden, das soll künftig stets von einer sorgfältigen Analyse der Frage abhängen, ob und inwiefern die Logiken sowie die Integrität der jeweils betroffenen gesellschaftlichen Bereiche tangiert, respektiert oder erodiert werden. Entsprechend zeigt diese Studie auf, inwiefern dem Datenschutzrecht und seiner faktischen Einhaltung ungeachtet jeglicher technischer Fortschritte eine grundlegende gesellschaftliche Bedeutung zukommt. Sie skizziert, wie die facettenreichen Bedeutungsdimensionen des Datenschutzes künftig angemessen adressiert werden können. Inspiriert ist diese Schrift von den Beiträgen Vieler, namentlich indes von den Studien der US-amerikanischen Philosophin Helen Nissenbaum.

7 Die Analyse in diesem Beitrag zur daten- und informationsrechtlichen Grundlagenforschung ist *methodologisch einem kontextuellen Ansatz verpflichtet*. Ziel ist es, eine *Gesamtlandschaft* abzubilden. Deshalb spannt sie zunächst chronologisch einen weiten Bogen von der ferneren Vergangenheit über die Verabschiedung der ersten Datenschutzgesetze hin zur Beschreibung der jüngsten legislativen Entwicklungen. Die sog. Grenzenlosigkeit der Personendatenströme und Verarbeitungshandlungen fordert eine Betrachtung, die über das nationale Recht hinausgeht. Die datenschutzrechtlichen Erlasse werden in den Fassungen der Rechtstexte vor und nach den jüngst erfolgten legislativen Neuerungen dogmatisch durchdrungen, wobei eine Charakterisierung anhand von Strukturmerkmalen und Entwicklungstrends die Funktionsmechanismen freilegt. Untersucht werden darüber hinaus Bedeutungszuweisungen, wie sie dem Datenschutzrecht vonseiten der Privatunternehmen sowie der öffentlichen Verwaltung, aber auch von den Verwaltungsbehörden sowie Gerichten als Durchsetzungsbehörden beigemessen werden. Unverzichtbar ist eine Auseinandersetzung mit empirischen Evaluationen von Datenschutzregulierungen sowie mit den medialen und politischen Debatten. Granular dargestellt werden die Realitäten, mit denen sich das Datenschutzrecht konfrontiert sieht und innerhalb derer es funktionstüchtig

seine Schutzaufträge zu verfolgen hat. Topoi wie der rasante technische Fortschritt oder die Kommerzialisierung von Personendaten sind zu unpräzis, um Leitkriterien für die Gestaltung eines wirksamen Datenschutzrechts der Zukunft gewinnen zu können. Die Integration von ausserrechtlichen Diskursen sowie der vonseiten der Wissenschaften, insb. den Rechtswissenschaften, präsentierten Analysen und Lösungsansätze generiert weitere richtungsweisende Erkenntnisse. All dies mündet in einen Vorschlag zur Rekonzeptionalisierung des Datenschutzrechts der Zukunft.

Anlass zu dieser Studie gab eine beklagenswerte Situation: In der Schweiz wurde 8
dem Datenschutzrecht selbst nach der Verabschiedung des eidgenössischen Datenschutzgesetzes im Jahre 1988 mit seinem Inkrafttreten 1992 über lange Jahre nur wenig Beachtung geschenkt. Die Unternehmens- und Behördenpraxis hielt das Datenschutzgesetz nur ungenügend ein und auch das Schrifttum interessierte sich kaum für das Thema. Ursächlich für das jahrzehntelang *brach liegende Feld* des Datenschutzrechts wurden benannt: wirtschaftliche Interessen, der rasante technische Fortschritt, die schwachen Durchsetzungsinstrumente des DSG, aber auch das fehlende Verantwortungsbewusstsein der Datensubjekte.

Von einem *Vollzugsdefizit* wurde, bis zum Anbrechen der jüngsten datenschutz- 9
rechtlichen Neuerungswellen, keineswegs bloss in der Schweiz gesprochen. Die faktisch marginale Relevanz des Datenschutzrechts kontrastierte allerdings seit jeher scharf mit dem öffentlichen Diskurs, der die Bedeutung des Datenschutzrechts in oft dramatischen Worten zum Ausdruck brachte. Eindringlich wurden und werden Datenschutzverletzungen und -skandale laufend angeprangert. Illustrativ der jüngste Facebook-Skandal, wo auf der sozialen Plattform geteilte Personendaten von Cambridge Analytica ausgewertet und mutmasslich zur Manipulation im US-Wahlkampf nutzbar gemacht worden seien. Der Aufschrei war wohl deshalb so laut, weil mit den Verarbeitungshandlungen nicht nur das einzelne Subjekt, sondern darüber hinaus das demokratische System beschädigt wurde.

Das allgemeine Unbehagen bezüglich der Praktiken und Techniken von Perso- 10
nendatenverarbeitungen im Zeitalter der Digitalisierung – jeglicher Affinitäten und Vorteile, die diese mit sich bringen, zum Trotz – darf als starkes Indiz verstanden werden, wonach dem Datenschutz und dem Datenschutzrecht eine *fundamentale Bedeutung* zukommen. Es erstaunt nicht, wenn mit dem Inkrafttreten der DSGVO sowie mit der Totalrevision des Schweizer DSG Bewegung in die datenschutzrechtliche Brache kommt. Beide Gesetze spülen das Datenschutzrecht weg von den Rändern in das Zentrum der Aufmerksamkeit. In der Folge erfährt das formelle und materielle Datenschutzrecht auch in der Schweiz eine intensivierte Bearbeitung. Die jüngste Neuerungswelle führt den Datenschutz in eine neue Ära, wobei das bisherige Datenschutzrecht mit seinen stabilisierten

Leitprinzipien signifikant erweitert wird. Der Fokus der legislativen Neuerungen liegt unter anderem auf der Stärkung der Betroffenenrechte, der erhöhten Transparenz, der Einführung von effektuierenden Umsetzungsinstrumenten, aber auch einer gestärkten Behördenhand. Prozedurale und organisatorische Elemente gewinnen an Gewicht. Die Schweiz fügt dem DSG in seiner Totalrevision seinem lange Zeit isoliert defensiven, retrospektiven und individualrechtlichen Konzept zusätzliche Ingredienzen bei: Neu gilt Datenschutz als *Compliance-Aufgabe*, für deren Einhaltung personendatenverarbeitende Stellen proaktiv und unter Integration risikobasierter Erwägungen zuständig sowie verantwortlich sind.

11 Gleichwohl: Im Zuge dieser Revisionswellen wurden *keineswegs sämtliche datenschutzrechtlichen Basisannahmen kritisch hinterfragt*. Ihnen und namentlich der zentralen Frage, welchen Zweck das Datenschutzrecht zu gewährleisten hat, widmet sich diese Studie. Die Arbeit geht von der Hypothese aus, wonach die mangelnde Effektivität des bisherigen Datenschutzrechts auf mehrere Faktoren zurückzuführen ist: zu enge kognitive Grundannahmen und Sichtweisen, überholte Normierungsansätze resp. Regelungsstrukturen, die ungenügende Adressierung der faktischen Rahmenbedingungen wie der Potenzen der Informationstechnologien sowie der gesellschaftlichen Strukturen, expansive ökonomische Begehrlichkeiten, zudem eine undifferenzierte Fixierung des Schutzzwecks sowie die erkennbare Fehleinschätzung betreffend das Konzept der informationellen Selbstbestimmung.

12 Den facettenreichen und tiefgreifenden Bedeutungsgehalt des Datenschutzrechts leitet diese Schrift – in gut juristischer Manier – anhand einer Analyse von diversen Rechtstexten her. Mehrere juristische Dokumente wie der bahnbrechende Aufsatz von Warren/Brandeis aus dem 19. Jahrhundert, aber auch das berühmte Volkszählungsurteil des Bundesverfassungsgerichts aus dem 20. Jahrhundert haben keineswegs bloss Rechtsgeschichte geschrieben. Vielmehr lassen sich in diesen Rechtstexten Indizien zur Weiterentwicklung des Datenschutzrechts post 2022, *de lege ferenda*, freilegen. 1993 hatte das Bundesverfassungsgericht im Volkszählungsurteil von Verfassung wegen unmissverständlich die Bedeutung des Datenschutzes und seiner Einhaltung zum Ausdruck gebracht, indem es ein Recht auf informationelle Selbstbestimmung statuierte und konkrete Vorgaben für die rechtmässige Personendatenverarbeitung formulierte. In besagtem Urteil ist ein *Recht auf informationellen Systemschutz* angelegt. Auch Warren/Brandeis, welche für die Anerkennung des Right to Privacy als subjektives Recht plädierten, beklagten bei Lichte betrachtet zugleich die schädliche Wirkung informationeller Praktiken auf die *Kontextintegrität*.

13 Der Vorschlag einer paradigmatischen Erweiterung ist folglich *kein Deus ex machina*. Vielmehr ist das *Recht auf informationellen Systemschutz* in diversen, teilweise sehr alten informationellen Praktiken und Anekdoten, aber auch in den

Gesetzestexten mit ihren Materialien und Entstehungshintergründen, Regelungsinstrumenten und -strategien angelegt.

Dem präsentierten *Recht auf informationellen Systemschutz* liegt eine Betrachtungsweise zugrunde, wonach Personendatenflüsse in netzwerkartigen Strukturen, eingebettet in die darunterliegende facettenreiche gesellschaftliche Landschaft, zu adressieren sind. Geboten ist eine Evaluierung der jeweils betroffenen Kontexte mit ihren Rationalitäten, um alsdann die passenden Informationsnormen resp. Transmissionsprinzipien aus dem Katalog der mannigfaltigen Gestaltungsinstrumente zu ermitteln. Weder Geheimhaltung im Sinne der Informationsblockade noch die Einwilligung als illusorisches Instrument der Selbstbestimmung noch die absolute Freiheit von Informationsflüssen sind pauschal vorzugswürdig. Vielmehr sind informationelle Transmissionsprinzipien differenziert im Lichte auch der systemischen Schutzdimension festzulegen. Damit nimmt das Datenschutzrecht seine Garantenstellung sowohl für den Schutz des Individuums als auch zum Schutz der Funktionstüchtigkeit gesellschaftlicher Kontexte wahr. 14

Die Studie ist anhand von **drei Teilen mit jeweils drei Kapiteln** wie folgt strukturiert: 15

Der **erste Teil** erscheint für eine datenschutzrechtliche Arbeit *prima vista* anachronistisch. Hier werden in der *Vergangenheit Schlüssel zur Gestaltung der Zukunft* aufgesucht. Nicht zu erwarten ist an dieser Stelle eine abschliessende rechtshistorische Untersuchung. Vielmehr lädt der erste Teil anhand einer Beschäftigung aus Distanz mit etwas ferneren Texten zu neuen Perspektiven ein. Er soll an den Gang der Untersuchung im zweiten und dritten Teil heranführen. Das Vorgehen gleicht demjenigen einer Wünschelrutengängerin, die Problemlagen und Sichtweisen informationeller Praktiken und Situationen in der ferneren Vergangenheit detektiert. Der Teil will somit eine Sensibilisierung für alte und neue Kategorien liefern und diese für die weiteren Schritte nutzbar machen. Denn die Zukunft des Datenschutzrechts liegt in der Vergangenheit angelegt. 16

Im *I. Kapitel* findet eine Auseinandersetzung mit den sagenumwobenen Geheimworten, wie sie in Märchen vorkommen, aber auch mit den traditionsreichen Geheimhaltungspflichten statt. Gezeigt wird, wie es stets um das Abschotten resp. Blockieren von Informationsflüssen zwischen heterogenen Bereichen geht. Die Geheimhaltungspflichten werden als die ältesten datenschutzrechtlichen Instrumente beschrieben. Eingeführt werden die Begriffe der *dynamischen* sowie der *akzessorischen Dimension informationeller Situationen*. Sie werden sich wie ein roter Faden durch diese Schrift ziehen. 17

Das *II. Kapitel* befasst sich in einer historischen Betrachtung mit verschiedenen Informationspraktiken und der *Etablierung informationeller Ordnungen*, nicht zuletzt, wie sie für das Mittelalter beschrieben sind und die ebenso als *Herr-* 18

schaftspraktiken figurieren. Gezeigt wird, dass Personendatenerfassungen schon damals Widerstand auslösten und dass Informationen seit jeher in bares Geld umgesetzt wurden.

19 Das *III. Kapitel* wendet sich der Herausbildung der *Dichotomie von öffentlich versus privat* zu. Für den Schutz des Privaten kommt dem *Liberalismus* sowie der Anerkennung der Freiheitsrechte zentrale Bedeutung zu. Genauer ausgeleuchtet wird sodann die zweite Kammer dieses Dualismus, das *Private im Privaten*. Hier werden die Bedeutung der bürgerlichen Gesellschaft und mit ihr diejenige der Kleinfamilie als intuitiver Kategorie des Privaten sowie die Entwicklung einer *statischen Konzeption* des Privaten mit seiner Symbolisierung durch das Haus sichtbar.

20 Der **zweite Teil** leistet einen Beitrag zur dogmatischen Durchdringung des Datenschutzrechts *de lege lata* unter Integration der Anpassungen nach Totalrevision. Hierbei werden die wichtigsten Entwicklungslinien und -trends präsentiert und die drei Strukturmerkmale herausgearbeitet, die das DSG prägen und seine strukturelle Funktionsweise bestimmen: der *Dualismus*, das *generalklauselartige Regelungsregime*, insb. in Gestalt der allgemeinen Verarbeitungsgrundsätze, sowie die *persönlichkeitsrechtliche Anknüpfung für den privaten Bereich*. Wie gezeigt wird, hält die Totalrevision an diesen drei Strukturmerkmalen fest, bettet sie allerdings neu ein und ergänzt sie um weitere Facetten. Abermals lassen sich den bereits in Kraft stehenden Regelungen produktive Impulse für die rechtliche Weiterentwicklung entnehmen.

21 Im *IV. Kapitel* wird der *Dualismus als erstes Strukturmerkmal* des DSG mit einem divergierenden Schutzniveau für den öffentlichen Bereich des Bundes gegenüber dem privaten Bereich beschrieben. Der entgegengesetzte Ausgangspunkt für die beiden Bereiche ist ein Charakteristikum des DSG. Das Kapitel fördert unter anderem zu Tage, dass die Frage nach der bereichsspezifischen Differenzierung resp. Vereinheitlichung eine Kernfrage des Datenschutzrechts ist.

22 Das *V. Kapitel* widmet sich den *generalklauselartigen Verarbeitungsgrundsätzen als zweitem Strukturmerkmal*. Auch diese belässt die Totalrevision weitgehend unberührt. Vertieft analysiert werden die materiellrechtlichen Datenschutzgrundprinzipien mit ihren Regelungsinhalten. Parallel dazu wird dieses gemeinsame Fundament des DSG für den öffentlichen und privaten Bereich daraufhin untersucht, inwiefern in ihnen die Saat zur Weiterentwicklung des Datenschutzrechts der Zukunft liegt. Auch in den einzelnen Verarbeitungsgrundsätzen zeigt sich die Einschlägigkeit bereichsspezifischer datenschutzrechtlicher Ausdifferenzierung. Über die Analyse der traditionsreichen Datenschutzinstrumente der generalklauselartigen Verarbeitungsgrundsätze werden Impulse für das Datenschutzrecht *de lege ferenda* generiert.

Das *VI. Kapitel* verengt den Fokus auf den privatrechtlichen Bereich des DSG, indem es *die persönlichkeitsrechtliche Anknüpfung als drittes Strukturmerkmal* beschreibt. Präzis dargelegt wird die Regelungsmechanik des DSG für den privaten Bereich, die konsequent an Art. 28 ZGB angelehnt ist. Beleuchtet werden die Verarbeitungshandlungen, welche die Demarkationslinie zur Persönlichkeitsverletzung (nicht) überschreiten, sowie das Rechtfertigungsregime. Anhand eines Blicks auf Einwilligungserfordernisse im Zusammenhang mit dem Umgang mit Personendaten ausserhalb des DSG, dem Recht am eigenen Bild sowie Einwilligungskonstruktionen in Bezug auf Personendaten im biomedizinrechtlichen Kontext werden die ausdifferenzierten Autonomiebereiche resp. abgestuften Schutzpositionen in Bezug auf den Willen des Datensubjekts im Umgang mit Personendaten sichtbar. Das Konzept des DSG wird für den privaten Bereich als eines der *Missbrauchsverhinderung* und *nicht der informationellen Selbstbestimmung* taxiert. Deutlich wird die *subjektiv-, abwehr- und deliktsrechtliche Struktur des DSG für den privaten Bereich*. 23

Der **dritte Teil** befasst sich mit Fragen der *Funktionstüchtigkeit resp. Wirksamkeit des Datenschutzrechts de lege lata*, aber auch *de lege ferenda*. Es geht um eine Reflexion der Bedeutungszuweisungen, die dem Datenschutzrecht verliehen werden. Gefragt wird nach evaluierenden Bewertungen und Effektuierungen, wie sie in der Unternehmenspraxis, von Datensubjekten, der Lehre und Rechtsprechung geleistet werden. Kritisch für das Datenschutzrecht und seine Wirksamkeit ist das *Vollzugsdefizit* mit seinen Erklärungsmustern. Sodann sind zwei bedeutsame Herausforderungen für das Datenschutzrecht zu betrachten: die *Potenzen neuer Informationsverarbeitungstechnologien* sowie die *expansive Tendenz ökonomischer Rationalitäten*. Sie stellen den Datenschutz auf die Probe. Es folgt eine Beschreibung der *legislativen Reaktionen* auf besagte Herausforderungen, wobei diese anhand von Entwicklungstrends präsentiert werden. Im Anschluss werden die vonseiten der Lehre diskutierten *informations- und datenschutzrechtlichen Lösungsansätze* reflektiert. Aus den bis an diese Stelle generierten Erkenntnissen wird im Ergebnis ein *eigener Lösungsansatz* abgeleitet. 24

Das *VII. Kapitel* wendet sich unter dem Titel «Datenschutz auf dem Prüfstand» dem sog. *Vollzugsdefizit* zu. Dargestellt werden die gegenüber dem Datenschutzrecht vorgenommenen Bedeutungszuweisungen. Neben empirischen Evaluationen kommt namentlich die *Effektuierung* durch die Lehre und Praxis zur Sprache. Nach einer Darstellung des Datenschutzrechts in der medialen und politischen Debatte folgt eine granulare Beschreibung der *faktischen Herausforderungen*, in denen das Datenschutzrecht erfolgreich operationalisiert werden soll. Umrissen werden zum einen die *technologischen Entwicklungen anhand der Beschreibung von drei Kernkapazitäten*. Es folgt zum anderen eine Auseinandersetzung mit der sog. *Kommerzialisierung von Personendaten*, der Persönlichkeit. 25

Diese Entwicklung wird unter dem Titel der *expansiven Kraft ökonomischer Rationalitäten* beschrieben, wobei anhand einer Stufenfolge verschiedene Informationspraktiken beleuchtet werden, namentlich auch im Internet.

26 Im *VIII. Kapitel* folgt eine Diskussion der aktuellen Lösungsansätze. Den Auftakt bildet eine Darstellung der jüngsten *legislativen Neuerungen* anhand der Beschreibung von acht Trends. Sie integrieren neue Funktionsmechanismen in das Datenschutzrecht, womit die im zweiten Teil beschriebenen drei Strukturmerkmale ergänzt oder neu eingebettet werden. Nach der Kompilation der legislativen Entwicklungslinien folgt eine Auseinandersetzung mit den *aktuell vonseiten der Wissenschaft präsentierten*, aber auch in der Praxis zu findenden *Vorschlägen* zur Beantwortung der datenschutzrechtlichen Herausforderungen. Eine Analyse der verschiedenen Ansätze auf Stärken und Schwächen vor dem Hintergrund der faktischen Herausforderungen des Datenschutzrechts sowie des Bewusstseins für neue, gleichwohl seit jeher angelegte Perspektiven bereitet den Boden, um im letzten Kapitel einen paradigmatischen Lösungsansatz für die Weiterentwicklung des Datenschutzrechts der Zukunft zu skizzieren.

27 Das *IX. Kapitel* nimmt zur Verifizierung und Erhärtung der bis zu diesem Punkt erarbeiteten These und der neuen Perspektiven einen Gerichtsentscheid zum Ausgangspunkt. «Der Fall» EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, war ein im Nachgang zu einem Verkehrsunfall in aller Härte geführter Versicherungsstreit über den Invaliditätsgrad einer Frau. Der Entscheid, in dem es im Kern um die Rechtmässigkeit der geheimen Observation durch einen Privatdetektiv ging, mündete in eine Verurteilung der Schweiz durch den Europäischen Gerichtshof für Menschenrechte. Anhand des konkreten Sachverhalts wird die kollektive Dimension dieses Rechtskonfliktes herausgearbeitet. Die Analyse des Falles unter Berücksichtigung sämtlicher bis zu diesem Punkt generierten Erkenntnisse *verifiziert den Ansatz eines Rechts auf informationellen Systemschutz*. Es wird gezeigt, dass eine geheime Observation und damit ein spezifisch gestalteter Personendatenfluss nicht nur individualrechtlich für das betroffene Datensubjekt relevant ist. Vielmehr durchkreuzt eine solche Praxis ebenso die Integrität des Gesundheits- und Sozialversicherungsbereichs. Sie untergräbt die ebenda geltenden Ziele, Logiken und Rationalitäten. Daran ändert auch eine gesetzliche Grundlage nichts, welche die Praxis «legitimieren» will. Das letzte Kapitel wird abgerundet mit einer Konkretisierung des Systemschutzparadigmas anhand von Eckpunkten und Leitkriterien. Zusammenfassende Schlussfolgerungen markieren das Ende der Schrift in der Hoffnung, dass diese zu weiterführenden Arbeiten anregen möge.

28 Im **Ergebnis** plädiert das vorliegende Werk für die Anerkennung eines neuen Paradigmas für die Gestaltung des Datenschutzrechts der Zukunft: ein *Recht auf informationellen Systemschutz*. Mit ihm wird das Datenschutzrecht zum Garan-

ten auch für die Robustheit gesellschaftlicher Bereiche. Es leistet einen Beitrag zum Schutz der Demokratie, des privaten und freiheitlichen Lebens, der Gesundheit, der Wissenschaft und Forschung, des Sozialstaats, des Arbeitskontextes usf.

Das *Recht auf informationellen Systemschutz* inkludiert den informationellen 29
Subjektschutz. Ein Datenschutzrecht der Zukunft – ein wirksames Datenschutzrecht und ein Datenschutzrecht, das seine weit über den Schutz des Individuums hinausgehenden Schutzaufträge wahrnimmt – kann nur ein *systemadäquates Recht* sein.

Erster Teil: Vergangene Zukunft

«In vertrauten Welten dominiert die Vergangenheit über Gegenwart und Zukunft.»[2]

Von den rechtlichen Entwicklungen in der EU mit angestossen, unterzog auch 30
die Schweiz ihr Datenschutzgesetz (DSG) einer Totalrevision.[3] Die Schlussfassung dieser Totalrevision lag Ende 2020 und damit zum Zeitpunkt des Abschlusses dieser Studie vor. In Anbetracht dieser grossen datenschutzrechtlichen Neuerungswellen mag es überraschen, diese Schrift zum Datenschutzrecht mit einem historischen Teil zu beginnen. Der Blick in die weiter zurückliegende Vergangenheit allerdings ermöglicht es, etablierte Konzepte sowie Sichtweisen, denen das Datenschutzrecht bis heute verpflichtet und verhaftet ist, freizulegen und um weitere, zukunftsträchtige Perspektiven anzureichern.

Die aktuelle datenschutzrechtliche Debatte zeigt sich gerade in der Schweiz weit- 31
gehend geschichts- und vergangenheitsvergessen. Das Mantra der modernen Informationstechnologien und des rasanten technischen Fortschrittes scheint jeden Blick auf die Vergangenheit überflüssig zu machen. Allerdings: Woher kommt der pastorale Tonfall[4] in der Medien- und Datenschutzdebatte des 21. Jahrhunderts, wie er beispielsweise in einem Wort zum Sonntag vom 21. März 2015 erklingt, das unter dem Titel «Der gläserne Bürger – von Daten und Macht»[5] ausgestrahlt wurde?[6] Nach dem Hinweis auf den Fichenskandal verortet der Pfarrer das Grundanliegen des Datenschutzes darin, dass das Individuum die Kontrolle über seine Daten behalte, weil vertrauliches Wissen Menschen verletzlich mache und anderen Macht verleihe. Daher wolle man selbst entscheiden, wer was erfahren soll. Allwissend sei bislang nur Gott gewesen – und heute das Netz –, wobei Gott auch Güte habe, so die Worte des Pfarrers. Groebner hört in solchen heute verkündeten und allgegenwärtig vernommenen bedrohlichen Fantasien über die absolute Erfassung und Überwachung des Menschen Echos von literarischen und religiösen Topoi. Sie sind erheblich älter als Bildschirme, Fichen, Karteikarten.[7] Das «Neue» bleibt, wie zu zeigen sein wird, stark im Tradierten verhaftet. Ebendies wird auch eine vertiefte Analyse des eidgenössischen Datenschutzgesetzes, das die grosse Zweiteilung von «privat» und «öffentlich» überwinden wollte und doch wesentlich von dieser Dichotomie geprägt bleibt, zeigen.[8]

2 Luhmann, Vertrauen, 23.
3 Zu dieser Botschaft DSG 2017–1084, 17.059, 6941 ff., 6970.
4 Dazu auch Groebner, Zeitschrift des Hamburger Instituts für Sozialforschung 2013, 29 ff.
5 Kuse, SRF online, Wort zum Sonntag, Der gläserne Bürger – von Daten und Macht, Zürich 2015, <https://www.srf.ch/play/tv/wort-zum-sonntag/video/der-glaeserne-buerger---von-daten-und-macht?urn=urn:srf:video:6c903f8c-bd28-43d0-913f-dbae701e3f2a> (zuletzt besucht am 30. April 2021).
6 Skeptisch zu kulturkritischen Essays über den «entblössten Menschen» Bull, Computer, 36 f.
7 Groebner, 175.
8 Hierzu vertiefend insb. zweiter Teil, IV.–VI. Kapitel.

32 Es sind die Erosion des Privaten, wenn nicht sogar ihr Untergang, die dieser Tage beklagt werden.[9] Das Private figuriert bis heute als Dachbegriff datenschutzrechtlicher Anliegen. Es tritt über mehrere Epochen hinweg als wiederkehrendes, allerdings wandelbares Konzept in Erscheinung. Mit dem Begriff resp. der Kategorie haben sich herausragende Intellektuelle quer durch die Disziplinen befasst. Die unzähligen hierbei herausgearbeiteten konstituierenden Elemente zu systematisieren, welche eine Orientierung in dem Dickicht um das Private geben (wollen), würde Stoff für eine eigenständige Monografie liefern.

33 Auch wenn das Private bis heute der datenschutzrechtlichen Debatte als Anknüpfungspunkt dient, bleibt es ein wenig verlässliches Bezugsmerkmal. Die Bemühungen, die pluralen und divergierenden Facetten der Begriffsfassung zu vereinheitlichen, und der Versuch, den Schutz des Privaten im Recht griffig und trennscharf zu gewähren, waren bislang nur beschränkt erfolgreich. Das eigene Schutzobjekt jedoch nicht hinreichend präzis erfassen zu können, mag gerade für das Recht als eigentliche Bankrotterklärung erscheinen.[10] Ist die Tatsache, dass eine einheitliche Definition des Privaten bis heute auch juristisch nicht gefunden werden konnte, schlicht Ausdruck davon, dass sich das Private von Zeit zu Zeit und von Kultur zu Kultur immerfort wandelt?[11]

34 Die nachfolgenden Ausführungen nähern sich aus einer *historischen Perspektive* verschiedenen Aspekten an, die für die Privatheits- und Datenschutzdebatte und namentlich für deren Ursprünge informativ sind. Es geht dabei *nicht* darum, die vielen, weit in die Vergangenheit reichenden, losen Fäden, die sich rund um informationelle Zugriffe wickeln, zu entwirren. Entsprechend sind keine erschöpfenden Erläuterungen zu erwarten. Vielmehr sollen anhand von geschichtswissenschaftlichen Arbeiten mit Gegenwartsbezug, die einen Eindruck von der historischen Dimension der Personenerfassung sowie den Auswirkungen der Technikentwicklung geben, sowie anhand von Märchen *zentrale und prägende Aspekte und Problematisierungen von Personendatenerfassung* in den Blick ge-

9 Vgl. Nissenbaum, 2; Dies., Dædalus 2011, 32 ff., 32; Eckhardt/Fattebert/Keel/Meyer, 5, schien es so, als ob die Bedeutung der Privatsphäre für viele Menschen abnehme; Bergelson, UC Davis L. Rev. 2003, 379 ff., 382; zum gefühlten Verlust der Privatheit m. w. H. Dörflinger, 83 ff.; allerdings wies bereits Fried, Yale L.J. 1968, 475 ff., 475 auf die Sorgen hin, welche der Privacy-Schutz bereite; Simitis beschreibt die Besorgnis, was die Notwendigkeit des Schutzes der Privatsphäre anbelangt, schon in den 1970er Jahren; vgl. Simitis, in: Schlemmer (Hrsg.), 67 ff., 67; Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 217 f.; Rudin, in: Sutter-Somm/Hafner/Schmid/Seelmann (Hrsg.), 415 ff., 425 ff.; Güntner, 82 ff.; zur Gefährdung der Privatsphäre durch die neuen Technologien Miller, 29 ff.; zur Erosion des Privaten insb. im Internet mit ihrem Einfluss auf eine Verschärfung der Preisdiskriminierung Odlyzko, 355 ff.

10 Zu den Herausforderungen und Problemen insofern die Ausführungen im dritten Teil dieser Schrift.

11 Vgl. Schiedermair, 23; Amelung, 9 ff.; vgl. weiter Hotter, 71 ff.; spezifisch in Bezug auf die grund- und arbeitsrechtlichen Bezüge Pärli, EuZA 2015, 48 ff., 48.

nommen werden.[12] Die auf diesem Weg herausgearbeiteten Betrachtungsweisen werden gleichzeitig fruchtbar für die aktuelle Debatte gemacht.

Den Anfang machen die traditionsreichen *Geheimworte und Geheimhaltungspflichten*, woraufhin auf historisch weit zurückverfolgbare, systematische Personenerfassung zu sprechen zu kommen ist. Insofern wird der Aufbau informationeller Infrastrukturen als Herrschaftstechnik beschrieben, womit gleichzeitig die systembildende Wirkungskraft von Prozessen der Personendatenverarbeitung sichtbar wird. Von zentraler Bedeutung ist dabei die Herausbildung eines Zweikammersystems – des Öffentlichen und des Privaten. Es folgt eine vertiefte Beschäftigung mit dem *Privaten im Privaten*. An dieser Stelle verengt sich der Fokus zumindest teilweise auf die Entwicklung der subjektiven Rechte. Den Abschluss dieses ersten Teils bildet ein Blick auf die Entwicklungsphase der ersten Datenschutzgesetzgebungen. Die grobgeschnitzte, oft anekdotenhafte Erzählung von Geschichten der Personendatenverarbeitung wollen Richtungshinweise für den weiteren Fortschritt dieser Studie geben: Mit der Rückblende werden Anregungen vermittelt, die datenschutzrechtliche Perzeption und Konzeption zu erweitern. Diese zugegebenermassen bruchstückhaften Ausführungen sollen auf die vertiefenden Ausführungen einstimmen. In der Vergangenheit lassen sich Episoden, Regeln, Praktiken sowie Einschätzungen freilegen, welche richtungsweisend für die Weiterentwicklung eines Datenschutzrechts der Zukunft, eines wirkungsstarken Datenschutzrechts sind. Die Schlaglichter beleuchten die Stellen, die es vertieft unter die Lupe zu nehmen gilt. Anders gewendet: Dieser erste, eingehende Teil ist als Hinführung gedacht an den zweiten und dritten Teil, die einen Perspektiven- und im Ergebnis einen Paradigmenwechsel herleiten. In diesem ersten, durchaus ausführlichen, nicht aber erschöpfenden Teil erfolgt eine Einladung, informations- und datenschutzrechtliche Konzepte in einem anderen Licht zu lesen. An dieser Stelle zeichnet sich ab, wohin der Weg im zweiten und namentlich dritten Teil gehen wird. 35

12 Aufschlussreich hierzu sind insb. die Beiträge von Dommann, allem voran ihre Habilitationsschrift Autoren und Apparate. Die Geschichte des Copyrights im Medienwandel, Frankfurt a. M. 2014; Krajewski, Der Diener. Mediengeschichte einer Figur zwischen König und Klient, Frankfurt a. M. 2010; Groebner, Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters, München 2004; Tantner, Die ersten Suchmaschinen. Adressbüros, Fragämter, Intelligenz-Comptoirs, Berlin 2015; Vec, Die Spur des Täters. Methoden der Identifikation in der Kriminalistik (1879–1933), Baden-Baden 2002; Bernard, Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur, Frankfurt a. M. 2017; sodann die Beiträge in Brandstetter/Hübel/Tantner (Hrsg.), Vor Google. Eine Mediengeschichte der Suchmaschine im analogen Zeitalter, Wien 2012; hingewiesen sei an dieser Stelle weiter auf die Schriften der Rechtshistorikerin und Medientheoretikerin Vismann, z. B. die posthum ausgewählten Schriften, Das Recht und seine Mittel, Frankfurt a. M. 2012.

I. Kapitel: Schlüssel zum Perspektivenwechsel

A. Geheimworte und Geheimhaltungspflichten

36 Geheimworte und Geheimhaltungspflichten sind sagenumwoben, abenteuerlich und sehr alt. Sie verraten eine Menge über den Umgang mit (persönlichen) Informationen im Ablauf der Menschheitsgeschichte. Schweige- resp. Geheimhaltungspflichten, welche einen Informationsempfänger zum Geheimnisträger machen, sind auch unserer Tage für zahlreiche Berufsgattungen positivrechtlich verankert:[13] Das Arztgeheimnis wird ergänzt durch Schweigepflichten für viele im medizinischen Sektor tätige Personen wie Hebammen, Psychologen, Apothekerinnen und deren Hilfspersonen, vgl. Art. 321 Abs. 1 StGB, und bewehrt deren Verletzung mit strafrechtlichen Sanktionen. In diesem Zusammenhang ist auch Art. 321bis StGB zu lesen, der die Verletzung des Geheimnisses für Forschende nach dem Humanforschungsgesetz unter Strafe stellt. Weitere Berufsgeheimnisträger sind Geistliche, Notare und Anwältinnen, vgl. dazu Art. 321 StGB.[14] Das Berufsgeheimnis der Advokaten hat das spezifische Interesse durch die eigene Gilde erfahren.[15] Sodann stehen gemäss Fernmeldegesetz Personen unter dem sog. Post- und Fernmeldegeheimnis, dessen Verletzung nach Art. 321ter strafbewehrt ist.[16] Und für die Schweiz nicht unerwähnt bleiben dürfen sodann Verschwiegenheitspflichten für kreditgebende Institutionen in Gestalt des sog. Bankgeheimnisses, genauer Bankkundengeheimnisses, vgl. Art. 47 BankG.[17] Demnach gilt entsprechend einer Definition der schweizerischen Bankiervereinigung:

13 Vgl. insofern auch Art. 35 DSG, neuerdings insb. Art. 62 nDSG; zu Rechten (und Pflichten) der Geheimhaltung Druey, BJM 2005, 57 ff.; Hoeren, MMR 1998, Beilage, 6 ff., 7, bezeichnet das Geheimnis als das älteste informationelle Zuordnungskonzept; zum «kleinen» Berufsgeheimnis nach totalrevidiertem DSG und den «grossen Berufsgeheimnissen» vgl. Rosenthal, Jusletter vom 16. November 2020, N 202 f.

14 Jüngst zu den einschlägigen Rechtsquellen Bohnet/Melcarne, JdT 2020 II, 31 ff.; zum strafrechtlichen Schutz der Geheim- und Privatsphäre in der Pflege Diethelm, in: Landolt/Blum-Schneider/Breitschmid u. a. (Hrsg.), 9 ff.; zu den Amts- und Berufsgeheimnissen gemäss Art. 320 f. StGB auch spezifisch im Kontext des medizinischen Kontextes Brühwiler-Frésey, 110 ff.

15 Hierzu Schluep/Lüchinger (Hrsg.), mit zahlreichen Beiträgen, die das Anwaltsgeheimnis in verschiedenen Facetten und Bezügen darstellen; zum Schutz der Verschwiegenheit von Rechtsanwälten, Steuerberatern und Notaren vor strafprozessualen Ermittlungsmassnahmen nach deutschem Recht Kühne, 17 ff.

16 Allgemein zum Persönlichkeits- und Datenschutz im Fernmelde- und Telekommunikationsbereich, Bondallaz, mit Hinweisen zum Fernmeldegeheimnis, N 1060 ff.

17 Vertiefend zu diesem auch in seinem Zusammenspiel mit dem DSG, dem Schutzzweck der Persönlichkeit und der Frage der Auswirkungen von Pseudonymisierung und Anonymisierung unlängst Hirsch/Jacot-Guillarmod, RSDA 2020, 151 ff.; Emmenegger/Zbinden, 193 ff., 203; Aubert/Béguin/Bernasconi et al., *passim*; vgl. sodann Anhang 3 des Rundschreibens 2008/21 der FINMA; zur Rolle des Datenschutzrechts im Bankaufsichtsrecht auch Meier, in: Emmenegger (Hrsg.), 1 ff., 4 ff.; zu den jüngsten Entwicklungen im Zusammenhang mit dem globalen Standard über den automatischen Informationsaustausch über Finanzkonten (AIA) <https://www.efd.admin.ch/efd/de/home/steuern/steuern-international/steuerlicher-informationsaustausch.html> (zuletzt besucht am 30. April 2021); Michlig,

> «Das Bankkundengeheimnis (Art. 47 des Bankengesetzes) ist ein eigentliches Berufsgeheiminis und als solches vergleichbar mit jenem der Ärzte oder Anwälte. Es zielt auf den Schutz der finanziellen Privatsphäre und schützt sämtliche Tatsachenfeststellungen, Werturteile und sonstige Daten (einschliesslich personenbezogener Auswertungsresultate), die sich einem Bankkunden zuordnen lassen.»[18]

Zudem werden Amtsträgerinnen und Amtsträger verschiedenenorts öffentlich- 37
rechtlich unter Geheimhaltungspflichten gestellt, strafrechtlich abgesichert über Art. 320 StGB.

Geheimhaltungspflichten lassen sich, wenn sie sich auf Personenangaben bezie- 38
hen, als das *älteste Instrument mit datenschutzrechtlicher Stossrichtung* beschreiben. Ebendies wird, ausgehend vom berühmten Hippokratischen Eid, sogleich vertieft werden.[19]

Der Einstieg erfolgt indes literarisch: Aufschlussreich für eine datenschutzrecht- 39
liche Arbeit, die einen Beitrag zur Weiterentwicklung der Materie leisten will, sind die *Geheim- und Passworte*. Sie spielen in unzähligen literarischen Werken eine Schlüsselrolle. Ein Seitenblick auf zwei berühmte *Volksmärchen*, *Ali Baba und die vierzig Räuber* sowie *Rumpelstilzchen*, zeigt, dass beide zahlreiche informationelle und damit informative Aspekte, Motive und Elemente verwenden. In diesem Sinne: *Sesam, öffne Dich!*

«Sesam, öffne Dich!», das ist das gehackte Passwort, der «PIN- 40
Code» zum «Safe» in *Ali Baba und die vierzig Räuber.*[20] An dieser Stelle eine kurze Erinnerung zur Erzählung aus Tausendundeine Nacht: Ali Baba vernimmt das geheime Wort vom Hauptmann der Räuberbande und es gelingt ihm, sich damit Zutritt zum Berg und dem dort gelagerten Schatz zu verschaffen. Ali Baba nimmt einen Teil des Schatzes an sich und bringt ihn nach Hause, wo seine Frau diesen mit einem Mass der Frau von Ali Babas Bruder, Casim, misst. Als sie das Mass zurückgeben will, übersieht sie eine Goldmünze am Boden des Masses. Damit erfahren auch Casim und seine Frau von dem Schatz, den Ali Baba an sich genommen hatte. Casim stellt Ali Baba zur Rede. Letzterer verspricht seinem

---

AJP 2014, 1055 ff.; <https://www.finews.ch/service/advertorials/39491-dswiss-tobias-christen-bankgeheimnis-datenschutz-schweiz-banken-privatsphaere-schutz> (zuletzt besucht am 30. April 2021); weitere datenschutz- und informationsrechtliche Themen werden mit verschiedenen Beiträgen in Emmenegger (Hrsg.) abgehandelt; zu Informationspflichten des Bankiers namentlich bei Anlagegeschäften Emmenegger, in: Chappuis/Winiger (Hrsg.), 67 ff.; viel Aufmerksamkeit auf sich gezogen haben das Bankkundengeheimnis, der Datenschutz resp. die Pflicht zur Lieferung von Personenangaben, namentlich mit Blick auf Tax Law Offences und dem Verhältnis zwischen der Schweiz und den USA; Althaus Stämpfli zur Verteilung von Bankkundendaten innerhalb von Konzernstrukturen und an dritte Dienstleister, *passim;* zum Bankgeheimnis in Deutschland Wech, *passim*; Kahler/Werner, 143 ff.

18 <https://www.swissbanking.ch/de/finanzplatz/informationen-fuer-bankkunden-und-unternehmen/datenschutz-und-datengovernance> (zuletzt besucht am 30. April 2021).

19 Vgl. allerdings kritisch zum Eid Steinke, SAEZ 2016, 1699 ff.

20 Christensen/Spies (Hrsg.), 123; auch Hoeren, MMR 1998, Beilage, 6 ff., bezieht sich in einem informationsrechtlichen Aufsatz auf dieses alte Märchen.

Bruder die Hälfte seines Schatzes, sofern dieser die Sache für sich behält. Damit gibt sich Casim aber nicht zufrieden: Er will von Ali Baba das Zauberwort erfahren, um selbst in die Schatzhöhle zu gelangen. «Sesam, öffne Dich!» – auch für ihn öffnet sich das Tor zur Höhle mit dem Schatz. Allerdings wird Casim zum Verhängnis, dass er das Zauberwort beim Verlassen der Höhle vergessen hat. Die Räuber wollen nunmehr herausfinden, wie das Geheimwort zu Casim gelangt ist, was dieser unter der Bedingung der Geheimhaltung sowie des Erhalts von Gold verrät. Nichtsdestotrotz markiert die Räuberbande in der Folge das Haus, in dem Ali Baba lebt, mit einem Kreidezeichen. Ali Babas Frau bemerkt beim Verlassen des Hauses ebendieses Zeichen und wittert Gefahr. Sie nimmt eine Kreide und markiert weitere Nachbarshäuser mit demselben Zeichen.[21] Die daraus resultierende Unmöglichkeit, den Gesuchten aufzuspüren, führt letzten Endes zur Tötung des Hauptmanns. Zudem wird die gesamte Räuberbande von Ali Baba und seiner Frau bezwungen. Das Geheimwort (der «PIN-Code») «Sesam, öffne Dich!» und damit auch der Schatz werden in der Folge von Ali Baba auf seinen Sohn und von Generation zu Generation vererbt.[22]

41 Offensichtlich präsentieren sich damit Informationen und (Personen-)Daten keineswegs erst seit dem 20. Jahrhundert Gold wert zu sein. Vielmehr berichten schon alte Märchen davon, wie geheime Information den Zugang zu etwas Wertvollem, zu einem Goldschatz – einem Gut – eröffnet. Dem Geheimnisträger – dem Hauptmann der Räuberbande in Ali Baba – wird zum einen zum Verhängnis, dass Ali Baba von ihm das Zauberwort erfahren konnte. Zum anderen versagt er dabei, die Geheimnisbrüchigen durch ein Zeichen an der Hauswand einwandfrei zu identifizieren. Dem Anführer der Räuberbande kommt somit informationell die Schlüsselrolle zu. Im Hauptmann der Räubergruppe kulminieren mehrere Informationsprivilegien und -pflichten. Sie markieren und konsolidieren seine Herrschaftsposition. Diese wird allerdings sogleich erodiert: Mehrere informationelle Versäumnisse im Verantwortungskreis des Räuberhauptmanns führen nicht nur zu seiner Entmachtung, sondern zu seiner Enthauptung: Man meinte es ernst mit dem korrekten Umgang mit Informationen; informationelle Verstösse wurden drakonisch geahndet. Geheimnisse stehen seit jeher unter einem ganz besonderen Schutz.

21 Zur Praxis der Häusernummerierung im Genf des 18. Jahrhunderts Cicchini, Urban Hist. 2012, 614 ff.; «Obfuscation» benannten im 21. Jahrhundert die Philosophin Nissenbaum, eine Pionierin der Datenschutzwissenschaft, und der Medien-Historiker Brunton eine Praxis, die darauf zielt, Identifizierungsprozesse zu torpedieren, vgl. Brunton/Nissenbaum, First Monday 2011, 1; Dies., Obfuscation, *passim;* Howe/Nissenbaum, in: Kerr/Steeves/Lucock (Hrsg.), 417 ff., 434 f.; zu Strategien, welche die Identifizierung und Personendatenverarbeitungen torpedieren, Litman, Stan. L. Rev. 2000, 1283 ff., 1285; zum Widerstand von «renitenten Adligen» und «maulenden Mönchen» gegen die Häusernummerierungen auch Tantner, Ordnung der Häuser, 138 f.

22 Christensen/Spies (Hrsg.), 129; ein ganz ähnliches Thema wird im Märchen vom Simeliberg der Gebrüder Grimm verarbeitet, vgl. Gebrüder Grimm, 648 ff.

Zwei Metaphern der Geschichte aus Tausendundeine Nacht werden im Laufe dieser datenschutzrechtlichen Arbeit wiederholt auftauchen. Die erste davon sticht ins Auge und weist starke Symbolkraft auf: 42

Erstens der Berg resp. das Berginnere oder das Haus resp. das Hausinnere als Schutzbereiche für das Geheime, das Private, das Schutzwürdige. Diese *räumlich-statische Repräsentanz* bleibt bis heute, namentlich in der persönlichkeitsrechtlichen Sphärentheorie, wirkungsmächtig.[23] 43

Zweitens bringt die Geschichte ein weiteres Bild hervor: dasjenige von *Informations- und Goldflüssen* zwischen zwei einander gegenübergestellten «gesellschaftlichen Einheiten». Auf der einen Seite der Nukleus der Räuberbande, von dem aus Informationen wie auch Gold in ein anderes System mit anderen Akteuren, Ali Baba und dessen Familie, transmittiert werden. Ali Baba betont denn auch, dass er selbst nicht zum Räuber werde, wenn er mittels Geheimwort auf das Raubgut zugreife. Anlehnend lässt sich die Geschichte auch aus einer *dynamischen Perspektive* lesen, deren Linse sich auf (un-)erwünschte Informations- und Edelmetallflüsse zwischen verschiedenen Gesellschaftsgruppen richtet. 44

Beide Bilder scheinen auch im zweiten hier interessierenden Märchen auf, *Rumpelstilzchen*.[24] Es ist auf der einen Seite die Müllerstochter, die zur Königin werden kann, sofern sie die ihr gestellte Aufgabe erfüllt, aus Stroh Gold zu spinnen. Auf der anderen Seite steht Rumpelstilzchen, das an ihrer statt und nicht ohne eine Gegenleistung zu fordern das Stroh zu Gold verarbeitet. Nachdem die Müllerstochter ihm für seine Dienste erst ihr Halsband und dann einen Ring gegeben hat, kann sie dem Rumpelstilzchen beim dritten Mal kein Gut mehr anbieten. Dieses will nun etwas Lebendiges und verlangt ihr erstes Kind. Nach der Geburt dieses Kindes räumt das Rumpelstilzchen der verzweifelten Königin eine dreitägige Frist ein. Nur wenn sie innerhalb dieser Zeit seinen *Namen* erraten könne, werde es ihr das Kind lassen. Die Königin entsendet Boten, um den Namen herausfinden zu lassen – zunächst ohne Erfolg. Erst am dritten und letzten Tag berichtet ein Bote der Königin: 45

> «Neue Namen habe ich keinen einzigen finden können, aber als ich an einen hohen Berg um die Waldecke kam, wo Fuchs und Has sich gute Nacht sagen, so sah ich da ein kleines Haus, und vor dem Haus brannte ein Feuer, und um das Feuer sprang ein gar zu lächerliches Männchen, hüpfte auf einem Bein und schrie: „Heute back ich, morgen brau ich, übermorgen hol ich der Königin ihr Kind; ach, wie gut, dass niemand weiss, dass ich Rumpelstilzchen heiss!“»[25]

23 Zur verletzten Wohnung innerhalb eines Heftes zur Privatsphäre auch Güntner, 15 ff.

24 Auf beide Märchen – *Ali Baba* und *Rumpelstilzchen* – wird, ohne genauere Auseinandersetzung, in zeitgenössischen rechtswissenschaftlichen Arbeiten verwiesen, vgl. Schiedermair, 7; Hoeren, MMR 1998, 6 f.; Weber, in: Schweizer/Burkert/Gasser (Hrsg.), 1009 ff.

25 Gebrüder Grimm, 316.

46 Der Name als personenbezogene Angabe, wie man es heute nennen würde, ist in dieser Geschichte wegen seiner bizarren Natur ein zuverlässiger Personenidentifikator. Für die Königin ist er das «Macht-» resp. «Zauberwort», um ihr Kind nicht zu verlieren.

47 Das ist bemerkenswert: In heutiger Zeit wird der Name meist pauschal als «belanglose», «gewöhnliche» Personenangabe taxiert. Er wird gerade nicht zu den «besonders schutzwürdigen Personenangaben» gezählt.[26] Die Kategorie der *besonders schutzwürdigen resp. schützenswerten Personendaten* wird in den späteren Datenschutzerlassen ein Kernelement sein. Für ihre Verarbeitung werden qualifizierte, strengere Datenschutzvorgaben festgelegt. Ausgegangen wird von einer Idee, wonach die «Natur» bestimmter Personendaten diese per se «besonders schutzwürdig» machen.[27] In diesem Konzept spiegelt sich unübersehbar das Konzept einer räumlichen und sphärisch-abstrakt definierten «Privatheit» oder «Intimität». Allerdings greift das Konzept zu kurz, wie im Zuge dieser Arbeit an mehreren Stellen festgestellt wird. Anhand der Kategorie der besonders schutzwürdigen Personendaten liesse sich denn auch das in dieser Schrift entwickelte neue Paradigma, das Recht auf informationellen Systemschutz, entfalten.

48 Das Märchen zeigt uns bereits, dass es stets die *Geschichte und der Kontext im Hintergrund* sind, die für die Frage der (spezifischen) Schutzwürdigkeit der Angabe einschlägig sind. Der Identifikator wird der Königin sodann von einem Boten zugetragen, der als Informationsmittler resp. *Medium* fungiert.[28] Dieser belauscht das Männchen, fern von den königlichen Mauern, am Waldrand. Das Männchen macht seinen Namen unvernünftigerweise in einem nicht geschützten Aussenbereich «öffentlich», anstatt seine Vorfreude diskret in seinem Haus zu besingen. Aus dem Lebensbereich des Rumpelstilzchens fliesst nun die entsprechende Personenangabe der Königin zu. Zwei verschiedene Welten mit zwei so unterschiedlichen Akteuren – Königin einerseits, Rumpelstilzchen andererseits – und dem Boten als Informationsmittler. Der Transfer einer Personenangabe wird

26 Vgl. Art. 3 lit. c DSG resp. Art. 5 lit. c nDSG; allgemein kritisch zu der Idee eines «belanglosen Personendatums» unter Bezug auf das Volkszählungsurteil Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 34; Ders., in: Brem/Druey/Kramer/Schwander (Hrsg.) illustrativ nicht nur zur Fehlvorstellung, wonach der Name ungeachtet des Verarbeitungszusammenhangs (k)eine besonders schutzwürdige Angabe sei, 469 ff.; Ders. im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt abgerufen am 30. April 2021); zur Anknüpfung spezifischer Rechtsfolgen je nach Zuweisung einer Personenangabe zu den besonders schützenswerten Angaben oder zu den nicht besonders schützenswerten Angaben vgl. zweiter Teil, VI. Kapitel, B.; zur Kategorie der besonders schützenswerten Personendaten Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff.; bemerkenswert in diesem Zusammenhang BGE 124 I 85, kritisch dargestellt im dritten Teil, VII. Kapitel.

27 Hierzu mehr zweiter Teil, IV. Kapitel, B.2.2.

28 Historisch zur Funktion des Boten (auch des Engels) als Informationsmittler Krajewski, 75, 155 ff., 389; Groebner, 37, 54, 57, 63, 122 ff., 120, 124, 126, 178; Dommann, 43 ff. zur mechanischen Vervielfältigung und zur Kontrolle der Verwertung mit Blick auf durch Copyright geschützte Werke und zur Kopie sowie Geheimhaltung, 138 ff.

zum entscheidenden Element für den Verbleib des Kindes – man könnte es als das wertvollste «Gut» im Familiensystem bezeichnen – in seiner herkömmlichen Welt.

Auch in diesem Märchen sind informationell betrachtet *zwei verschiedene Sichtweisen resp. Aspekte* angelegt: zum einen die räumliche Metapher des Aussenbereichs – vor dem Haus am Waldrand –, zum anderen auch die dynamische Dimension des Transfers von Personenangaben aus dem Lebensbereich des Rumpelstilzchens in denjenigen der Königin, das Königreich. Der Wert der Information ist in diesem Märchen gleichermassen unermesslich. Die Information entscheidet über den Verbleib des Kindes bei seiner Mutter resp. dessen Verlust an das Rumpelstilzchen. Darin, dass die Königin seinen Namen in Erfahrung gebracht hat, sieht das Männchen einen Pakt mit dem Teufel und zerstört sich in der Folge selbst. Auch dieses Märchen lässt keinen Zweifel daran: Gewünschte oder ungewünschte Informationsflüsse zeitigen einschneidende Konsequenzen über die isolierte informationelle Betrachtung hinaus. 49

Was aber lehren uns die Geschichten? Beide Erzählungen – Ali Baba und Rumpelstilzchen – thematisieren zunächst die *Bedeutung und den Wert von Informationen*, mit denen der Zugriff auf ein monetäres Gut – der Goldschatz bei Ali Baba – resp. auf einen nicht-monetären Wert – das Kind – möglich wird. Der Transfer der Information steht in einer engen Korrelation zum Transfer eines anderen Gutes, sei es eines der ökonomischen Sphäre, sei es eines aus dem Familienbereich. Insofern lässt sich sagen, dass die *Information ein Mittel zum Zweck* ist und damit gewissermassen eine *akzessorische Bedeutung* hat. Die Märchen greifen zudem gleichermassen eine bis heute prägende, *räumlich-statisch konnotierte Zuordnung* von Informationen in Innen- und Aussenbereiche, in «geheim», «privat» resp. «öffentlich» auf. 50

Darüber hinaus aber laden beide Geschichten zu einem *Perspektivenwechsel* ein. Sie erzählen von der Relevanz verschiedener Akteure in ihren Rollen, die in verschiedenen Lebensbereichen agieren. Hierbei werden die *zwischen* diesen Bereichen stattfindenden *Informationsflüsse* als erwünscht resp. unerwünscht beschrieben. Das Geheimnis resp. das Geheimwort, aber auch die Geheimhaltungspflicht lassen sich damit schon früh als *Schutzinstrumente* ausmachen: Sie blockieren den Informationsfluss.[29] Der Schutz der Information dient dahinterliegend dem Schutz von Gütern anderer «Ingredienz» – von Gold, einem Kind. 51

29 Das Konzept resp. Bild von Datenflüssen konnte sich bis heute nicht als Bezugspunkt für die datenschutzrechtliche Normierung durchsetzen; gleichwohl erwähnt insb. Druey, BJM 2005, 57 ff., 66, das Bild in mehreren seiner informationsrechtlichen Schriften, z. B. auch in einem Beitrag zur Geheimhaltung. Ebenda wird auch das Bild des Schliessens resp. Öffnens von einem Hahn verwendet; zur Frage einer Gestaltung von Informationsflüssen unter Ausrichtung an der Gerechtigkeitstheorie von John Rawls Hoeren, 38 ff.

Entsprechend wird bereits an dieser Stelle der Begriff der *Akzessorietät des informationellen Schutzes* vorgeschlagen.

52 *Back to reality:* Nicht nur Geheimworte, auch Geheimhaltungspflichten haben eine lange Tradition. Sofern sie sich auf Personenangaben beziehen, sind sie, wie erwähnt, die wohl ältesten Instrumente, die – in heutiger Terminologie – auch Datenschutzfunktionen wahrnehmen.[30] In der datenschutzrechtlichen Literatur werden der Eid des Hippokrates, das Arztgeheimnis sowie das Beichtgeheimnis – nebst der Errichtung bürokratischer Informationssysteme im Zuge nationalstaatlicher Konsolidierungsprozesse – als historische Vorläufer des Datenschutzrechts beschrieben.[31] Traditionsreich sind sodann Staats- und Amtsgeheimnisse, Geheimhaltungspflichten, denen Postboten («Postgeheimnis») und Diener unterstellt wurden, sowie Diskretionspflichten von Betreibern von Adressbüros.[32] Bleibt man beim Bild des Informationsflusses, so bildet das *Geheimnis gewissermassen das Wehr* oder die *Stauvorrichtung*.[33] Die Information soll nicht weiterfliessen, stattdessen beim Informationsempfänger vertraulich verbleiben. Diesen Bedeutungsaspekt bringt der lateinische Begriff für Geheimnis, *secretum, secernere – abgetrennt, trennen,* unmissverständlich zum Ausdruck.[34] Geheimhaltungspflichten blockieren den *Fluss bestimmter Informationen zwischen verschiedenen Personen und Bereichen*.

53 In Anbetracht der Bedeutung, welche Geheimhaltung und Verschwiegenheit überlieferterweise haben, erstaunt es auch nicht, dass sich historisch entsprechende Symbole der Repräsentation finden. So rief beispielsweise die Rose bereits im Mittelalter als Signum in Gestalt einer Schnitzerei oder getrocknet als Ausstattung des Beichtstuhles die Verschwiegenheit, die Pflicht zur Geheimhaltung ins

30 Dass es sich z. B. bei den beruflichen Schweigepflichten, vgl. Art. 321 StGB, wie der ärztlichen Schweigepflicht um eine datenschutzrechtliche Vorgabe handelt, zeigt neben dem Verweis in Art. 35 DSG nicht zuletzt auch der Blick auf die Homepage des EDÖB. Hier finden sich Informationen unter den Rubriken «Telekommunikation» (wozu das Fernmeldegeheimnis gehört), «Handel und Wirtschaft», «Versicherung», «Statistik», «Register» und «Forschung» usf. Der Titel «Gesundheit» widmet sich ausführlich den ärztlichen resp. medizinalberuflichen Schweigepflichten. Geheimhaltungs- und Schweigepflichten – sie blockieren Informationsflüsse – sind ein traditionsreiches und erprobtes Kernelement des Datenschutzrechts; nach Totalrevision vgl. in diesem Zusammenhang Art. 62 nDSG; Bull, Computer, 77 ff., beschreibt die Geheimhaltungspflichten unter dem Titel der geistigen Wurzeln des Datenschutzrechts.

31 M. w. H. Nissenbaum, 172; von Lewinsky, in: Arndt/Augsberg (Hrsg.), 196 ff., 201 ff.; zum Arztgeheimnis auch der Beitrag zum Datenschutz im Gesundheitsbereich Günter, in: Schweizer (Hrsg.), 151 ff., 151 f., der die Bezeichnung Patientengeheimnis als treffender beurteilt – die Strafnorm schütze den Patienten; so auch Brühwiler-Frésey, 121, wonach es um den Schutz der Geheim- und Privatsphäre der Personen gehe, die mit Personen der jeweiligen Berufsgattungen verkehren; zur Bürokratie als Symbol für die rational handelnde Regierung Herzfeld, 17 ff.

32 Hierzu Tantner, Suchmaschinen, 194; Groebner, 112; Krajewski, 412; zur Bedeutung des späteren Briefgeheimnisses Güntner, 71 ff.

33 In den Worten von Nissenbaum würde es sich um ein «Transmissionsprinzip» handeln, 201 f.; zum Begriff des Informationsflusses Miller, 148.

34 M. w. H. hierzu im Kontext des Familieninformationsrechts Pfaffinger, N 116.

Bewusstsein.[35] Die Rose ermahnte auch in Rats- und Rittersälen über Tafeln zur Diskretion. *Sub rosa dictum*, ein Dictum, wie es beispielsweise bei Sebastian Brant um 1494 zu finden ist,[36] war denn auch während Jahrhunderten eine gebräuchliche «Redewendung» für Angelegenheiten, die «unter dem Siegel der Verschwiegenheit» bleiben sollten. In diesem Zusammenhang ist sodann auf den jünglingshaften Gott der Verschwiegenheit, Harpokrates, hinzuweisen, dessen Abbild die Römer auf ihren Siegelringen trugen. Harpokrates wird meist am Tempeleingang sitzend dargestellt, seinen Zeigefinger an den Mund gelegt. Er ist Schutzpatron für das Briefgeheimnis und damit eine prägende Figur.[37]

Vertiefend werden nachfolgend *drei traditionelle Geheimhaltungspflichten* be- 54
leuchtet – der Eid des Hippokrates, das Beichtgeheimnis und das Geheimnis der Adoption. Hierbei wird sich bestätigen, dass Geheimhaltungspflichten *als Steuerungsinstrument von Informationsflüssen* zu verstehen sind.

Das achte Prinzip des auf ca. 400 v. Chr. datierenden Eides des Hippokrates 55
lautet zu Deutsch:

> «Über alles, was ich während oder ausserhalb der Behandlung im Leben der Menschen sehe oder höre und das man nicht nach aussen tragen darf, werde ich schweigen und es geheim halten.»[38]

Ein entsprechendes Bekenntnis ist ebenso aus der islamischen (Rechts-)Kultur 56
durch den persischen Haly Abbas Ahwazy aus dem 10. Jahrhundert überliefert: In seinem Liber Regius, in dem sich der Arzt in einem einleitenden Kapitel den ethischen Grundfragen des Ärztestandes widmet, bezieht er sich auf den Hippokratischen Eid:

> «A physician should respect confidence and protect the patient's secrets. In protecting a patient's secrets, he must be more insistent than the patient himself. A physician should follow the Hippocratic counsel.»[39]

Die ärztliche Schweigepflicht bildet heute einen festen Bestandteil des staatlichen 57
Standesrechts, in der Schweiz, vgl. Art. 40 lit. f. des eidgenössischen Medizinalberufegesetzes, Art. 16 lit. f. des Gesundheitsberufegesetzes und Art. 323 StGB. Begründet wird diese Schweigepflicht vorab mit dem Schutz der *Intim- und Privat-*

35 Heinz-Mohr/Sommer, Die Rose, 112 f.
36 Brant, Abschnitt 7, von Zwietrachtstiftern, 16/Z13.
37 Vgl. zu diesem ägyptischen Götterkind Sandri, *passim*, die allerdings auf eine Fehlinterpretation des Fingers am Mund als Symbolisierung des Schweigens hindeutet, 100; zum Briefgeheimnis Güntner, 71 ff.
38 Pschyrembel Klinisches Wörterbuch, 267. Aufl., 2017, 695.
39 Vgl. Reich (ed.), Encyclopedia of Bioethics, Advice to a Physician, Advice of Haly Abbas, New York 1995, <http://www.bioethics.org.au/Resources/Codes%20and%20Oaths/Advice%20to%20a%20Physician.pdf> (zuletzt besucht am 30. April 2021); Nissenbaum, 173.

sphäre der zu behandelnden Person, der Patientin und des Patienten.[40] Hier spiegelt sich die heutige Orientierung am Subjekt- und Persönlichkeitsschutz, wie sie auch das DSG prägt, vgl. Art. 1 DSG und Art. 1 nDSG. Zugleich sichert die ärztliche Schweigepflicht das *Vertrauensverhältnis* zwischen Ärztin und Patient, womit es eine relationale Bedeutung enthält.[41] Des Weiteren wird mit dem Institut der Gesundheitssektor selbst geschützt.[42] Würden Informationen, welche die Ärzteschaft im Rahmen von Behandlungsverhältnissen erlangen, unbeschränkt zirkulieren, würde damit das Hauptziel des Gesundheitsbereichs an sich – der Schutz der Gesundheit – untergraben: Menschen würden keine ärztliche Hilfe mehr in Anspruch nehmen, von Pontius zu Pilatus resp. von Ärztin zu Ärztin pilgern oder nur punktuell Symptome schildern. Ebendies würde den allgemeinen Gesundheitsschutz nachhaltig erodieren.

58 Allerdings gilt die ärztliche Schweigepflicht auch unserer Tage *nicht absolut*: Eine Entbindung davon kann zum einen durch die Einwilligung der behandelten Person erfolgen, zum anderen aufgrund einer gesetzlichen Grundlage, welche die näheren Voraussetzungen präzisiert (z. B. Notwendigkeit eines behördlichen Entscheides). Für den Fall, dass jemand sich selbst oder Dritte gefährdet, ist eine Entbindung von der Schweigepflicht beispielsweise nach Art. 453 ZGB im Rahmen von Kindes- und Erwachsenenschutzmassnahmen denkbar.[43]

59 Kaum ein Fall hat die Komplexität der (datenschutz)rechtlichen Herausforderungen und die Frage nach den Grenzen der ärztlichen Schweigepflicht dringlicher aufgezeigt als der Fall Lubitz.[44] Lubitz brachte am 24. März 2015 als Co-Pilot ein Flugzeug zum Absturz und riss damit 150 Menschen in den Tod. Lubitz hatte lange vor dem schicksalhaften Tag mehrere Ärzte konsultiert, wobei depressive Züge beim Patienten und Piloten attestiert wurden. Wäre zum Schutz des Transportsektors, wo die Sicherheit der Flugpassagiere höchste Priorität hat, ein Informationsfluss unter Durchbrechung des Arztgeheimnisses angezeigt gewesen? Oder ist die Flugsicherheit auf anderem Wege sicherzustellen?

60 Nicht nur historisch betrachtet ist ebenso das *Beichtgeheimnis* der katholischen Kirche, welches sein Pendant für die reformierte Kirche wohl im Seelsorgege-

40 Kuhn/Poledna, 743, 746; eine aktuelle Thematisierung der datenschutzrechtlichen Relevanz der ärztlichen Schweigepflicht im Zusammenhang mit der COVID-19-Krise findet sich bei Dougoud/Pfaffinger, «Das wahre Problem mit den Schüler-Masken», Inside Paradeplatz vom 25. Januar 2021.

41 Kuhn/Poledna, 744.

42 Vgl. Nissenbaum, 172; zum öffentlichen Interesse hinter dem Arztgeheimnis, welches neben die privaten Interessen sowie Standesinteressen tritt, m. w. H. Boll, 6 ff.

43 Vgl. Geiser, BSK ZGB I, Art. 453 N 1; zur Entbindung vom Arzt- sowie Anwaltsgeheimnis auch Boll, 14 ff.

44 NZZ, 11 Minuten, Zürich 2015, <https://www.nzz.ch/nzzas/nzz-am-sonntag/11-minuten-1.18512325?reduced=true> (zuletzt besucht am 30. April 2021); NZZ, Wenn Ärzte nicht mehr schweigen, Zürich 2015, <https://www.nzz.ch/schweiz/wenn-aerzte-nicht-mehr-schweigen-1.18519132?reduced=true> (zuletzt besucht am 30. April 2021).

heimnis findet, für eine datenschutzrechtliche Studie von Interesse. Ersteres ist im *Codex Iuris Canonici* in c. 983 f. niedergelegt. Es gilt absolut, wobei selbst gewichtige öffentliche bzw. staatliche Interessen keinen Rechtfertigungsgrund für die Offenbarung dessen, was im Rahmen der Beichte zur Kenntnis genommen wurde, liefern können. Es darf entsprechend nicht einmal zur Rettung des eigenen oder fremden Lebens preisgegeben werden und gilt über den Tod des Pönitenten hinaus.[45] Vom Beichtgeheimnis kann einzig der Oberhirt als höhere Instanz dispensieren, was bislang allerdings nie geschehen ist.[46] Geheimhaltungspflichten sind also verschiedenen Institutionen bekannt und dienen entsprechend verschiedenen Systemen, wobei das Beichtgeheimnis der katholischen Kirche eine scharfe Grenze – gerade mit Blick auf den Transfer der Informationen, die im Kontext der Beichte gemacht werden – zum staatlichen System markiert. Umgekehrt und gleichzeitig wird das Beicht- wie auch das Seelsorgegeheimnis vom staatlichen Recht geschützt.[47] Immerhin ist vor Augen zu führen, dass die «öffentliche Brandmarkung» von Sünderinnen und Sündern seit jeher ein wichtiges Sanktionierungsinstrument war. Die kanonische Busse war eine «öffentliche» Angelegenheit, die meist im Gottesdienst bekannt gegeben und vollzogen wurde. Hierzu die Worte von Augustinus:

> «Die ihr Busse tun seht, haben ein Verbrechen, ein Vergehen oder sonst eine greuliche Tat begangen. Deshalb büssen sie.»[48]

Die Schwere der Sünde sowie die Dauer und Art der Busse wird für die Gemein- 61
deangehörigen sichtbar gemacht. Über die Kirchengemeinde hinaus wurden Sünden allgemein öffentlich gemacht und Sündiger der allgemeinen Diskreditierung ausgesetzt, mit Praktiken wie der Busspilgerschaft. Bei ihr mussten Büsser auf langen Wallfahrten schwere Ketten tragen oder Geleitbriefe vorlegen und unterschreiben lassen.[49] Den «hierarchischen Blick» des Justizapparates und damit die Überwachung, die durch architektonische Konstruktionen bei Gefängnisbauten unterstützt wurde, beschreibt Foucault als einfaches und erfolgreiches Instrument der *Disziplinarmacht*.[50]

Drakonische Strafen finden sich historisch betrachtet in einem weiteren Kon- 62
text, der ebenso mit Geheimnissen arbeitet: *der Familienkontext*. Insofern ist

45 Suter, 40.
46 Vgl. dazu Schwendenwein, 336 ff.; Browe, Das Beichtgeheimnis im Altertum und Mittelalter, Vierteljahresschrift für Theologie und Philosophie, Sonderabdruck, 1 ff.; Dr. Markus Arnold sei herzlich für diese Hinweise gedankt; vertiefend zum kirchlichen Datenschutzrecht die Beiträge in Sydow (Hrsg.), Kirchliches Datenschutzrecht. Datenschutzbestimmungen der katholischen Kirche. Handkommentar. Nomos-Kommentar 2020.
47 Zum Ganzen mit dem Hinweis, wonach für die Schweiz umstritten sei, ob ein Schutz über Art. 321 StGB erfolge, Suter, 39 ff.
48 Zit. nach Browe, Scholastik 1934, 1 ff.
49 Ders., a. a. O., 1 f.
50 Foucault, 220 ff.

namentlich das *Institut der Adoption* zu nennen, wobei der Adoptionsakt als Tatsache historisch immer wieder stigmatisiert und verdrängt wurde.[51] Im *Codex Hammurabi* wird die Geheimhaltung der Kindesannahme statuiert, wobei eine Verletzung dieser Pflicht mit Schärfe sanktioniert wurde: Sprachen Adoptierte über die Adoption, wurde ihnen die Zunge abgeschnitten; suchten sie nach ihren leiblichen Eltern, stach man ihnen die Augen aus. Aus der Antike überliefert ist die Sage von Ödipus, der als Kind durch ein Königspaar adoptiert wurde. Er versuchte seine Herkunft in Erfahrung zu bringen, begegnete auf seiner Suche seinem leiblichen Vater und verlor am Ende sein Augenlicht.

63 In Europa setzte sich ab den 1950er Jahren im Familienrecht die geheime Volladoption durch, die einen informationellen *clean break* zwischen der leiblichen Familie und der adoptierenden Familie umsetzte.[52] An erster Stelle sollte sie es der Adoptivfamilie ermöglichen, ein Leben zu führen, als ob sie eine «ganz normale» Familie sei. Damit war gemeint, dass sich die Adoptiveltern so fühlen sollten, als ob sie die «echten» bzw. leiblichen Eltern wären, und das Kind, als ob es das «echte» bzw. leibliche Kind der Adoptiveltern wäre. Mittlerweile allerdings hat sich die Erkenntnis durchgesetzt, dass die Inkognito-Adoption in aller Regel weder dem Wohl des Kindes noch demjenigen der abgebenden Eltern und ebenso wenig dem Interesse der Adoptiveltern zuträglich ist. Vielmehr wird die Inkognito-Volladoption heute als Instrument des Institutionenschutzes beschrieben, das auf den Schutz eines Familienideals, der ehelichen Einheitsfamilie, abzielt.[53]

64 Heute wird sie in Recht und Praxis sukzessive durch halboffene und offene Adoptionsmodelle ersetzt. Sie zielen darauf ab, in transparenter(er) Weise die beiden familiären Systeme und persönlichen Bedürfnisse auch im Rahmen der Identitätsbildung zu koordinieren.[54] Ging man lange davon aus, dass die Inkognito-Adoption das System der Familie schütze, wird heute überwiegend die Meinung vertreten, dass Adoptionsformen, in denen der Adoptionsprozess offen thematisiert wird, nicht nur den Personen des Adoptionsdreiecks als Individuen und Persönlichkeiten sowie deren Beziehungen besser Rechnung tragen, sondern auch den familiären Systemen an sich förderlich sind. Im zeitgenössischen Familienrecht lässt sich nicht zuletzt im Zuge der gestiegenen Toleranz für plurale Familien- und Lebensmodelle dieser Trend zu erhöhter Transparenz auch ausserhalb des Adoptionsrechts verzeichnen.[55]

51 Hierzu m. w. H. Pfaffinger, N 8 ff.
52 Dies., N 93 ff.
53 Hierzu Dies., Ancilla Iuris (anci.ch) 2016, 49 ff.
54 Vgl. die Lockerung in den Art. 268b–e ZGB in der seit dem 1. Januar 2018 in Kraft stehenden Fassung; vertiefend zur Entwicklung und Forderung auf Anerkennung von halboffenen und offenen Adoptionsformen Dies., N 139 ff.
55 In Bezug auf die Vaterschaftsvermutung Dies., FamPra.ch 2014, 604 ff.

Der Blick auf die drei Geheimnisse mit langer Geschichte – das Arztgeheimnis, das Beichtgeheimnis sowie das Adoptionsgeheimnis – hat gezeigt, dass diese nicht isoliert auf den (vermeintlichen) Schutz des Individuums und seiner Beziehung gegenüber dem Informationsempfänger gerichtet sind. Vielmehr verfolgen die *Geheimnisse eine spezifische Funktion mit Blick auf den Kontext*, in welchen die entsprechenden Informationsflüsse resp. deren Blockaden eingebettet sind.[56] So dient das Arztgeheimnis namentlich ebenso der Funktionstüchtigkeit des Gesundheitssektors selbst. Sein Ziel, Gesundheit und Heilung zu gewährleisten, würde durch die fehlende ärztliche Schweigepflicht unterminiert. Geheimhaltungspflichten strukturieren und schützen – weit über das Individuum und konkrete (Rechts-)Beziehungen hinaus – gesellschaftsrelevante Kontexte, Systeme und Institutionen.[57] 65

Gleichzeitig wurde anhand eines Blicks auf Geheimhaltungspflichten gezeigt, inwiefern solche *nicht per se angemessen oder unangemessen* sind. Vielmehr sind sie – in den Worten von Nissenbaum – ein sog. Transmissionsprinzip, also ein Steuerungsinstrument zur Gestaltung von Informationsflüssen. Ihre Angemessenheit, ihr Einsatz und ihre Gestaltung *en détail* lassen sich einzig anhand einer Reflexion der dahinterstehenden gesellschaftlichen Bereiche und der ebenda verfolgten Ziele und Schutzerwartungen beurteilen.[58] 66

Die mit dieser Rückblende freigelegte *dynamische sowie kontextuelle Dimension*, die sich in den traditionsreichen Geheimworten und Geheimhaltungspflichten unübersehbar abbildet, setzt früh einen Kontrapunkt zu einer Perzeption, wonach eine Information, auch eine Personenangabe, quasi naturgegeben oder per se als «geheim» zu gelten hat. Vielmehr erlangt sie diese Qualifizierung aufgrund des Verarbeitungszusammenhanges. Damit wird zugleich sichtbar, wie *Geheimhaltungspflichten* keineswegs isoliert auf den Schutz einer konkreten Person oder einer konkreten Beziehung abzielen, sondern dazu dienen, verschiedene soziale Bereiche und Institutionen zu konsolidieren und die ebenda verfolgten Zwecke wirksam werden zu lassen.[59] 67

56 Als Pflicht zur Informationsverweigerung auch unter Bezug auf Informationsansprüche wird das Geheimnis von Hauser, 34 ff. beschrieben.

57 Richtungsweisend Nissenbaum, *passim*.

58 Dies., 129 ff.; etwas allgemeiner und früh zu verschiedenen rechtlichen Gestaltungsmöglichkeiten von Informationsflüssen resp. Kanälen Dreier, in: Bizer/Lutterbeck/Riess (Hrsg.), 65 ff., 71 ff.; zu den Elementen einer Verfassung des Informationsflusses im Internet vgl. Karavas, Digitale Grundrechte, 13 ff.

59 Zu diesem kontextuellen Ansatz Nissenbaum, *passim*; vgl. die Thematisierung von Zusammenhängen zwischen Berufsgeheimnissen, dem Schutz von Gütern der Allgemeinheit Druey, 379 ff.

B. Resümee und Überleitung

68 Im Sinne eines *Resümees* kann festgehalten werden: Geheimnisse, Geheim- resp. Passworte und Geheimhaltungspflichten können, wo sie sich auf Angaben über Personen beziehen, zugleich als Vorläufer sowie als Kernelemente des zeitgenössischen Datenschutzrechts bezeichnet werden. In den reflektierten Märchen mit ihren bizarren Geheimworten «Sesam, öffne Dich!» resp. «Rumpelstilzchen» steht zwar ganz das Wort im Vordergrund, was zu einer isolierten und statischen Sichtweise verleitet, in welcher Informationen gewissermassen per se und bezugslos als geheim erscheinen. Eine solche quasi-naturgegebene Einteilung zwischen «geheim» resp. «privat» und «öffentlich», die in den Märchen mit markanten räumlichen Metaphern – dem Berg und seinem Inneren, dem Haus und seinem Innenbereich resp. seinem Aussenbereich – symbolisiert wird, prägt die Konzeptionierung des Datenschutzrechts bis heute. Zugleich allerdings eröffnet eine Auseinandersetzung mit den Märchen die Möglichkeit, eine *dynamische Perspektive* freizulegen*:* Ihr gemäss erscheinen *Geheimhaltungspflichten als Instrumente zur Blockierung von Informationsflüssen*.[60]

69 Präzisiert und bildlich gesprochen geht es in beiden Erzählungen darum, dass *die geheime Information nicht aus einer Welt in eine andere Welt fliessen soll*. Der Informationsfluss soll verhindert resp. ermöglicht werden, um etwas als wertvoll Beurteiltes – einen Goldschatz, die Freiheit resp. ein Kind, ein «Gut» – erhalten resp. behalten zu können. Die damit herausgeschälte *kontextuelle und akzessorische sowie dynamische Dimension von (persönlichen resp. vertraulichen oder geheimen) Informationen* wurde anhand der historisch traditionsreichen Geheimhaltungspflichten des medizinischen, kirchlichen und familiären Bereichs detaillierter herausgearbeitet.

70 Hierbei hat sich gezeigt, dass der Geheimnisträgerin eine Diskretionspflicht auferlegt wird aufgrund der *Rolle*, in der sie dem Informanten (in der Regel dem Informationssubjekt) begegnet. Es sind spezifische (berufliche) Kontexte und Systeme, in denen von den offenbarenden Personen *als Patientin oder Beichtendem* persönliche Informationen zum Informationsempfänger als *Arzt, Geistlichem oder Familienmitglied* usf. fliessen. Mit dieser Perspektive rücken indes die Individuen und eine Vorstellung in den Vordergrund, wonach es eine *Person* – immerhin eine Person in einer spezifischen Rolle – und die sie betreffenden Informationen sind, die es zu schützen gilt. Gleichzeitig grenzen sich die Wissenden – das Informationssubjekt sowie die Eingeweihte – von anderen, nichtwissenden Personen ab: Die nichtwissenden Personen sind aus dieser Beziehung *exkludiert*.

60 Vgl. Druey, BJM 2005, 57 ff., 66; dass eine rechtswissenschaftliche Studie zum Datenschutzrecht im Medizinbereich das Bild der Informationsflüsse prägt, erscheint damit naheliegend; vgl. Brühwiler-Frésey, 154 ff.

Damit erlangt die *Beziehung* zwischen Informationssubjekt und Geheimnisträgerin, in welcher im Binnenverhältnis Informationen fliessen, die nach aussen abgeschirmt werden, ein *exklusives Element*. Es ist eine *Vertrauensbeziehung*.[61] Umgekehrt kann die Vorenthaltung von Informationen ein Beziehungsgefüge belasten. Die *Gestaltung von Informationsflüssen ist ein zentrales Element der Beziehungsgestaltung*.

71 Der Dienst von Geheimhaltungspflichten erschöpft sich allerdings nicht im Schutz der Person und der Vertraulichkeit der Beziehung. Vielmehr erfüllen Geheimhaltungspflichten eine *systemische Schutzfunktion*: Sie dienen der Konsolidierung sowie dem Schutz der Funktionstüchtigkeit des jeweiligen Kontextes, dem die Erfüllung spezifischer Ziele und Aufgaben zugewiesen wird.[62]

72 Die *nunmehr folgenden Ausführungen* richten die Aufmerksamkeit – wiederum aus einer historischen Perspektive – auf die systematisierten und systematisierenden Informationserfassungen, namentlich Personenerfassungen, sowie auf die Herausbildung entsprechender Infrastrukturen. Der Versuch, durch die Sammlung von Wissen und Informationen *Ordnung in eine unordentliche Welt* zu bringen, hat eine lange Tradition.[63]

73 So wurden in Jurisprudenz, Philosophie und Medizin zwischen dem Hochmittelalter und dem 16. Jahrhundert Menschen kategorisiert, bezeichnet und beschrieben, beispielsweise im Rahmen der Physiognomie.[64] Aus dem Bagdad des 10. Jahrhunderts stammt das «ktab al fihrist», das Buch der Kataloge, in welchem bisher verstreutes Wissen zusammengetragen wurde. Diesem ähnlich ist das enzyklopädische «speculum maius» aus dem Europa des 13. Jahrhunderts. In seinem grossen Werk «De inventione rerum» listete der aus Italien stammende Humanist Vergilio auf, welche Erfindungen erstmals durch wen gemacht wurden.[65] Umfangreiche Informationssysteme mit Listen und Tabellen erstellten später Athanasius Kircher und Gottfried Wilhelm Leibniz, wobei Letzterer auch als Bibliothekar tätig war.[66]

74 Um gewonnene Erkenntnisse zusammenzutragen und so zentral auffindbar zu machen, dienten später Lexika. Im 21. Jahrhundert erfolgt indes das «Aus» des

61 Zu den Themen Vertrauensperson, Vertrauen und Information Luhmann, Vertrauen, 27 ff. und 38 ff.; zur Bedeutung des Vertrauens und des Berufsgeheimnisses in der Beziehung zwischen Anwältin und Mandant sowie allgemeiner im anwaltlichen Bereich Fellmann, N 456 ff.; zur Struktur des Rechts des Geheimseins Druey, 251 ff. und zu den Berufsgeheimnissen 317 ff., ohne allerdings den Fokus auf den relationalen Aspekt zu richten.

62 Dazu richtungsweisend Nissenbaum, 127 ff.; vgl. spezifisch für das Anwaltsgeheimnis Fellmann, N 456 ff., insb. N 458 f.; rechtsvergleichend zum Anwaltsprivileg Magnus, 1 ff.; zu den Berufsgeheimnissen, die den Diensten der jeweiligen Berufe dienen, Druey, 379.

63 Vgl. dazu Groebner, 10.

64 Zur Physiognomie als Element der Kriminalistik Vec, 4 ff.; Groebner, 33.

65 Groebner, 105.

66 Krajewski, 194.

Brockhaus, dessen Anfänge auf 1796 zurückgehen. Ursächlich für dieses Ende ist die Digitalisierung, wobei heute Algorithmen und künstliche Intelligenz ganz ähnliche Funktionen erfüllen. So bietet Starmind, ein Schweizer Unternehmen, ein Tool zur Generierung kollektiver Intelligenz in Organisationen an.[67] Es ermöglicht den Mitarbeitenden ihre Fragen einzutippen, wobei diese in der Folge an die potentiell zur Beantwortung kompetenten Personen weitergeleitet werden. Die auf diesem Weg gesammelten Informationen werden katalogisiert und stetig angereichert, womit eine Art kollektiver Intelligenz generiert wird. Im Ergebnis entsteht nichts anderes als ein riesiges Nachschlagewerk. Zirkulierten früher Bibliotheksdiener, um in den Bibliotheken mit ihren Katalogen und Schriften Antworten zu finden, wird heute über das Netz gesucht und gefunden.[68]

75 Nicht nur aus einer historischen Perspektive sind die Kontrolle über und die Ordnung *von Informationen für hoheitliches, obrigkeitliches Handeln von höchster Bedeutung*. Hierbei liefert das alte Instrument der *Volkszählung* ein Verbindungsglied zur hochaktuellen Thematik des Datenschutzes. Die Volkszählung ist das Verfahren schlechthin, wenn auch nicht das einzige, welches die Bedeutung der informationellen Erfassung von Personen durch hoheitliche Institutionen dokumentiert. Die Relevanz informationeller Erfassungen für die Etablierung von Macht konnte bereits im Rahmen der Betrachtung des Märchens von Ali Baba herausgeschält werden: Der Räuberhauptmann ist Herr des Geheimnisses, wobei seine informationellen Versäumnisse ihn am Ende nicht nur seine Macht, sondern auch sein Leben kosten. In diesem Geiste ist auch der nachfolgende Titel gesetzt.

67 Vgl. Starmind, Zürich 2020, <https://www.starmind.com> (zuletzt besucht am 30. April 2021); zum Einsatz von neuen Technologien wie künstlicher Intelligenz, Machine Learning, Block Chain usf. durch Unternehmen und die Herausforderungen, die hieraus für die Compliance resultieren, vgl. Bartuschka, CB 2019, 340 ff.; zur Frage, ob es ein Grundrecht auf Schutz vor künstlicher Intelligenz braucht, Pfeil, InTeR 2020, 82 ff.

68 Krajewski, 21, 186, 259, 348, 593.

II. Kapitel: Informationsverarbeitung als Herrschaftstechnologie

A. Etablierung informationeller Ordnungen

Die *Praxis der Volkszählung* ist für die datenschutzrechtliche Entwicklung richtungsweisend.[69] Juristisch hat an erster Stelle das Deutsche Bundesverfassungsgericht in der zweiten Hälfte des 20. Jahrhunderts mit seinem Mikrozensusurteil vom 16. März 1957 und dem berühmten Volkszählungsurteil vom 15. Dezember 1983 mit dem hier anerkannten *Recht auf informationelle Selbstbestimmung* die Entwicklung des Datenschutzrechts geprägt.[70] Buchner bezeichnet im 21. Jahrhundert das Volkszählungsurteil des Bundesverfassungsgerichts als «Magna Carta des Datenschutzrechts», die eine Zäsur in der bislang lustlos geführten Auseinandersetzung um das Datenschutzrecht markierte.[71] Das Bundesverfassungsgericht formulierte in seinem Urteil einen umfassenden Katalog von Rechten und Pflichten sowie konkreten Vorgaben zur Formatierung der hoheitlichen Machtposition, die (potentiell) über das Instrument der Volkszählung generiert wird. 76

69 Vgl. mit Blick auf die USA auch aus einer historischen Perspektive Solove, Stan. L. Rev. 2001, 1400 ff.; zum «Drama» der Volkszählung Bernard, 155 ff.; zur Geschichte der eidgenössischen Volkszählung Busset, in: Bundesamt für Statistik (Hrsg.), 9 ff. (Vorwort durch Jost) und 15 ff., zum Widerstand gegenüber dem Instrument, 80 ff. und zum Datenschutz 86 ff.; Schaar, 99 ff.; Bull, Computer, 308 ff.

70 BVerfGE 27, 1 – Mikrozensus, Urteil vom 16. Juni 1969; BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983; zum Recht auf informationelle Selbstbestimmung vertiefend Bull, Vision, 22 ff.; vgl. auch Ehmann, Juristische Schulung, Zeitschrift für Studium und praktische Ausbildung 1997, 193 ff., 196 f. sowohl zum Schutzbereich der Selbstbestimmung, zur Sphärentheorie und zur Entwicklung der informationellen Selbstbestimmung; zum Recht auf informationelle Selbstbestimmung insb. Hufen, JZ 1984, 1072 ff.; m. w. H. Buchner, 30 ff.; zur Beschreibung als «Dekodifikation» vgl. von Lewinski, in: Kloepfer (Hrsg.), 107 ff., 117; Aulehner, CR 1993, 446 ff.; Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 27 ff.; Ders., NJW 1984, 394 ff.; Garstka, in: Schulzki-Haddouti (Hrsg.), 48 ff.; Ders., in: Götting/Schertz/Seitz (Hrsg.), 392 ff.; zu diesem Urteil auch Bull, in: Hohmann (Hrsg.), 173 ff., der auf die Ambivalenz hinweist, die das Urteil auslöste; Hoffmann-Riem, AöR 1998, 513 ff., insb. 519 ff.; Langer, *passim*; Geiger, NVwZ 1979, 35 ff.; Vogelsang, *passim*; Maisch, 34 ff.; Placzek, *passim*; im Kontext von Zugangskontrollen zu Spielstätten Ronellenfitsch/Denfeld, *passim*; zur Ökonomisierung informationeller Selbstbestimmung Specht 11 ff.; Specht/Rohmer, PinG 2016, 127 ff.; für die Schweiz im Zusammenspiel mit dem Medienrecht resp. der Medienfreiheit Glaus, *passim*; Rudin, digma 2008, 6 ff. zur Anonymität als Element informationeller Selbstbestimmung; Ders., in: Schweizer/Burkert/Gasser (Hrsg.), 907 ff.; für die Schweiz mit Blick auf das Schengener Informationssystem Stämpfli, *passim*; für die Schweiz grundlegend Waldmeier, *passim*; richtungsweisend, was die Klärung der Schweizer Rechtslage anbelangt, insb. Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), 19 ff. und Gächter/Egli, Jusletter vom 6. September 2010.

71 Buchner, 30; dazu, dass das Urteil zum epochalen Meilenstein gemacht wurde, der kritische Stimmen unter sich begrub, Bull, Computer, 45; zum Urteil auch Schaar, 101 ff.; Donos, 69 ff. mit Übersicht über die Kommentarliteratur und Beschreibung zweier Lager, der Befürworter und der Kritiker, die eine reduktionistische Interpretation fordern; dazu, dass dem Volkszählungsurteil des Bundesverfassungsgerichts bis heute richtungsweisende Impulse entnommen werden, wobei in dieser Arbeit insb. anhand der Erwägungen zur Zweckbindung der kontextuelle Bezugsrahmen des Datenschutzrechts herausgearbeitet wird, vgl. zweiter Teil, V. Kapitel, B.4.

77 Seit jeher geht die Praxis der Volkszählung mit der für hoheitlich resp. obrigkeitliche Personendatenerhebungen typischen *Ambivalenz* einher: Exemplarisch erscheint die im Alten Testament wiedergegebene Volkszählung Davids – anders als der weihnachtsgeschichtliche Zensus – als sündhaft und Teufelswerk.[72]

78 Die informationelle Erfassung von Menschen mittels Volkszählungen hat eine lange Tradition und institutionelle Bedeutung. Sie beschränkt(e) sich selten auf die Registrierung der Existenz von «Bürgerinnen und Bürgern». Vielmehr wurden mit ihr in aller Regel diverse Einzelangaben zu Personen erhoben. Bekannt sind hierbei sowohl diejenigen Zählungen, in denen Volkszähler («Staatsdiener») die zu erfassenden Personen aufsuchten, als auch jene, in denen sich die zu zählenden Personen in einer «Amtsstube» einzufinden hatten. Die Praxis der Volkszählung ist aus dem alten Ägypten sowie der römischen und griechischen Antike übermittelt.[73]

79 Volkszählungen erfolgten nicht *l'art pour l'art*. Vielmehr sollten mit den so generierten Informationen *konkrete Verwaltungsmassnahmen* durchsetzbar werden: Sie dienten der Steuereintreibung und Heeresrekrutierung, wobei es sich bei den im Alten Testament wiedergegebenen Volkszählungen meist um militärische Musterungen handelte. Zudem wurden sie zwecks Rekrutierung von Fremden zwecks Tempelbaus oder zur Eintreibung von Geldern genutzt.[74] Insofern zeigt sich erneut die *akzessorische Dimension* der informationellen Praxis.[75]

80 Auch für das *Mittelalter* sind Bevölkerungszählungen dokumentiert, beispielsweise durch die Städte nördlich der Alpen. Sie stehen im Zusammenhang mit kriegerischen Konflikten, beschränkten sich allerdings keineswegs auf die Erfassung wehrpflichtiger Männer. Vielmehr wollte man sämtliche in der Stadt wohnenden Personen registrieren. Sukzessive wurden spezielle Register eingerichtet und der Zugriff auf Fremde, Steuerzahler, Bettler, Kranke, Soldaten oder Verbrecher intensiviert.[76] 1576 sah Jean Bodin in der Volkszählung das administrative Mittel, Parasiten loszuwerden, die als Bettler und gefährliche Müssiggänger das Gemeinwesen belasteten: Würden alle königlichen Untertanen mit Name, Stand und Wohnort erfasst, könnten die Wölfe unter den Schafen entlarvt werden.[77] In der Habsburger Monarchie wurden Bevölkerungserfassungen nach diversen

72 2 Sam 24 und 1 Chr 21; vgl. zu den Musterungen und Volkszählungen in der Bibel: <https://www.bibelwissenschaft.de/wibilex/das-bibellexikon/lexikon/sachwort/anzeigen/details/volkszaehlung-zensus-at/ch/247544d04b778610b4faab76e15317ea/> (zuletzt besucht am 30. April 2021).

73 Vgl. insofern auch Mayer-Schönberger/Cukier, 20 f.

74 Hierzu Hieke, Volkszählung, abrufbar unter: <https://www.bibelwissenschaft.de/wibilex/das-bibellexikon/lexikon/sachwort/anzeigen/details/volkszaehlung-zensus-at/ch/247544d04b778610b4faab76e15317ea/> (zuletzt besucht am 30. Juni 2021).

75 Vgl. zu dieser in dieser Arbeit vorgeschlagenen Begriffsdimension erster Teil, I. Kapitel, A.

76 Groebner, 57.

77 Vgl. den Hinweis bei Ders., 144; zur Erfassung und Vertreibung von Beschäftigungslosen im 16. Jahrhundert auch Herwig/Tantner, 24.

Kategorien vorgenommen.[78] Und in Wien sollte per Dekret von 1645 die gesamte Bevölkerung für militärische Zwecke erfasst werden.[79]

Eine neue Dimension der Datenverarbeitung in diesem Kontext wird mit dem Jahr 1890 erreicht, als die von Hermann Hollerith entwickelte Lochkartenmaschine für die elfte Volkszählung in den USA eingesetzt wurde.[80] Aufgrund ihrer Effizienz fanden Holleriths Lochkarten bald auch in Europa Verwendung. 81

Die Volkszählung im Sinne einer detaillierten Erfassung der in einem («Staats-») Gebiet lebenden Bürgerinnen und Bürger in ihren persönlichen Verhältnissen wird als bedeutsames *Instrument zur Konstituierung von Staaten sowie ihrer Herrschaft* beschrieben.[81] Entsprechend zeigen sich Personendatenerhebungen auch in diesem Zusammenhang als *Herrschaftsinstrument*.[82] 82

Den Konnex zwischen allgemeiner Volkszählung und Durchführung anderer Verwaltungsvollzugsmassnahmen, gestützt auf die durch die Volkszählung generierten Personenangaben, wird später, im 20. Jahrhundert, das Bundesverfassungsgericht als datenschutzrechtliches Kernproblem thematisieren und daraus Vorgaben für das Datenschutzrecht ableiten.[83] 83

Zahlreiche Institutionen und Bereiche bedienten sich weiter zur Personenerfassung diverser (schwarzer) *Listen und Register*. Insofern ist vorab auf diejenigen aus dem *religiösen und kirchlichen Kontext* hinzuweisen. 84

Eine weit über das weltliche Dasein hinausreichende Idee mit schicksalhafter Bedeutung ruht in der *ordnenden Hand Gottes*. Sie kommt in der *mittelalterlichen Vorstellung vom Buch des Lebens* zum Ausdruck: Hier werden die Namen der Erlösten aufgelistet, wohingegen das Buch der Verdammten Gegenstand der 85

78 Zum Ganzen Tantner, Ordnung der Häuser, 199 ff.

79 Ders., a. a. O., 17 f.

80 Vgl. zum Zensus in der US-amerikanischen Geschichte Regan, 46 ff.; Heise online, Zahlen, bitte! Die Lochkarte mit 80 Zeichen wegweisend in die EDV, Hannover 2019, <https://www.heise.de/newsticker/meldung/Zahlen-bitte-Die-Lochkarte-Mit-80-Zeichen-wegweisend-in-die-EDV-4274778.html> (zuletzt besucht am 15. April 2021); Redaktion Damals, Lochkarten für die Volkszählung, Stuttgart 2019, <https://www.wissenschaft.de/zeitpunkte/8-januar-lochkarten-fuer-die-volkszaehlung/> (zuletzt besucht am 30. April 2021).

81 Von Lewinski, Interview vom Oktober 2010, <https://www.datenschutzzentrum.de/artikel/938-Interview-mit-PD.-Dr.-Kai-von-Lewinski.html> (zuletzt besucht am 30. April 2021).

82 Vgl. in anderem Zusammenhang Krajewski, 140, 178 f.; von Lewinski, in: Arndt/Augsberg (Hrsg.), 201 f.; vgl. Westin, in: Schoeman (ed.), 56 ff., 70; zum Zensus mit dem Hinweis, wonach Validität Macht heisst, Porter, 33 ff., 41 ff.; zu Metaphern für das Verhältnis von privacy und Macht Solove, Stan. L. Rev. 2001, 1393 ff.; zu den historischen Wurzeln der Kontrollgesellschaft und dem Interesse herrschender Instanzen an den «Personendaten» der Untertanen Herwig/Tantner, 11 ff.; Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 28, bezeichnet die Informationsverarbeitung als zentrales staatliches Machtinstrument.

83 Vertiefend hierzu BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983.

Inquisitionslisten war.[84] Die Menschheit wurde damit der *Dualität* anheimgestellt und in zwei Kategorien eingeteilt: die Erlösten und die Verdammten, das Himmelsreich und das Reich Gottes einerseits, die Hölle und das Reich des Teufels andererseits.

86 Damit gelangt man zu den *Ketzerlisten* der *Inquisition*, wie man sie aus der zweiten Hälfte des 13. Jahrhunderts kennt: Die Inquisition beanspruchte für sich die Kompetenz, das Gegenstück zum Buch des Lebens zu verfassen: ein Buch, welches die Verdammten auf Erden fichiert. Vielbedeutend, demonstrativ und manipulativ-erpresserisch wurde während der Verhöre in diesem Buch geblättert: Den Verdächtigen oder schlicht Missliebigen wurde damit – als Einschüchterungs- und Druckmittel – suggeriert, dass gegen sie bereits umfangreiche, unheilvolle Aufzeichnungen vorlägen.[85] Entsprechend wird auf die etymologische Nähe des Begriffs der *Inquisition* zum Begriff der *Information* hingewiesen. Als «informatio» wurde der Bericht der untergeordneten Untersuchungsbeamten an den vorgesetzten Richter bezeichnet.[86]

87 *Religiösen Ursprungs* waren die wohl ältesten *Namenslisten*. So sollte die 1215 im vierten Lateralkonzil verankerte Beichtpflicht durch Verzeichnisse in den Pfarreien kontrolliert werden. Aufgrund solcher Beichtverzeichnisse wurden ab dem 13. Jahrhundert Beichtbescheinigungen ausgestellt: Nur jene, die eine solche vorlegen konnten, durften die Kommunion empfangen.[87] In den kirchlichen Aufschreibesystemen des 15. und 16. Jahrhunderts finden sich weiter Tauf-, Trauungs- und Sterbeverzeichnisse.[88] Zieht man das weiter oben beleuchtete Beichtgeheimnis mit in Betracht, zeigt sich, dass sich gerade auch die *Kirche als Institution* resp. der religiöse Kontext umfassender informationeller Instrumente bediente, um *institutionelle Ziele und Zwecke* umzusetzen.

88 Im *juristischen Bereich* sind Listen aus der Zeit um 1250 bekannt. Sie führten die Verbrecher und Geächteten auf und sollten das Rechtsprechungs- und -durchsetzungsmonopol des Gerichts dokumentieren.[89] In Namenslisten waren ab dem 13. resp. 14. Jahrhundert auch *Soldaten* verzeichnet. In der Schweiz ist aus der Stadt Bern ein Dokument von 1468 überliefert, welches die aufgebotenen

84 Vgl. dazu Groebner, 52, 175; zu der menschlichen Vorstellung, selbst wenn sie alleine sind, von Göttern oder Geistern beobachtet zu werden, vgl. Westin, in: Schoeman (ed.), 56 ff., 67; zur Persistenz des Bösen (als Gegenbegriff zum Guten resp. Erlösten) in den göttlichen Ordnungen religiöser Systeme vgl. Herzfeld, 5 ff.

85 Groebner, 52.

86 Zum Ganzen Ders., 140 f.; zur Etymologie und Bedeutung des Wortes «Information» auch Hauser, 23 ff., wobei der Autor bei der Definition auf die Relevanz der Rollen des Informators, des Informanden, der Informationsquelle usf. hinweist.

87 Groebner, 51.

88 Ders., 43 f.

89 Ders., 52; zu den Identifikationsmethoden in der Kriminalistik zwischen 1879 und 1933 vgl. Vec, 5 ff.

Soldaten auflistet. Einem Luzerner Rödel von 1476 lässt sich entnehmen, dass der grösste Teil der registrierten *Soldaten* nicht aus Luzern, sondern vielmehr aus Süddeutschland eingezogen wurde.[90] Besondere Kennzeichen wie Narben (im Übrigen beschrieb man Personen anhand von Grösse, Geschlecht, Haarfarbe und Bekleidung) finden sich als identifizierende Merkmale in einer Söldnerliste datierend auf das Jahr 1446.[91] Anhand besonderer Kennzeichen wurden auch *Räuber* beschrieben. Die Fahndung nach ihnen erfolgte zunächst mittels Steckschreiben, später mittels enzyklopädierter *Gaunerlisten*, die man zirkulieren liess.[92] Die ersten dieser Gaunerlisten, die als offizielle Dokumente verbreitet wurden und detaillierte Personenbeschreibungen der Gesuchten enthielten, werden Schaffhausen 1692 und Zürich 1698 zugeordnet.[93]

89 Auf einer Liste chiffriert und registriert zu sein, musste allerdings keineswegs stets etwas Negatives wie Abgaben, Militäreinzug, Strafverfolgung bedeuten. Mittels Listen und Registern wurden gleichermassen *Privilegien* ausgewiesen. In entsprechenden Dokumenten kündigte sich somit im Europa des 16. Jahrhunderts auch ein Bewusstsein für *soziale Verantwortlichkeiten* an: Bekannt sind amtliche Register, in denen bestimmte Bettler und Arme als *Almosenberechtigte* aufgeführt wurden.[94]

90 Umgekehrt wurden auch *Spender* aufgelistet. Zwar wurden solche Listen damit begründet, dass mit ihnen die Ausgaben planbar würden. Allerdings ging es zugleich um die Überprüfung der Liebe der Untertanen zu Gott, den Mitmenschen und die öffentliche Ordnung.[95]

91 Die Bettlerinnen und Bettler, die als Almosenberechtigte erfasst waren, konnten sich von nun an durch entsprechende *Bettlerausweise* legitimieren. Dagegen waren Bettlerinnen und Bettler in der Stadt Nürnberg gemäss der Almosenordnung aus dem Jahr 1370 noch verpflichtet, *obrigkeitliche Zeichen* an den Kleidern zu tragen, wobei die einheimischen Armen andere Markierungen als die auswärtigen zu tragen hatten. Bettlerabzeichen kannte man auch in Paris, England und Holland bereits im 14. Jahrhundert.[96] Mit ihnen sollte zugleich die Beaufsichtigung und Disziplinierung von Armen und Bettlern durch städtische wie kirchliche Beamte effektuiert werden.

92 Die schriftlichen Informations- und Personenerfassungen intensivierten und verdichteten sich sukzessive. Gegen Ende des 15. Jahrhunderts hatten sich umfas-

90 Groebner, 125.
91 Ders., 81.
92 Vgl. auch Blauert/Wiebel, 12 ff.
93 Groebner, 163.
94 Ders., 128 ff.
95 Wagner, in: Schmidt/Aspelmeier (Hrsg.), 21 ff., 48.
96 Groebner, 38.

sende *Registrierungssysteme* installiert.[97] Durch die schriftliche Erfassung von (Personen-)Gruppen – Söldner, Pilger und (Aus-)Reisende, Almosenberechtigte, Steuerpflichtige, Deserteure, Kranke und Kriminelle – wollte man *Hoheitsfunktionen durchsetzen und damit auch Ordnung sowie Herrschaft herstellen*.[98]

93 Mit der sukzessiv intensivierten schriftlichen Registrierung sollte – nebst der sichtbaren materiellen Welt – eine zweite, für Normalsterbliche unsichtbar bleibende Welt erschaffen werden, die nur in den Akten existierte. Insofern führten die zentralisierten bürokratischen Systeme unter Philipp II. von Spanien zu einem (ersten) Höhepunkt, der namentlich der informationellen Erfassung aller Auswanderer in die neue Welt, aber auch von Zigeunern gemäss der Reichspolizeiordnung von 1551 besondere Aufmerksamkeit angedeihen liess.[99] Seine Ambitionen, lückenlose bürokratische Registrierungssysteme zu installieren, verliehen Philipp II. den Titel «Papierkönig».[100] Einem informationellen Paralleluniversum allerdings drohte stets die Gefahr, zur Scheinwelt zu verkommen und den Bezug zur Realität zu verlieren.[101]

94 Ein weiterer Höhepunkt für die Machtkonstruktion auch durch umfassende Informationsverarbeitung wird im Zuge der Etablierung absolutistischer Herrschaftsformen angesiedelt. Als exemplarisch gilt die Passpolitik des *Ancien Régime*, die mit ihrer Möglichkeit, die Bewegungen der Untertanen zentraler Kontrolle zu unterwerfen, als beinahe allmächtiges Steuerungsinstrument der absolutistischen Verwaltung beschrieben wird.[102]

95 Nicht nur Bettlerinnen und Bettler wurden im Rahmen ihrer Ein- und Ausreise der Kontrolle unterworfen. Bereits im späten Mittelalter kannte man Instrumente wie Geleitbriefe, laisser-passer-Dokumente oder Gesundheitsbriefe, um Menschen bei ihrer Fortbewegung zu kontrollieren.[103] Anselm Adorno berichtet gar von dreierlei verschiedenen Geleitbriefen, die er auf seiner Reise von Köln nach Aachen vorzuweisen hatte.[104] Besagte Dokumente wurden gegen *Entgelt* erworben, womit der grösste Kreis an Personen von entsprechenden Ortsveränderungen von vornherein ausgeschlossen war.

96 Der zweiten Hälfte des 16. Jahrhunderts und den fürstlichen Kanzleien entstammen die ersten *zusammenhängenden Serien von Reisedokumenten*. Die Überprüfung von Reisenden, Einreisenden und Ausreisenden mittels Listen, Registern

97 Vgl. von Lewinski, in: Arndt/Augsberg (Hrsg.), 196 ff., 201.
98 Groebner, 10 und 57 ff.
99 Ders., 138.
100 Ders., a. a. O.; vgl. zu einer Herrschaftsutopie qua totaler Kontrolle über den Bevölkerungsstand im Paris des 18. Jahrhunderts Herwig/Tantner, 26 f.
101 Groebner, 138.
102 Ders., 161.
103 Ders., 10 und 124 ff.
104 Ders., 127.

und Dokumenten war ein Element der *administrativen Kontrolle*. Nicht nur Menschen, auch Informationen wurden zusehends *mobil*.

97 Entsprechend baute sich *peu à peu* eine Infrastruktur auf, in welcher die Angaben und Dokumente gemeinsam mit ihren Trägerinnen zirkulierten; jeweils an Knotenpunkten wurden von Kontrollinstanzen Prüfungen vorgenommen.[105]

98 Mit dieser Beschreibung wird erneut die *dynamische Dimension informationeller Prozesse* vor Augen geführt. Nunmehr rücken insb. *institutionalisierte und netzwerkartige Infrastrukturen mit stationären Knotenpunkten der Kontrolle* in das Blickfeld.[106] Eine Betrachtungs- und Konzeptionierungsweise, die sich – wie im Zuge dieser Schrift wiederholt gezeigt werden wird – *im zeitgenössischen datenschutzgesetzlichen Regime erst ansatzweise den Weg bahnt.*[107]

99 Im Zusammenhang mit der Bedeutung von Personenerfassungen für die Etablierung und Konsolidierung obrigkeitlicher Macht sei sodann spezifisch auf die gut dokumentierten *Städteordnungen Europas aus dem 18. Jahrhundert* eingegangen: Die Praktik der städtischen Häusernummerierung des 18. Jahrhunderts ist für diese Studie von besonderem Interesse, zumal in deren Zentrum erneut das *Haus resp. dessen Inneres bzw. Äusseres* steht. Auf die Symbolkraft der inneren Räume im informationellen Kontext wies diese Arbeit erstmals im Rahmen der Auseinandersetzung mit den Märchen Ali Baba und Rumpelstilzchen hin.[108] Das Innere des Hauses bildet, wie im Kapitel über das Private im Privaten gezeigt werden wird, eine bedeutsame Metapher für die Entwicklung des rechtlichen Privatheitsschutzes durch Warren/Brandeis, auf deren Aufsatz «The Right to Privacy» bis heute in vielen nicht nur datenschutzrechtlichen Arbeiten referiert wird.[109] Das Hausinnere, das Innerhäusliche repräsentiert und symbolisiert den geschützten Raum und das, was intuitiv mit dem Begriff des Privaten assoziiert wird. Es bildet damit die (Gegen-)Welt jenseits des Öffentlichen.[110]

105 Zu der in dieser Arbeit vorgeschlagenen Begrifflichkeit der «dynamischen Dimension» vgl. erster Teil, I. Kapitel, A. und B.

106 Groebner, 124 ff.; später insofern im Lichte der Digitalisierung Tinnefeld/Buchner/Petri, 18 ff.

107 Vgl. Art. 1 DSG und Art. 3 lit. a und lit. c DSG mit den Kernkategorien der «Person» als Subjekt und der Personenangabe als «Quasi-Objekt»; mit der Einführung der DSGVO, aber auch in der Totalrevision des DSG bildet sich die dynamische Dimension des Datenschutzrechts stärker ab als in den Erlassen des 20. Jahrhunderts.

108 Vgl. erster Teil, I. Kapitel, A.

109 Vgl. z. B. European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, Luxemburg 2018, 373; Schaar, 19 f.; Allen, Harv. L. Rev. Forum 2013, 241 ff., 244; Kang/Buchner, Harv. J.L. & Tech. 2004, 229 ff., 234; Samuelson, Stan. L. Rev. 2000, 1125 ff., 1130, 1139, 1150; Epiney/Hofstötter/Meier/Theuerkauf, 6 f.; Flückiger, PJA 2013, 837 ff., 839; hierzu auch Höning, 10; vgl. zum Schutz ideeller Persönlichkeitsrechte durch das Right to Privacy und die Rolle von Warren/Brandeis sowie der Rechtsprechung auch Meyer Caroline B., 79 ff.; Richards, Vand. L. Rev. 2010, 1295 ff.; Lessig, Soc. Res. 2002, 247 ff., 264.

110 Vertiefend hierzu sogleich erster Teil, III. Kapitel, A. und B.1.–3.

100 Mit der Praxis der Häusernummerierung durch die Stadtverwaltungen des 18. Jahrhunderts wurde dem Haus als Rückzugsort eine andere Bedeutung zugewiesen: Die Häusernummerierung machte gewissermassen das Innere nach aussen hin sichtbar.[111] Die Häusernummerierung für die Stadt Genf in den Jahren 1730–1780, die dem Bedürfnis nach Transparenz und Identifikation in den städtischen Gebieten Rechnung tragen sollte, gilt als *Paradebeispiel* für die Politik der Administration.[112] Die Etablierung lokaler Ordnungssysteme mittels Häusernummerierungen sollte keineswegs bloss verhindern, dass Soldaten im unadressierten Häusermeer untertauchen konnten.[113] Vielmehr diente die Häusernummerierung der Wahrnehmung jedweder institutioneller und hoheitlicher Aufgaben wie Strafverfolgung, Schuldeneintreibung usf. Mit ihr sollte der Anonymität der Stadt und damit der Unkontrollierbarkeit ihrer Bewohner und deren Verhalten zumindest partiell ein Riegel vorgeschoben werden. Die *städtische Verwaltung* erlangte ein *Instrument zur Kontrolle der Einwohner und zum Vollzug ihrer Verwaltungskompetenzen*.[114]

101 Mit der Häusernummerierung wurden allerdings nicht nur Mauern markiert, sondern es wurde zugleich auch *Herrschaft demonstriert*. Bereits mit der Nummerierung an sich symbolisierte die Verwaltung hoheitliche Präsenz; zudem konnte sie damit die städtischen Verwaltungsaufgaben aufsetzen. Der Herrschaftsanspruch wurde sodann durch die *Sicherung der Zeichen* markiert: Um Sabotageakte zu verhindern, sah sich die Stadtverwaltung veranlasst, nächtliche Nummernwächter patrouillieren zu lassen.[115] In diesem Zusammenhang ist eine Episode überliefert, wonach eine Frau, die in klandestiner Aktion eine Hausnummer auslöschte, alsdann im Rahmen eines Strafprozesses als Kriminelle einvernommen wurde. Unumwunden gab sie dabei zu, die Nummer ihres Hauses weiss übertüncht zu haben, weil sie sich wie eine Ketzerin in der Inquisition fühle. Argumentativ wurde die Opposition gegen diese Häusernummerierung weiter auf das Privateigentum sowie die Würde der Person gestützt, würde man doch mit der Chiffrierung der Häuser nunmehr zur anonymen Nummer degradiert.[116] Die dramatische Artikulierung des Geschehens durch die Handelnden, der «Delete-Mechanismus», die Referenz auf die Würde des Menschen als ideell ausgerichtetes Schutzgut auf der einen und auf das Privateigentum auf der anderen Seite könnte genauso gut aus der heutigen Zeit stammen.[117]

111 Zu einer solchen Mechanik bereits die Geschichte von Ali Baba, vgl. erster Teil, I. Kapitel, A.
112 Cicchini, Urban Hist. 2012, 614 ff., 616.
113 Vertiefend zur Häusernummerierung insb. Tantner, Ordnung der Häuser, 22 ff.
114 Cicchini, Urban Hist. 2012, 614 ff., 616 f., 621 ff.
115 Ders., a. a. O., 614 ff., 620.
116 Ders., a. a. O.
117 Vgl. insb. zum informationellen Widerstand gegenüber Machtasymmetrien basierend auf Datenerhebungen Brunton/Nissenbaum, First Monday 2011, mit aktuellen Beispielen unter 3.; Dies., in: Hildebrandt/Bries (Hrsg.) mit einem historischen, ggf. legendären Beispiel, wonach in Dänemark

Gegen solche *informationelle Opposition* griff die Stadt mit *drakonischen Sanktionen* in ganzer Machtfülle durch. Damit wurde erneut der Herrschaftsanspruch umgesetzt: Die Obrigkeit war nicht bereit, Störungen der informationellen Prozesse sanktionslos hinzunehmen. Es hatte sich ein System des Regierens über Nummern etabliert.[118] 102

Wie gezeigt sind mit der informationellen Erfassung des Menschen somit untrennbar die *kognitiven Annahmen von Macht*, aber auch deren *Missbrauch* verbunden. Beides löste seit jeher *Angst und Irritation* aus.[119] Einen einschüchternden Effekt zeitigten, wie die Reaktionen der Stadtbewohnenden von Genf dokumentierten, allerdings nicht nur die Praktiken der Personenerfassung an sich. Angsteinflössend wirkten zudem bereits früher *rhetorische und symbolhafte Elemente*, mit denen Macht durch Informationsverarbeitung untermauert wurde. So kursierten mit dem Siegeszug der autorisierten Schriftlichkeit zwischen dem 13. und dem 16. Jahrhundert stets auch Hinweise auf *drohende illegitime Vervielfältigungen*.[120] 103

Paradoxerweise war indes exakt das öffentliche Beklagen von Fälschungen starke *Rhetorik*. Denn die Betonung der Einzigartigkeit und Authentizität von Dokumenten (sowie allfälliger Sanktionierungen von Fälschungen) diente der Verfestigung von Autoritäten und neuer Imaginationen von Ordnung.[121] Zugleich wurde nicht selten suggeriert, eine Instanz habe allerlei problematische Informationen über den «armen Sünder», selbst wenn dem nicht so war. So bediente sich die Inquisition nur dem Schein nach vorhandener Informationen zur Machtdemonstration, indem der Inquisitor vielbedeutend in den Inquisitionsbüchern blätterte. Die als Ketzer vorgeführten Menschen machte man damit glauben, dass umfassende Aufzeichnungen gegen sie vorlägen. Geständnisse oder Informationen wurden somit durch Einschüchterung, Täuschung und Drohung erlangt.[122] Eine wirkungsmächtige Einschüchterungsstrategie im Rahmen von Verhören dürfte sein, eine mutmasslich erdrückende Aktenlage zu suggerieren. 104

Die Praktiken der Erhebung von Informationen über Personen, ihrer Erfassung in Listen und Registern, die dem Vollzug hoheitlicher Aufgaben dienten, sowie 105

sowohl der König als auch die gesamte Bevölkerung den Judenstern trugen, um eine Identifikation und Deportation der jüdischen Bevölkerung zu verhindern, 164 ff., 171; zum Einsatz der Lochkarten im NS-Regime Schaar, 27 und 34 f.; zur Bedeutung des Löschens resp. Vergessens, gerade im Zuge der Digitalisierung, vgl. Mayer-Schönberger, *passim*; vgl. zum Recht auf Löschung, auch als Recht auf Vergessen bezeichnet, Art. 17 DSGVO; vertiefend zum Recht auf Löschung Hunziker, 15 ff.

118 Cicchini, Urban Hist. 2012, 614 ff., 617.

119 Groebner, 175 f.

120 Ders., 131 ff.

121 Ders., 163 f.

122 Ders., 52; es dürfte davon auszugehen sein, dass die entsprechende Manipulationstaktik auch zu anderen Zeiten und von anderen Regimes wie z. B. der Stasi eingesetzt wurde; vgl. insofern auch Tinnefeld/Buchner/Petri, 61 ff.

die Präsenz obrigkeitlicher Zeichen sind auch als *Praktiken und Techniken der Machtkonsolidierung, -demonstration und -erhaltung* zu bezeichnen.[123] Ebendies liess sich gleichermassen anhand der Kontrollinstrumente mit Blick auf *Informationsflüsse* nachzeichnen. Die angesprochene dynamische Perzeption wurde erstmals aufgrund einer Auseinandersetzung mit den Geheimworten sowie Geheimhaltungspflichten vorgestellt. Sie blockieren den Informationsfluss *innerhalb*, namentlich aber *zwischen* verschiedenen sozialen Bereichen. Damit ist es Zeit, das Thema *Medien* auch anhand der *Mediengeschichte* aufzugreifen.[124]

106 Für die Grenzenlosigkeit von Informationsübermittlungen finden sich vorab im *spirituell-religiösen Kontext* eindrückliche Symbolisierungen. Zahlreiche Kulturen kennen Gottheiten, welche die Rolle von Götterboten innehaben, so Hermes, Iris, Algis oder der Donnervogel in der indigenen Mythologie Nordamerikas.[125] Bei Thomas von Aquin sind Engel der «verlängerte Mund Gottes». Engel transportierten die göttlichen Nachrichten zwischen Himmel und Erde.[126] Sie galten als zuverlässige Mittler, die Informationen unverfälscht überbringen – ein einzigartiges Fernmeldesystem zwischen den Welten. Zur Manipulation berufen waren allerdings die Dämonen.[127]

107 Auch im Diesseits kam dem Prozess der Verbreitung von Informationen und parallel dazu dem Schutz von Informationsprozessen Bedeutung zu: Solange effiziente Medien fehlten, floss die Information nicht zum Menschen, sondern der Mensch ging zur Information hin. Zunächst wurden Informationen stationär gesammelt und/oder vor Ort zur Kenntnis genommen, beispielsweise durch die Portraitierung von Verbrechern, Verrätern und Bankrotteuren im 14. Jahrhundert auf den *Mauern* öffentlicher Gebäude.[128]

123 Zusammenfassend darf das Bonmot «Wissen ist Macht» von Bacon zitiert werden, vgl. hierzu auch Mayer-Schönberger, Delete, 118 ff.; vgl. sodann die zahlreichen Beiträge zu Machtfragen in der Informationsgesellschaft in Drossu/van Haaren/Hensche et al. (Hrsg.).

124 Zum «Bild» des Informationsflusses im Zusammenhang mit der Geschichte des Copyrights im Medienwandel, Dommann, 235 f.; die Autorin hält weiter in einem Aufsatz zum Copyright im Zeitalter des Mikrofilmes fest, dass in den Kinderschuhen von Medien stets auch die Kreierung neuer Welten fantasiert wird, Dies., ZfM 2010, 79, auch mit einem Hinweis auf das Internet. Dieser Befund lässt sich ebenso in dem für das Datenschutzrecht prägenden Narrativ «Big Brother is watching you» aus Orwells Werk «1984» erkennen; Druey verwendet das Bild des Informationsflusses in mehreren Beiträgen, vgl. Druey, BJM 2005, 57 ff., 66; Ders., in: Brem/Druey/Kramer/Schwander (Hrsg.), 379 ff., 392; die Regelung von Informationsflüssen als Aufgabe des Informationsrechts wird auch erwähnt von Dreier, in: Bizer/Lutterbeck/Riess (Hrsg.), 65 ff., 71 ff.; das Bild des Informationsflusses verwendet auch Brühwiler-Frésey, 154 ff.

125 Vgl. Wikipedia, Götterbote, Mai 2020, <https://de.wikipedia.org/wiki/Götterbote> (zuletzt besucht am 30. April 2021).

126 Dazu m. w. H. Krajewski, 318 f.

127 Zur Rolle des Dämons im informationellen Kontext Ders., 12, 167, 291 ff., 300, 332, 336 f., 385 f., insb. zum Dämon als Störfaktor der Kommunikation, 417.

128 Groebner, 30 f.; eine Bildgeschichte von Lavater bis Facebook präsentiert jüngst Meyer Roland, 11 ff.

Personenbeschreibungen und Nachrichten wurden vorab *lokal und oral* zugänglich gemacht. Mit dem Siegeszug des *Papiers* im 13. Jahrhundert in den Kanzleien des christlichen Europas zirkulierten Informationen zusehends *schriftlich*, zu Fuss oder auf dem Rücken von Pferden.[129] Entsprechend wurden, sobald es die technischen Möglichkeiten zuliessen, visuelle Repräsentationen (Fahndungsbilder) *gedruckt*, als *Briefe versandt und ausgehängt*.[130] Es ging nicht mehr nur darum, Informationen zu erheben, sondern zugleich auch darum, obrigkeitliche Dokumente *mobil* zu machen sowie den unerwünschten Zugriff auf Informationen zu verhindern.[131] Die umfassenden obrigkeitlichen Bestrebungen, ebenso den *Fluss von Informationen zu kontrollieren*, dokumentieren deutlich den *institutionellen Aspekt* der Thematik des Umgangs mit Informationen: Der Schutzgedanke im Sinne der Kontrolle von Informationsflüssen ist hier nicht auf das Individuum gerichtet, stattdessen auf die Sicherung von Herrschaftssystemen und deren Infrastrukturen: «des stats gehaim».[132] 108

Im 14. Jahrhundert wird in Europa für den *Austausch von Dokumenten und Listen der weltlichen Behörden* ein eigentliches *Boten- und Briefbeförderungssystem* errichtet.[133] Parallel zur Verdichtung der Aufschreibesysteme werden die Nachrichtennetze zwischen den Städten ausgebaut.[134] Bis zur Umstellung des Informationstransfers auf technische Medien, zunächst durch das Telegrafieren, kommen zur Erfüllung dieser Aufgabe *Diener und Boten* zum Einsatz.[135] Rund um die Figuren der Diener, Boten und Spione ranken sich nicht nur unzählige abenteuerliche Geschichten, sondern allem voran ein zusehends ausgeklügeltes informationelles Transport- und Schutzsystem. Die im Einsatz stehenden Briefboten mussten einen Amtseid leisten und wurden Schweige- und Geheimhaltungspflichten unterworfen sowie in Botenbüchern registriert.[136] Namentlich für die Verwaltung, Diplomatie und Politik der deutschen Reichsstädte ab 1380 gewinnt der Einsatz vereidigter Briefboten hohe Relevanz.[137] 109

1464 wird in Frankreich per Dekret das königliche Botenwesen durch Louis XI. neu geordnet und einer strengeren Kontrolle unterworfen. Von nun an mussten sämtliche Briefboten der Grenzstädte ein Ausweispapier bei sich tragen. Die transportierten Dokumente waren von der postmeisterlichen Vertretung zu öffnen, zu sichten und zu verschliessen sowie mit Amtssiegeln zu belegen. Bewegun- 110

129 Vgl. Groebner, 9 und 120; Krajewski, 366 ff.
130 Groebner, 31; zu den Methoden der Identifikation in der Kriminalistik und der Bedeutung von Fahndungsbildern in den Jahren zwischen 1879 und 1933 Vec, 25 ff.
131 Groebner, 9 und 120; Krajewski, 365 ff.
132 Groebner, 53.
133 Ders., 54 f.
134 Ders., 57.
135 Ders, 10; Krajewski, 412 ff.
136 Krajewski, 124.
137 Ders., 120.

gen von Postboten und Dokumenten waren damit einer fast lückenlosen Kontrolle unterworfen, «damit jede Reise jedes einzelnen Briefboten im Nachhinein rekonstruierbar sei».[138]

111 Mit besagten Massnahmen adressierte man die besondere *Vertrauensstellung*, die menschlichen Boten zukam: Indem sie die Verfügungsgewalt über Nachrichten innehatten, kam ihnen zugleich *Souveränität über das Wissen* zu.[139] Das Bild des unberührten Briefes, vom Diener auf dem Silbertablett serviert, trifft denn auch die Wahrheit weit weniger gut als das Bild des Dieners als «Medium in actu».[140] Als Störfaktoren wirkten nicht nur die Boten selbst. Vielmehr wurden diese mit ihren mehr oder minder geheimen Nachrichten, zu Fuss oder zu Pferd unterwegs, nicht selten überfallen. Mit der Geburt des Boten hat auch der Spion seinen Auftritt.[141]

112 Die zahlreichen Widrigkeiten – Langsamkeit, Indiskretion, Manipulierbarkeit, Überfallsgefahr – waren empfindliche Schwachstellen für Machthaber, denen Informationsprozesse (wie beschrieben) als Herrschaftstechnik dienten.[142] Konsequenterweise suchte man nach Mitteln, den Boten zu ersetzen, beispielsweise durch den Rückgriff auf Tiere, namentlich die Brieftaube. Schneller unterwegs konnten sie – unauffällig und weniger anfällig für Überfälle, Aushorchung und Manipulationen – selbst Hindernisse mühelos passieren. Sie spielten bis zur Etablierung technischer Übermittlungssysteme wie dem Telegrafenwesen eine bedeutsame Rolle beim Nachrichtentransport.[143]

113 Neben Boten und Postboten kam ganz allgemein dem *Diener* eine herausragende Rolle zu, wenn es um die Kenntnisnahme, Sammlung und Weiterleitung von Informationen ging. Krajewski hat der Figur seine medienhistorische Habilitationsschrift gewidmet. Er beschreibt unter anderem, wie zwischen den nummerierten Stadthäusern und Regalen Bibliotheksdiener navigierten, die Bücher verteilten und wieder eintrieben, wobei diese mit Zettelkatalogen der Unübersichtlichkeit Herr zu werden versuchten.[144]

114 Anhand unzähliger Konstellationen, Bereiche und Episoden präsentiert der Autor den *Diener als Informationszentrale* und Schaltstelle, der zusammen mit den leer gegessenen Tellern der vornehmen bürgerlichen oder herrschaftlichen Gesell-

138 Krajewski, 124 f.
139 Ders., 159.
140 Zum Ganzen mit zahlreichen Hinweisen Ders., 411 ff.
141 Groebner, 10.
142 Vgl. zu den Störfaktoren Ders., 119 ff.; hierzu auch Krajewski, 159, 411 ff.; Westin, in: Schoeman (ed.), 56 ff., 70.
143 Vgl. Wikipedia, Brieftaube, <https://de.wikipedia.org/wiki/Brieftaube> (zuletzt besucht am 30. April 2021).
144 Der Diener wird hier zur paradigmatischen Figur, die durch ein doppeltes Lokalgedächtnis zwei Adressräume miteinander verschaltet: Er koppelt Bücher- und Häuserordnung und erbringt hierdurch eine eigenständige medientechnische Leistung, Krajewski, 198.

schaften zugleich auch die Informationshappen, die ihm bei seiner Tätigkeit zu Ohren kamen, abservierte.[145] Wenig später wanderten diese vom Salon in die Küche und von der Küche auf den Markt. Auf dem Markt wurden in der Folge nicht nur Gemüse, sondern auch Informationen feilgeboten.[146]

115 Mit den Domestiken und Mägden als medialen Hauptfiguren lässt sich erneut zunächst der *dynamische Aspekt zirkulierender Informationen und Angaben zwischen verschiedenen sozialen Sphären* veranschaulichen. Zudem wird mit ihnen gleichermassen ein Aspekt vor Augen geführt, der die zeitgenössische Debatte um den Datenschutz intensiv beschäftigt: die *ökonomische Dimension* von Informationen und deren Austausch. Der Domestik kannte die Geschäfte seines Herrn bestens und konnte dieses Wissen folglich in ökonomisch oder strategisch wertvolle Informationen umsetzen.[147] Damit war es möglich, vom Domestiken zum Kapitalisten zu werden – durch Nutzung von Insiderwissen und Börsenspekulationen.[148] Für Dritte war es interessant zu wissen, wo sie die aus dem Bedienstetenverhältnis generierten Informationen erlangen konnten. Als Umschlagplätze etablierten sich die Küche, der Gesindetisch, aber auch die Foyers der bürgerlichen Palais, in der Öffentlichkeit der Dorfbrunnen, der Markt, die Barbierstuben («clearing house of information») oder das sog. Dienstmännerinstitut.[149]

116 Mit dieser Schilderung wurde eine neuralgische Stelle der (allzu) menschlichen Diener offensichtlich: Unter Umständen erledigten sie ihre (Haus-)Aufgaben *comme-il-faut*; allerdings riskierten die Herrschaften stets, dass die Bediensteten die gebotene *Diskretion* vermissen liessen und Informationen ausser Haus transportierten. Damit taucht erneut die Metapher des Hauses auf – genauer beim Herrschaftshaus resp. Palast – als Ursprung dessen, was mit dem *Begriff des Privaten assoziiert* wird.[150] Mit der medienhistorischen Analyse des Subalternenverhältnisses zeigte sich zugleich und erneut die Relevanz informationeller Prozesse als *Herrschaftstechnik*.[151] Denn sobald der Subalterne Insider-Informationen hat, kommt ihm durch das Herrschaftswissen eine spezifische Souveränität zu, was ihn vom Dienstverhältnis emanzipiert. Spätestens dann, wenn der Diener mehr weiss als sein Herr, drängt sich die Frage auf, wer wen beherrscht.[152]

117 Erneut folgt aus der Entwicklung neuer Technologien sukzessive die Eliminierung der präsentierten mediengeschichtlichen Figur: Mittels Gerätschaften wie eines

145 Krajewski, 155; Ders., in: Brandstetter/Hübel/Tantner (Hrsg.), 151 ff.
146 Ders., 178 ff.
147 Zum Ganzen Ders., 176 f.
148 Zur sog. Dienstmädchenhausse Ders., 177.
149 Ders., 178 f.; dazu, dass das Private ein bürgerlicher Wert ist, Bartsch, in: Bartsch/Briner (Hrsg.), 31 ff., 31 f.; vgl. auch Simitis, in: Schlemmer (Hrsg.), 67 ff., 71.
150 Vertiefend insofern zum Privaten im Privaten als Privileg auch der Herrschafts- und Oberschicht Bartsch, in: Bartsch/Briner (Hrsg.), 31 ff., 32 f.
151 Vgl. m. w. H. Krajewski, in: Brandstetter/Hübel/Tantner (Hrsg.), 151 ff., 156 ff.
152 Dazu Krajewski, 177.

Lifts, der die leeren Teller in die Küche transportierte, dezimierte man zugleich die Möglichkeiten der Dienerschaft, in die Nähe der Herrschaften zu gelangen und aus deren Tischkonversationen bedeutsame Informationshappen zu gewinnen. Selbst wenn die Dienerschaft durch neue Technologien wie Haushaltsgeräte, aber auch Kommunikationstechnologien ersetzt wurde, haben die Subalternen als Medienfiguren ihre Spuren hinterlassen: Die erste Web-Suchmaschine aus dem Jahr 1996 hiess «Ask Jeeves», wobei ein entsprechender Schriftzug mit der Zeichnung eines Dieners präsentiert wurde – *vom Diener zum Server*.[153] Machte schon der Diener Information zu Geld, so *forciert das Internet die Transformation von Informationen in Güter* weiter.[154]

118 Aufgrund der *informationellen Sonderposition*, die Domestiken wegen ihrer Anstellung innehatten, war die Vermittlung und Anstellung *geeigneter Personen* eine besondere Herausforderung. Selbst unter diesem Aspekt zeigt sich der Wert gewisser Informationen: So wurden bereits im Paris des 14. Jahrhunderts Dienstleistungen von Domestiken gegen Gebühr in Comptoirs vermittelt.[155]

B. Resümee und Ausblick

119 Informationelle Erfassung, Wissen und die Verfügungsgewalt darüber verleihen seit jeher *Autorität* und sind nicht zufällig das *vorrangige Herrschaftsinstrument des Patriarchen und Souveräns*.[156] Informationssysteme zu errichten und zu kontrollieren wird entsprechend als «politische Technologie» resp. als «Technologie der Macht» beschrieben.[157] Herrschaftsansprüche werden im Kontext von Informationen historisch betrachtet in mehrfacher Hinsicht relevant.

120 *Erstens* markiert der *Akt* der *Erhebung und Sammlung* selbst Herrschaft.

121 *Zweitens* ist die Informationserhebung schon früh nicht Selbstzweck, sondern in aller Regel *Instrument zur Erfüllung* eines «obrigkeitlichen» Zwecks. Informa-

153 Hierzu Krajewski, 149 ff.

154 Insofern Vesting, in: Ladeur (Hrsg.), 155 ff., 164; zur Ökonomisierung von Personendaten resp. des Rechts auf informationelle Selbstbestimmung vgl. auch Weichert, in: Bäumler (Hrsg.), 158 ff., 158; die zunehmende Kommerzialisierung von Personendaten wurde bereits in den 1970er Jahren beschrieben, vgl. Mallmann, 23; zur Transformation von Personendaten in Commodity auch Schwartz, Harv. L. Rev. 2004, 2055 ff., 2057; zu Daten als einem Wirtschaftsfaktor auch Schaar, 179 ff.; zum Handel mit der Privatheit resp. der Privatheit als Gut Dörflinger, 49 ff.; zu Rechtsfragen kommerzieller Nutzung von Daten vgl. Hilty, in: Weber/Hilty (Hrsg.), 81 ff.; zu Personendaten als Wirtschaftsgut auch Giesen, JZ 2007, 918 ff.; vertiefend zur expansiven Kraft ökonomischer Rationalitäten dritter Teil, VII. Kapitel, B.2.

155 Vgl. Krajewski, 180; Ders., in: Brandstetter/Hübel/Tantner (Hrsg.), 151 ff.

156 Ders., 155.

157 Cicchini, Urban Hist. 2012, 614, 616; so auch Groebner, 121; indirekt zur dominanten Kognition staatlicher Herrschaftsmacht durch den Staat im Datenschutz Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff.; vgl. im Zusammenhang mit polizeilichen und justiziellen Aktivitäten und der Kriminalistik Vec, 5 f., 86 ff.; vgl. weiter zum Symbolismus von (staatlicher) Herrschaftsgewalt Herzfeld, 10 ff.

tionelle Zwecke werden damit angekoppelt, womit in doppelter Hinsicht Herrschaft ausgeübt wird: Durch die informationelle Erfassung werden die Eintreibung von Steuern, die Rekrutierung von Soldaten, die Kontrolle von ein- und ausreisenden Menschen und Waren usf. realisiert.

Drittens dient die *Steuerung von Informationsflüssen* der *Machtkonsolidierung*, 122
indem Informationen mobilisiert oder umgekehrt abgeschottet werden. Zum Einsatz kamen hierbei verschiedene Kontrollinstrumente: Siegelungen, Stempel, Amtsgeheimnisse, Vereidigung der Boten, sicheres Geleit, Registersysteme der Boten und ihrer Nachrichten sowie andere mehr. Die *dynamische Dimension*, wie sie anhand der Etablierung der Beförderungsinfrastrukturen mit ihren Kontrollen an den Grenzpunkten sowie anhand des Dieners als Medienfigur erneut sichtbar gemacht wurde, konterkariert – wie zu zeigen sein wird – eine Sichtweise, die in den Dualitäten eines statisch gedachten Zweikammersystems von öffentlich versus privat, aber auch von Informationssubjekt versus Informationsobjekt (Information als ökonomisches Gut) verhaftet ist.[158]

Viertens werden gegen Torpedierungen von Informationen und deren Erhebungen *obrigkeitliche Sanktionen* vorgesehen. Entsprechend wird im Zusammenhang mit den informationellen Praktiken der «hoheitliche Zwangsapparat» erfahrbar. Offensichtlich spielen die Informationsverarbeitung und namentlich der Umgang mit Personendaten (um in der zeitgenössischen datenschutzrechtlichen Terminologie zu sprechen) im Rahmen der *Konsolidierung und Erhaltung von Institutionen eine tragende Rolle*. 123

Die vorangehenden Ausführungen blieben zugegebenermassen anekdotenhaft, 124
schlaglichtartig und unvollständig. Schlagworte wie dasjenige der «Verrechtlichung» oder auch das der «werdenden Staatlichkeit», mit denen der grosse Prozess der Entstehung und Durchsetzung schriftlich fixierten Verwaltungshandelns in Europa zwischen dem 13. und 16. Jahrhundert beschrieben werden, haben ihre Defizite und werden von Historikern sowie Historikerinnen durchaus kritisch beurteilt.[159] Dennoch konnte gezeigt werden, dass die informationelle Erfassung, die Kontrolle des Menschen, die Ordnung der Welt sowie informationelle Widerstände keineswegs erst Phänomene unserer Zeit sind.[160] Zugleich wurde nachgezeichnet, inwiefern die Personenerfassung bedeutsam für die Etablierung obrigkeitlicher Herrschaft war.[161] Die Vorstellung einer umfassenden informationellen Personenerfassungen durch den *Staat* hat die datenschutzrechtliche

158 Hierzu vertiefend erster Teil, III. Kapitel; zu den Dichotomien von Privatheit und Öffentlichkeit sowie den Veränderungen resp. Auflösungstendenzen insofern z. B. Schachtner/Duller, ÖZS 2014, Sonderheft, 61 ff.; hierzu auch Schaar, 15 ff.
159 Groebner, 121 f.
160 Ders., 173 f., insbes. 175.
161 Vgl. Lewinsky, in: Arndt/Augsberg (Hrsg.), 196 ff., 201 ff.

Debatte im 20. und 21. Jahrhundert unter den Stichworten «Grosser Lauschangriff» und «big brother is watching you» massgeblich geprägt.[162]

125 Für die Schweiz ist insofern insb. die erste Fichenaffäre illustrativ, welche das Land nachhaltig erschütterte. Die NZZ widmete ihr einen Beitrag mit dem Titel «Der gefrässige Staat».[163] Berichtet wird von «bienenfleissigen Beamten», von der «Dunkelkammer der Nation», vom «Moloch Bundesanwaltschaft» und vom «Orwellschen Monster». Den Einzelnen vor der staatlichen Gewalt zu schützen wird ab den 1970er Jahren (im Zuge der Abkehr von Karteikarten und der Hinwendung zu Computern) mit den Tendenzen umfassender Kontrolle der Einzelnen zu einem wichtigen Anliegen der sog. Informationsgesellschaften.[164] Staatliche Rechenzentren, die wie Militär-, Polizei- oder Geheimdienstzentren gut bewacht in Sonderzonen abgeschirmt werden, versinnbildlichen staatliche Macht, Bedeutsamkeit, aber auch Gefährdungspotentiale, die aus elektronischen Datenbearbeitungen resultieren. Zwar wurde die Verhaftung datenschutzrechtlicher Thematisierungen in einer staatszentrierten Sichtweise später problematisiert.[165] Dessen ungeachtet wurde mit der Fokussierung auf die Bedeutung der Errichtung informationeller Strukturen zur Etablierung obrigkeitlicher resp. hoheitlicher Herrschaftssysteme die *bereichsspezifische Differenzierung* als datenschutzrechtlich zentrales Thema in den Blick genommen. Der Fokus auf die Etablierung und Kontrolle von Informationsverarbeitung als Herrschaftstechnik von Instanzen, die hoheitliches Handeln für sich einforderten – die Etablierung dieses Bereiches, der heute als öffentlicher Bereich tituliert wird – drängt nunmehr zum Blick auf die Etablierung des Gegenbereiches, des Bereiches des Privaten.

162 Vgl. Rössler, 34; Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff.; vgl. Baeriswyl, in: Baeriswyl/Rudin (Hrsg.), 47 ff., 49; illustrativ auch Busset, in: Bundesamt für Statistik (Hrsg.), 9 ff., 99; vgl. Bibas, Harv. J.L. & Pub. Pol'y 1994, 591 ff., 591; Schaar, 94 ff.

163 Tribelhorn, NZZ vom 22. November 2014, Fichenaffäre von 1989 – der gefrässige Staat, wobei der Autor diese als Jahrhundertskandal beschreibt, abrufbar unter: <https://www.nzz.ch/schweiz/der-gefraessige-staat-1.18429845?reduced=true> (zuletzt besucht am 30. April 2021); Kreis, digma 2009, 54 ff.; Baeriswyl/Rudin/Hämmerli/Schweizer J./Karjoth, digma 2009, 64 ff.; vgl. auch Busset, in: Bundesamt für Statistik (Hrsg.), 99.

164 Für Deutschland Vesting, in: Ladeur (Hrsg.), 155 ff., 168; für die Schweiz Bründler, SJZ 89, 129 ff., 129; zur Beschreibung der Epoche als Informationszeitalter im Jahr 1990 durch Druey, in: Brem/Druey/Kramer/Schwander (Hrsg.), 379 ff., 379; zu den Ängsten auslösenden Computer-Entwicklungen insb. Simitis, in: Schlemmer (Hrsg.), 67 ff., 67.

165 Hierzu Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff.

III. Kapitel: Das Private und sein Schutz

A. Der Dualismus von öffentlich und privat

Eine Auseinandersetzung mit der Kategorie des Privaten und den Studien, die sich dieser widmen, kommt dem Betrachten eines Vexierbildes gleich: Ständig zeigen sich neue Bilder oder Aspekte. Das Recht, das auf die Strukturierung mittels hinreichend präziser Kategorien hinarbeitet, sieht sich insofern mit einer schwierigen Ausgangslage konfrontiert. Kaum ein Begriff – oder besser Konzept – hat sich als dermassen *bestimmungsresistent* erwiesen wie derjenige des Privaten.[166] 126

Vor diesem Hintergrund erscheint es *paradox*, für «das» Private den *bestimmten Artikel* als Demonstrativpronomen einzusetzen. Damit wird suggeriert, dass im kollektiven Unbewussten jeder wisse, was damit gemeint ist, was der Bedeutungsinhalt des Privaten ist. Gleichwohl: Jeglichen Unberechenbarkeiten, Vagheiten oder der Komplexität und Mehrdimensionalität zum Trotz figuriert das Private bis heute als Schirmbegriff des Datenschutzes. Entsprechend führt in dieser Studie kein Weg um dieses Konzept herum – wenn auch dieser in gebotener Kürze zu absolvieren ist. 127

Das Private an erster Stelle und auf der einen Seite *als Gegenwelt zum öffentlichen Bereich* zu beschreiben, erscheint auf den ersten Blick trivial.[167] Der Kom- 128

166 Nissenbaum, 1 ff.; als kontrovers, umstritten, ambivalent und vage umschrieben von Bennett, 12 f.; bildstark beschrieben als Chamäleon von Murphy, Geo. L.J. 1996, 2381 ff., 2381; dazu, dass privacy ein Konzept mit «several understandings and more misunderstandings» ist, Birnhack, CLSR 2008, 508 ff., 508; zur Beschreibung als «hodgepodge» vgl. m. w. H. Janger, Hastings L.J. 2003, 899 ff., 899; vgl. zu den Theorien und Thematisierungen des Privaten grundlegend auch Rössler, 11 ff.; zur Geschichte des privaten Lebens in fünf Bänden Aries/Duby/Veyne (Hrsg.); Beiträge zu verschiedenen Dimensionen von privacy von Westin, Prosser, Fried u. a. finden sich bei Schoemann (ed.); zum Privaten und Öffentlichen als Kernkategorien feministischer Auseinandersetzungen insb. Landes (ed.); vgl. auch Büchler/Cottier, 39 f.; nicht nur Geuss, 17 ff., insb. 31 f. vertritt, dass der Begriff resp. die Grenzen des Privaten gegenüber des Öffentlichen variabel, facettenreich und evolutiv sein müssen; m. a. W. ist die Flexibilität, Wandelbarkeit und Vielschichtigkeit des Begriffes nicht als Defizit zu sehen; zum Strukturwandel der Öffentlichkeit Habermas, 21 ff.; zur Kritik am liberalen Konzept der Privatsphäre, insb. durch Rousseau, aber auch zur feministischen Kritik Hotter, 45 ff. und 54 ff.; zur Bedeutung des Privaten, auch aus einer historischen Perspektive, Dörflinger, 9 ff.; als Mantra beschrieben wird die privacy von Solove, Stan. L. Rev. 2001, 1393 ff., 1394; Simitis, in: Schlemmer (Hrsg.), 67 ff., 74 beurteilt es als in der Natur der Sache liegend, dass jede Definition des Privaten scheitern müsse, da eine Antwort resp. Konkretisierung nur in der Auseinandersetzung mit dem spezifischen Zusammenhang, in dem Information gefordert werde, gefunden werden könne.

167 Zum Begriffspaar Öffentlichkeit und Privatheit als analytische Konzepte moderner Gesellschaften, zur «Grand Dichotomy», auch unter Bezug auf Arendt und Habermas, vgl. Ritter, 10 ff.; m. w. H. dazu, dass die Trennung bereits über 2500 Jahre alt ist, Weber, in: Honsell/Zäch/Hasenböhler u. a. (Hrsg.), 411 ff., 411.

plexität des Privaten scheint dies nicht gerecht zu werden.[168] Doch gerade die Betrachtung dieser *zweigeteilt bereichsbezogenen Strukturierung und Definierung* schafft die Grundlagen für einen Erkenntnisgewinn. Auf der anderen Seite greift eine auf das Subjekt, die Persönlichkeit und Personendaten als Quasi-Objekte gerichtete Aufmerksamkeit mit Blick auf die gesellschaftlichen und *strukturellen Herausforderungen* ebenso zu kurz.[169] Mit beiden Perspektiven, ihren Potentialen sowie Defiziten wird sich diese Arbeit wiederholt auseinandersetzen.

129 Hinsichtlich der *Etablierung eines Bereiches*, den man den Bereich des Privaten nennt, kommt dem *Liberalismus* entscheidende Bedeutung zu.[170] Es war die sukzessive Verdichtung staatlicher Macht, auch mittels informationeller Infrastrukturen sowie deren Missbrauch,[171] die in den absolutistischen Systemen einen Kulminationspunkt fanden – und die *Reaktionen* auslöste: Gewichtig ist hierbei die *Erkämpfung und Anerkennung von Freiheitsrechten*, die dem staatlichen Handeln und staatlicher Macht Grenzen setzen sollen.[172] Die *Freiheitsrechte* haben für den *Dualismus konstitutive Wirkung*: Sie grenzen das obrigkeitliche, öffentliche Handeln von einem Bereich der Freiheit, dem privaten Bereich, ab.

130 Grundlagenarbeit ist insofern von Rössler geleistet worden: Die Philosophin hat die Theorien des *Liberalismus mit seinen vier tragenden Säulen von Freiheit, Gleichheit, Neutralität und Demokratie* in Bezug zu der *Kategorie resp. den Wert des Privaten* gesetzt und deren zentrale Bedeutung füreinander aufgezeigt.[173] Die liberale Trennung basiert auf der Idee, wonach es Bereiche oder Lebensdimensionen geben müsse, die der Gestaltung und Individualität des *Einzelnen* zu überlassen seien und aus denen sich der Staat mit seinen Eingriffsmöglichkeiten herauszuhalten habe.[174]

---

168 Vgl. zu verschiedenen Dimensionen des Privaten, die allesamt mit demselben Namen eingefangen werden, Rössler, digma 2002, 106 ff., 108 ff.

169 Illustrativ hier der Gesetzestext des DSG, wonach gemäss Art. 1 DSG das Gesetz den Schutz der Person und ihrer Grundrechte beabsichtigt, über die Daten bearbeitet werden; sodann werden Personendaten anhand ihrer «Natur» als besonders schutzwürdig spezifischen Vorgaben unterstellt, vgl. Art. 3 lit. a und lit. c DSG; kritisch zur Verengung der Regelungsperspektive des Datenschutzrechts als Unterfall des allgemeinen Persönlichkeitsrechts Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 und N 26.

170 Rössler, 27 ff.; Geuss, 21.

171 Vgl. exemplarisch die Beschreibung der Entwicklungslinien erster Teil, II. Kapitel.

172 Immerhin ist an dieser Stelle anzumerken, dass eine Grundrechtskonzeptionierung, die vom Schutz von Individuen vor staatlichen Eingriffen ausgeht, kritisch herausgefordert wird, illustrativ insofern Graber/Teubner, Oxf. J. Leg. Stud. 1998, 61 ff.; vgl. mit Blick auf eine Problematik der digitalen Drittwirkung von Grundrechten Karavas, Digitale Grundrechte, 13 ff. und vertiefend zum Diskurs über die Drittwirkung der Grundrechte im Internet gegenüber Privaten, 50 ff.

173 Hierzu und zum Nachfolgenden grundlegend Rössler, 27 ff.; zur Bedeutung des Datenschutzrechts als Rückgrat der Demokratie Spiecker genannt Döhmann, in: Epiney/Sangsue (Hrsg.), 1 ff., 3 ff.; zur Verfassungs- und Grundrechtsdogmatik und zum Datenschutz Donos, 87 ff.; interessant die Ausführungen bei Seemann, 39 ff., zur «herausragenden Persönlichkeit» im Liberalismus im Zusammenhang mit seiner Studie zu Prominenz als Eigentum.

174 Rössler, 27 ff.

In der *privaten Sphäre* soll es dem Einzelnen weitgehend selbstständig obliegen, über sein Handeln zu entscheiden. Folglich verortet die Autorin den Wert des Privaten im *Autonomieschutz*.[175] In der politisch-institutionellen Dimension präsentiert sich das Private und sein Schutz damit als *Abwehrkonzept und -strategie gegenüber staatlichen Invasionen in persönliche Sphären resp. Lebensbereiche*. 131

Mit dem staatstheoretischen Blick auf den Liberalismus werden die *Freiheitsrechte als Rückgrat der Privatheitsidee* offensichtlich: Die Sphären, die durch Freiheitsrechte vor *Interventionen des Staates abgeschirmt werden,* sollen den Bürgerinnen und Bürgern innerhalb dieser abgesteckten Bereiche grundlegende Freiheiten verleihen: eine eigene Meinung zu äussern, zu wirtschaften, familiäre Beziehungen zu leben usf. Mit dieser Betrachtungsweise verengt sich zugleich der Fokus auf das Individuum, die Person, das Subjekt – im Kontext der Freiheitsrechte auf die Bürgerinnen und Bürger. Das Konzept ist gleichzeitig defensiv, individualrechtlich sowie abwehrrechtlich angelegt. 132

Sämtliche dieser Elemente prägen das eidgenössische Datenschutzgesetz bis heute nachhaltig, wie im *zweiten Teil dieser Arbeit* zu zeigen sein wird. Jedenfalls aber macht der Blick auf die Konsolidierung des privaten Bereiches als gegenüber staatlichem Handeln abgeschottete Sphäre mittels Anerkennung von Freiheitsrechten eine *kontextuelle Dimension* sichtbar. Das Private ist tief im Abwehrkonzept gegenüber staatlicher Macht und der Anerkennung der Freiheitsrechte verwurzelt. 133

Für den *privaten Bereich und das Private* ist rechtswissenschaftlich das 19. Jahrhundert von besonderem Interesse.[176] Im Zuge der Ausbildung der Privatrechtskodifikationen wird die Dualität von öffentlichem Recht und Privatrecht als Basiskategorisierung des Rechts installiert. Hier, im 19. Jahrhundert, findet sich ebenso – zumindest in den Köpfen mancher Privatrechtsgelehrten – eine Vorstellung von der Reinheit des Privatrechts. Zugleich akzentuiert sich im 19. Jahrhundert eine Dimension, die Rössler als die *quasi-natürliche Dimension des Privaten* bezeichnet und die besondere Ausprägung mit der bürgerlichen Gesellschaft resp. der bürgerlichen Familie erfährt. Nachfolgend geht es darum, *Dimensionen* 134

175 Rössler, 27 ff.; dass dem wohl berühmtesten Datenschutzrechtler Deutschlands, Spiros Simitis, der sich zu Beginn seiner wissenschaftlichen Karriere auch mit dem Familienrecht befasst hat, eine Festschrift mit dem Titel «Zur Autonomie des Individuums» gewidmet wurde, erscheint auch vor diesem Hintergrund ebensowenig als Zufall, vgl. Simon/Weiss (Hrsg.) mit zahlreichen datenschutz- und informationsrechtlichen Beiträgen; juristisch insofern Garstka, in: Götting/Schertz/Seitz (Hrsg.), 392 ff.; zum Konnex von Privatheit und Privatautonomie bereits Mallmann, 52 ff.; zur Leitidee der Selbstbestimmung, auch in ihren verschiedenen Kontexten, Krähnke, 9 ff.

176 Berühmt wurden mit Blick auf ihr Plädoyer, den Schutz des Privaten rechtlich anzuerkennen, namentlich Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., Gareis sowie Gierke, vgl. Simitis, Calif. L. Rev. 2010, 1989 ff., 1990; zur Trennung von Staat und Gesellschaft im 19. Jahrhundert auch Auer, Diskurs, 29 ff.

des Privaten im Privaten herauszuarbeiten. Eine Kernthematisierung des Privaten findet sich im Häuslichen und Familiären.[177]

B. Das Private im Privaten – Wurzeln und Ingredienzen

1. Das Haus und die subjektiven Rechte von Eigentum und Ehrenschutz

135 Bezüglich der Entwicklungen des *Privaten im Privaten* ist rechtswissenschaftlich die *Ausbildung und Ausdifferenzierung der subjektiven Rechte* von besonderer Relevanz. Das ist die Stelle, an der auch eine Wurzel des aktuellen Schweizer Datenschutzgesetzes zu verorten ist: Es wählt für den privaten Bereich – auch nach der Totalrevision jeglichen Entwicklungen zum Trotz – die *persönlichkeitsrechtliche Anknüpfung*.[178] Analysiert man die Entwicklungen im Rahmen der Anerkennung eines spezifischen subjektiven Rechts auf Schutz «des Privaten», schwenkt der Fokus weg von der institutionellen resp. systemischen Perspektive, wie sie in den bisherigen Ausführungen in den Vordergrund gerückt wurde. Aus welchem (juristischen) Stoff also ist das Private im Privaten gemacht?

136 Als *subjektives Recht* ist es, grob gesprochen, ein *Derivat des Eigentums-, aber auch des Ehrenschutzes*.[179] Die historische Nähe zwischen dem Eigentumsrecht sowie dem Privatheitsschutz ist gut dokumentiert. Es geht an dieser Stelle nicht darum, ebendiese *en détail* darzulegen.[180] Erwähnenswert ist sie gleichwohl, zumal hier Basisannahmen von bis heute wirksamen privat- und datenschutzrechtlichen Debatten sichtbar werden, die sowohl blockierend wie auch konstruktiv

177 Eindrücklich hierzu der einleitende Passus von Wersig, in: Foljanty/Lembke (Hrsg.), 173 ff., N 1 mit ihrem Beitrag zur Care-Arbeit: «Jenseits der Erwerbsarbeit wird eine andere Art von Arbeit geleistet, die in der öffentlichen Sphäre weitgehend ausgeblendet ist und als private Verpflichtung gilt: Sorgearbeit und Hausarbeit»; vgl. auch Nissenbaum, 92.

178 Vgl. Art. 1 DSG sowie Art. 1 nDSG; Art. 12 DSG und Art. 30 ff. nDSG; hierzu vertiefend zweiter Teil, IV. Kapitel; zur persönlichkeitsrechtlichen Anknüpfung des Datenschutzes in der deutschen Rechtstradition vgl. auch Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 196.

179 Sichtbar wird dies anhand einer Lektüre des Aufsatzes von Warren/Brandeis, Harv. L. Rev. 1890, 193 ff.; mit Hinweis auf die komplexen Entwicklungen des Persönlichkeitsrechts, an welches das Datenschutzrecht anknüpft, Götting, in: Götting/Schertz/Seitz (Hrsg.), N 1 und N 5 ff.; vgl. zur Bedeutung der Ehrenordnung für die Entwicklung des Persönlichkeitsschutzes Vesting, in: Götting/Schertz/Seitz (Hrsg.), N 10 ff.; m. w. H. Büchler, AcP 2006, 300 ff., insb. 317 ff.; zum Sacheigentum, geistigen Eigentum sowie einer antithetischen Gegenüberstellung der Eigentumsrechte gegenüber dem Persönlichkeitsrecht vgl. Kohler, 125 f.; grundlegend zum Copyright, das wie kein anderes subjektives Recht eine ideelle, persönlichkeitsrechtliche sowie eine ökonomische, eigentumsrechtliche Komponente und die Idee eines Schöpfergenies beinhaltet, die Studien von Dommann.

180 M. w. H. Pärli, EuZA 2015, 48 ff.; aufschlussreich auch zu den Zusammenhängen von Persönlichkeitsrecht und (geistigem) Eigentumsrecht im 19. Jahrhundert und damit aus einer historischen Perspektive Kippel, ZNR 1982, S. 132 ff.; eine Darstellung des Zusammenspiels von Ehrenordnung und Persönlichkeitsschutz findet sich m. w. H. bei Vesting, in: Götting/Schertz/Seitz (Hrsg.), § 6 Verfassungsgeschichtliche und verfassungsdogmatische Grundlagen, N 1 ff.; zu historischen Eckpunkten auch Tinnefeld/Buchner/Petri, 37 ff.

für ein wirksames Datenschutzrecht *de lege ferenda* wirken. Charakteristisch ist, wie zu zeigen sein wird, eine *räumlich-statische Konstruktion*, die durch die *Metapher des Hauses repräsentiert* wird. Besagte Dimension wurde schon aufgrund der Auseinandersetzung mit den Märchen Ali Baba und Rumpelstilzchen, aber auch anhand der Genfer Häusernummerierung thematisiert. Zugleich findet man mit und im häuslichen Innenraum die *Kategorie der Familie*, die bekanntermassen im Ideal der bürgerlichen Kleinfamilie prägende Wirkung findet. Mit ihr wird gewissermassen ein naturgegebener Binärcode vertreten.[181] Dieser Innenbereich von Haus und Familie ist als Raum der Intimität und der Emotionen zugleich negativ bewertet und auch mit der Kategorie der Scham belegt.[182] Demgegenüber steht der öffentliche Raum, in welchem Geld, Ruhm und Ehre errungen werden können, die eine wichtige Rolle bei der Entwicklung eines zivilrechtlichen Persönlichkeitsschutzes einnehmen.[183] Die nachfolgenden Ausführungen arbeiten Ingredienzen und Elemente des «Privaten im Privaten» heraus.

Zu den Ursprüngen des *zweiten Dualismus* (der erste war der Dualismus von 137
öffentlicher Sphäre im Sinne des hoheitlichen, obrigkeitlichen und späteren staatlichen Bereiches in Abgrenzung zu dem namentlich über die Freiheitsrechte garantierten privaten Bereich): Das Haus ist die Metapher und symbolische Repräsentation für das Private im Privaten. Für die Herleitung eines spezifischen und eigenständigen Privatheitsschutzes zeitigten in den angloamerikanischen wie in den kontinentaleuropäischen Entwicklungen raumbezogene Konzeptionen sowie sachenrechtliche Instrumente initiale Wirkung. Das *Haus* und sein Inneres, die eigenen vier Wände und Mauern sowie invasive Grenzüberschreitungen beeinflussen die Entwicklungen zum Schutz des Privaten im Privaten: «My home is my castle» – das geflügelte Wort aus der Feder von Sir Edward Coke stammt aus dem 15. resp. 16. Jahrhundert. Das Bonmot leitete die Autoren Warren/Brandeis an der Wende vom 18. zum 19. Jahrhundert in ihrem bahnbrechenden Aufsatz «The Right to Privacy» an.[184] Und die auf das Jahr 1819 datierte Sentenz des französischen Philosophen und Politikers P.P. Royer-Collard

> «Voilà donc la vie privée murée, si je puis me servir de cette expression; elle est déclarée invisible, elle est renfermée dans l'intérieur des maisons»[185]

181 Zum Verhältnis der öffentlichen gegenüber der privaten Sphäre aus feministischer Perspektive die zahlreichen Beiträge in Landes (ed.); Rössler, 11 ff. und 41 ff.; Wersig, in: Foljanty/Lembke (Hrsg.), 173 1.

182 Zur Scham resp. Schamlosigkeit mit der Anekdote von Diogenes von Sinope, dessen Gewohnheit es war, auf dem Marktplatz zu masturbieren, Geuss, 33 ff.; vgl. zum Right to Privacy auch in einer rechtshistorischen Betrachtung Richards, Vand. L. Rev. 2010, 1295 ff., 1299, wonach es sich um ein Rechtsmittel zur Wiedergutmachung der emotionalen Verletzung handle, wie sie durch die Publikation von beschämenden privaten Fakten in der Presse; zum Zusammenspiel zwischen privacy, dem Häuslichen und gegenderten Rollenzuweisungen auch Ders., a. a. O., 1295 ff., 1304.

183 Vgl. Vesting, in: Götting/Schertz/Seitz (Hrsg.), N 10 ff.

184 Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 220.

185 Zit. nach Balthasar, Fn 56.

diente 1918 auch dem Schweizer Bundesgericht, um die Unverletzbarkeit des Rechts auf Privatleben als von Art. 28 ZGB erfasstes Schutzgut anzuerkennen: Hier wurde die systematische *Bespitzelung des Nachbarn* mit einer Absicht, die erhobenen Informationen zu verwerten, als widerrechtliche Persönlichkeitsverletzung beurteilt.[186]

138 Historisch präsentiert sich das Right to Privacy eng mit dem *Eigentumsrecht* verbunden.[187] Genauer mit dem *Grundeigentum*, weil die räumlich-häusliche Konzeptionierung augenfällig ist. Das Private im Privaten ist der innere Bereich des *Hauses*, wobei das Eigentum als Ursprungsrecht für die Entwicklung eines heute persönlichkeitsrechtlich basierten Persönlichkeitsrechts betrachtet werden kann, das den Schutz des Privaten inkludiert.[188]

2. Das Right to Privacy – Anstösse von Warren/Brandeis

139 Die beschriebenen Zusammenhänge sowie Entwicklungslinien werden eindrücklich sichtbar bei Warren/Brandeis. Die Autoren proklamierten im Jahr 1890, dass es *zu kurz greife*, den (rechtlichen) Schutz des Privaten auf das Verhältnis zwischen Bürgern und Staat zu beschränken («erster Dualismus»). Vielmehr bedürfe es ebenso der Anerkennung eines rechtlichen Schutzes des *Privaten im Privaten* («zweiter Dualismus»). Einen solchen sahen die Autoren bereits im geltenden Recht angelegt:

> «The common law has always recognized a man's house as his castle, impregnable, often even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?»[189]

140 Warren/Brandeis argumentierten für ein Recht, welches den Schutz eines privaten Lebensbereiches – eines «Right to be let alone» – auch vor invasiven *Verhaltensweisen privater Akteure* gewährleiste. Spezifisch ging es um den Schutz vor grenzüberschreitenden Berichterstattungen durch die Yellow Press. Letztere würde aus der Befriedigung des Bedürfnisses einer «primitiven Neugierde» und des Unterhaltungsinteresses der Allgemeinheit Profit generieren; und zwar zulasten des privaten Lebensbereiches jener Personen, über die berichtet wird.

---

186 Vgl. mit Hinweis auf die bundesgerichtliche Rechtsprechung Schmid, ZBJV, 809 ff., 814 f.; Ehmann, in: Stathopoulos/Beys/Philippos/Karakostas (Hrsg.), 113 ff., 119.

187 Vgl. Westkamp, 42 ff.; zur zeitgenössischen Diskussion, ob privacy rights eine Spezialform von property rights sind, Moore, 22 ff.; für ein property right an Personendaten tritt unter Bezug auf das US-amerikanische Recht z. B. Bergelson, UC Davis L. Rev. 2003, 379 ff., insb. 400 ff. ein, nachdem sie sich mit den kritischen Hinweisen auseinandergesetzt hat, die den beiden Paradigmen von privacy as secrecy und privacy as control entgegengebracht werden.

188 Vgl. auch Regan, 43 ff.; zur Bedeutung des Hauses und der bürgerlichen Familie für die Kategorie des Privaten Bartsch, in: Bartsch/Briner (Hrsg.), 31 ff., 31 f.

189 Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 220.

Der Aufsatz in der berühmten Harvard Law Review, der in die Rechtsgeschichte einging, wandte sich somit direkt *gegen die Informationserhebungen* – von Personendaten in heutiger Terminologie, vgl. Art. 1 DSG resp. Art. 1 nDSG und Art. 3 lit. a DSG resp. Art. 5 lit. a nDSG – *durch private Akteure*, die Medienunternehmen mit ihren Presseerzeugnissen.[190] Der Aufsatz stiess dessen ungeachtet sowohl die privatrechtlichen als auch die verfassungsrechtlichen Entwicklungen an.[191] 141

Vor der präziseren Analyse des rechtshistorischen Plädoyers von Warren/Brandeis ein kurzer Brückenschlag in die Gegenwart: Die Austarierung sowie Koordination zwischen Presse- und Meinungsfreiheit und dem Informationsinteresse der Allgemeinheit, dem Schutz der Persönlichkeit sowie Datenschutz, den Kommerzialisierungstendenzen und dem Unterhaltungsinteresse konfrontiert das Daten- und Informationsrecht bis heute mit spezifischen Herausforderungen.[192] Für den Medienkontext etablierte sich – in verschiedenen Gesetzen niedergelegt – ein spezifisches Regelungsregime.[193] Selbstredend findet sich auch dieses in steter Veränderung: Jüngst steht eine Anpassung der vorsorglichen Massnahmen gemäss Art. 266 ZPO zur Debatte, die als folgenschwere Einschränkung der Medienfreiheit kritisiert wird.[194] Es geht um die Löschung eines kleinen Wortes mit weitreichenden Konsequenzen: Die Mehrheit der Kommission für Rechtsfragen im Ständerat tritt für eine Anpassung der Bestimmung dergestalt ein, dass in Zukunft nur noch ein «schwerer Nachteil» notwendig ist, um eine Publikation vorsorglich zu verbieten. Anders ist für die Verfügung einer entsprechenden vorsorglichen Massnahme nach noch aktuellem Gesetzeswortlaut ein «besonders schwerer Nachteil» erforderlich.[195] 142

Warren/Brandeis forderten ein subkutan bereits existierendes zivilrechtliches subjektives Recht, das Right to Privacy, mit delikts- und abwehrrechtlichem Charakter anzuerkennen, mit folgenden Worten: 143

190 Der Beitrag von Warren/Brandeis wird als monumentaler Artikel bezeichnet von Post, Case W. Res. L. Rev. 1991, 647 ff., wobei der Autor die Ablösung der privacy von property als Kernerrungenschaft nennt.

191 M. w. H. Turkington, N. Ill. U. L. Rev. 1990, 479 ff.; Leebron, Case W. Res. L. Rev. 1991, 769 ff., 802.

192 Vgl. auch BGE 132 III 644 und BGE 127 III 481 m. w. H. bereits Peter, 193; zum Instrumentarium des Gegendarstellungsrechts vgl. Art. 28k ff. ZGB; zu den vorsorglichen Massnahmen im Medienkontext vgl. Art. 261 i. V. m. Art. 266 ZPO; datenschutzgesetzlich zu beachten insb. Art. 13 lit. D DSG, Art. 27 nDSG und Art. 31 Abs. 2 lit. D nDSG.

193 Zum Instrumentarium des Gegendarstellungsrechts vgl. Art. 28k ff. ZGB; zu den vorsorglichen Massnahmen im Medienkontext vgl. Art. 261 i. V. m. Art. 266 ZPO; datenschutzgesetzlich beachte insb. Art. 10 DSG, Art. 13 lit. d DSG sowie Art. 27 nDSG, Art. 31 Abs. 2 lit. d nDSG; zudem ist insb. auch an die Figuren der absoluten und relativen Personen der Zeitgeschichte zu erinnern, vgl. insb. BGE 127 III 481, E 2.c.

194 <https://www.infosperber.ch/medien/trends/staenderaete-wollen-medienfreiheit-weiter-einschraenken> (zuletzt besucht am 20. September 2021).

195 <https://www.parlament.ch/centers/eparl/curia/2020/20200026/S1%20D.pdf.> (zuletzt besucht am 31. August 2022).

> «Perhaps it would be deemed proper to bring the criminal liability for such publication within narrower limits; but that the community has an interest in preventing such invasions of privacy, sufficiently strong to justify the introduction of such a remedy, cannot be doubted. Still, the protection of society must come mainly through a recognition of the rights of the individual. Each man is responsible for his own acts and omissions only. If he condones what he reprobates, with a weapon at hand equal to his defence, he is responsible for the results. If he resists, public opinion will rally to his support. Has he then such a weapon? It is believed that the common law provides him with one, forged in the slow fire of the centuries, and to-day fitly tempered to his hand.»[196]

144 Ausgangspunkt sowie Dreh- und Angelpunkt der Argumentation ist eine Auseinandersetzung mit und eine Abgrenzung sowie Ablösung vom *property right*:

> «[…] the term „property" has grown to comprise every form of possession – intangible, as well as tangible.»[197]

145 In diesem Sinne handelt es sich bei der Ableitung und Anerkennung des Right to Privacy um eine Emanzipationsleistung. Ausgehend vom Eigentumsrecht differenzieren die Autoren die *subjektiven Rechte des Zivilrechts* weiter aus. Neu am Ansatz von Warren/Brandeis ist weniger der Befund, wonach eine «rechtlich geschützte Privatsphäre» bestünde, als vielmehr deren Abkoppelung bzw. deren Anerkennung *unabhängig von einem allfälligen Eigentumsrecht oder dem Recht auf Schutz der Ehre*.[198] Die Autoren nutzen und beziehen sich weiter auf urheberrechtliche Erwägungen.[199] Insofern vertreten sie die Ansicht, dass es «in reality» um den Schutz der «Immunität der Person», des «Right to one's Personality» gehe. Die Konzentration der Autoren gilt der Entwicklung, Ausdifferenzierung und Theoriebildung zu den zivilrechtlichen Individualansprüchen.

146 Im Kern handle es sich beim Right to Privacy, so Warren/Brandeis, um ein Recht, *alleine resp. in Ruhe gelassen zu werden*.[200] Um dieses verselbstständigte Recht wirksam durchzusetzen, würden allerdings die bisherigen Instrumente nicht genügen. Vielmehr bedürfe es der Schaffung eines neuen Rechtsmittels.[201] Gemäss der Argumentation der beiden Autoren müssten die Gerichte dazu bloss im *common law* bereits vorhandene Rechtsmittel weiterentwickeln.[202]

---

196 Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 220.
197 Dies., a. a. O.
198 Leebron, Case W. Res. L. Rev. 1991, 769 ff., 778; eine vertiefende Analyse zum Verhältnis der verschiedenen involvierten rechtlichen Kategorien von Privacy, Personality, Property und Copyright liefert insb. Post, Case W. Res. L. Rev. 1991, 647 ff.; vgl. für das britische common law zu den Rechtsquellen Westkamp, 25 ff.
199 Aus historischer Perspektive aufschlussreich in diesem Zusammenhang auch die Ausführungen zum Eigentum an Bildern von Dommann, in: Joly/Visman/Weitin (Hrsg.), 249 ff.
200 Diese Aussage ist vermutlich auf Judge Cooley in Union Pacific Railway v. Botsford, 141 U.S. 250 (1891) zurückzuführen: «The right to one's person may be said to be a right of complete immunity; to be let alone.»
201 Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 219; vgl. Leebron, Case W. Res. L. Rev. 1991, 769 ff., 779.
202 Dies., a. a. O., 193 ff., 220; zu Privacy & Publicity im britischen common law vertiefend Werstkamp, 17 ff.

147 Auch die Praxis sah sich mit den entsprechenden Herausforderungen konfrontiert: Während ein Right to Privacy in *Roberson v. Rochester Folding Box Co.*[203], einem in New York entschiedenen Fall, noch verworfen worden war, wurde das Recht kurze Zeit später im Bundesstaat Georgia, nämlich im Fall *Pavesich v. New England Life Insurance Co.,* anerkannt.[204] 1939 wurde der *privacy tort* in das Restatement of Torts § 867 (1939) aufgenommen.[205]

148 Einen weiteren Meilenstein zur Weiterentwicklung und Ausdifferenzierung des *privacy tort* lieferten die Arbeiten von Prosser. Der Autor analysierte in einem Aufsatz von 1960 zahlreiche Urteile und führte deren Inhalte und Kernaussagen einer Kategorisierung zu. Daraus entstand eine Nomenklatur von vier verschiedenen *privacy torts*, die später im Restatement (Second) of Torts § 652A-E von 1977 aufgeführt wurden. Sie werden zwischenzeitlich in den meisten Gliedstaaten komplett oder zumindest teilweise verankert.[206] Anerkannt werden die folgenden vier Verletzungsformen:[207] Die erste Verletzungsform definiert sich als «Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs». Es geht hierbei um das Eindringen in den persönlichen Bereich bzw. in die Privatsphäre einer Person, z. B. durch das Abhören eines Telefongesprächs. Die zweite Verletzungsform heisst «Public disclosure of embarrassing private facts about the plaintiff». Bei diesem Tort geht es um den Schutz vor unerwünschten Veröffentlichungen von unangenehmen Tatsachen aus dem Privatleben.[208] Die dritte Verletzung besteht in der «Publicity which places the plaintiff in a false light in the public eye». Mit anderen Worten geht es um die falsche oder entstellende Darstellung, welche die betroffene Person in der Öffentlichkeit in einem falschen Licht erscheinen lässt. Und die vierte Verletzungshandlung erfasst die «Appropriation, for the defendant's advantage, of the plaintiff's name or likeness», wobei dieser Tort auf die Abwehr von unerlaubter Verwendung und Ausnutzung der Persönlichkeitsmerkmale einer anderen Person zum eigenen Vorteil abzielt.[209]

203 New York Ct. App., 64 N.E. 442 – Roberson v. Rochester Folding Box Co., Urteil vom 27. Juni 1902.

204 Georgia Supreme Ct., 122 Ga. 190, 50 S.E. 68 – Pavesich v. New England Life Insurance Co. et al., Urteil vom 3. März 1905.

205 Goodhart, U. Pa. L. Rev. 1943, 487 ff., 487, 508.

206 M. w. H. Götting, GRUR Int. 1995, 656 ff., 657, insb. auch auf die Rechtsprechungsübersicht bei McCarthy.

207 Prosser, Calif. L. Rev. 1960, 383 ff., 393 ff.

208 Dies ergänzt die traditionellen Torts libel und slander insofern, als auch eine Tatsache, welche an sich korrekt ist, die Tatbestandsvoraussetzungen erfüllen kann. Es genügt, dass die geäusserte Tatsache sich herabsetzend auswirkt; sie muss darüber hinaus nicht falsch sein.

209 Diese Kategorie kam z. B. im Fall Pavesich v. New England Life Insurance Co. zur Anwendung. Dabei ging es um die unautorisierte Verwendung eines Fotos für Werbung; zu den Entwicklungen des Right of Privacy and Publicity im US-amerikanischen Recht vgl. auch Höning, 5 ff.; zur Bedeutung des Beitrages von Warren/Brandeis und den vier Torts auch Murphy, Geo. L.J. 1996, 2388 ff.

149 Die umrissene Kategorisierung wird *bis dato* aufrechterhalten.[210] Aus der Perspektive der betroffenen resp. verletzten Person formuliert bedeutet sie: Nur wer in einer der oben genannten vier Handlungsformen in seinem Right to Privacy angegriffen wird, erhält gerichtlichen Schutz bzw. wird entschädigt. Nicht in den Katalog fällt z. B. das Verkaufen von Adresslisten ohne Zustimmung der Betroffenen, sofern die Persönlichkeitsmerkmale nicht öffentlichkeitswirksam als Werbeträger eingesetzt werden.[211] Ebenso wenig gilt die Weitergabe von Interessenprofilen durch ein Kreditkartenunternehmen als Privacy-Verletzung, da die Betroffenen durch die Benutzung der Kreditkarte freiwillig ihr Konsumverhalten publik machen würden und deswegen kein Eindringen in den persönlichen Bereich vorliege.[212]

150 Dass die bestehenden Kategorien auf diese neueren Sachverhalte nicht angewendet und keine Fortbildung und Ergänzung der etablierten Fallgruppen vorgenommen wurden, sieht Buchner im traditionellen Zusammenspiel von Richter- und Gesetzesrecht begründet: Demnach ist das Tätigwerden des Gesetzgebers zwecks Anpassungen an gesellschaftliche Entwicklungen geboten.[213]

151 Im Rahmen der Anerkennung der privacy torts war dies unter Umständen deswegen nicht notwendig, weil Warren/Brandeis darlegen konnten, dass sowohl das Recht als auch das Rechtsmittel im common law bereits angelegt waren. Denn obschon sie ihr Right to Privacy im «Kleid» des Persönlichkeitsrechts präsentierten, steckte in ihm zu grossen Teilen das Eigentum. Dementsprechend ist das Right to Privacy gleichermassen tief in einem territorialen, räumlich-häuslichen Konzept verwurzelt wie von einer abwehr- sowie deliktsrechtlichen Struktur geprägt:

> «Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right „to be let alone". *Instantaneous photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life;* and numerous mechanical devices threaten to make good the prediction that „*what is whispered in the closet shall be proclaimed from the house-tops*"».[214] [Hervorhebungen durch die Autorin]

210 Vgl. Buchner, 13.

211 Keine «appropriation» in Ohio Ct. App., 341 N.E. 2d 337 – Shibley v. Time, Inc., Urteil vom 19. Juni 1975.

212 Vgl. kritisch Buchner, 13 f. m. w. H.; zum Ausmass der Re-Identifizierungsmöglichkeiten von Personen anhand von Kreditkartenabrechnungsdaten De Montjoye/Radaelli/Singh et al. (ed.), Science 2015, 536 ff.; zum kartengestützten Zahlungsverkehr vgl. Kahler/Werner, 143 ff.; jüngst zur Kreditkarte vor dem Hintergrund des schweizerischen Rechts vgl. die Zusammenfassung zur Dissertation Oppliger, ex ante 2020, 32 ff., 34, auch zur Anwendbarkeit des DSG.

213 Buchner, 14.

214 Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 195; aufschlussreich zu den Privacy-Konzepten im US-amerikanischen Recht, allgemeiner aber auch zum Einfluss neuer Technologien auf das Recht Friedman, in: Becker/Hilty/Stöckli/Würtenberger (Hrsg.), 405 ff.

Diesseits wie jenseits des Atlantiks charakterisieren folglich *verkörperlichte und territoriale Symbolisierungen die Sichtbarmachung des Privaten im Privaten* – die Burg, das Haus und dessen Inneres, das häusliche Leben als Bereich, der gegenüber der Öffentlichkeit abgegrenzt wird. Als unsichtbar wird dieses Leben im Inneren des Hauses beschrieben – und entsprechend unklar scheinen die Charakteristika der jeweiligen Schutzräume zu bleiben. Anerkannt wird primär, dass das «Private im Privaten» in Abgrenzung zur öffentlichen Sphäre schutzwürdig ist. Worin «das Private», die Privacy, allerdings genau besteht, was sie schutzwürdig macht usf., bleibt weitgehend im Dunkeln, im Inneren der «Mauern» verborgen. 152

Präsentiert wird mit dem Right to Privacy ein Konzept, nach welchem es um die Verteidigung einer Privatsphäre geht, die Gewährleistung eines Schutzraumes und die Respektierung von Grenzen gegenüber «Invasion».[215] In den Worten von Warren/Brandeis: *Eingefallen* wird in die *heiligen Bezirke* des Privat- und Familienlebens, durch die *Vordertür und die Hintertür*; von Waffen, die dagegen geschmiedet wurden, ist die Rede; vom Dach soll nicht verkündet werden, was im «stillen Kämmerlein» geflüstert wird. 153

Eine dergestalt imprägnierte räumliche und eigentumsrechtliche Konzeptionierung wird auch in der Schweiz Einfluss auf die Ausbildung des zivilrechtlichen Privatheitsschutzes nehmen. Schon der Titel einer Studie von Giesker aus dem Jahr 1905 illustriert dies: «Das Recht des Privaten an der eigenen Geheimsphäre – ein Beitrag zu der Lehre von den Individualrechten». 154

Wie im *zweiten Teil dieser Arbeit* zu zeigen sein wird, wirken die besagten Prämissen bis heute im zeitgenössischen eidgenössischen Datenschutzrecht fort – gesetzlich selbst nach seiner Totalrevision im 21. Jahrhundert, zudem in Lehre und Praxis. Ein Regime allerdings, das seinen Fokus auf einen *defensiv gedachten Subjektschutz* richtet, lässt – so die *These*, wie sie auch anhand der historischen Rückblende freigelegt wurde – allerdings die systemische, institutionelle Dimension datenschutzrechtlicher Regulierung in den Hintergrund rücken. Immerhin bleibt sie in dem Sinne sichtbar, als dass – ganz ähnlich zur Abgrenzung des privaten Bereichs gegenüber dem öffentlichen im Sinne des staatlichen Bereichs – ein *zweiter Dualismus* auch im Recht installiert wird, die *Privatsphäre innerhalb des Privatbereichs*. 155

215 Trefflich und in diesem Geiste z. B. auch der Titel des Aufsatzes von Simitis, in: Schlemmer (Hrsg.), 67 ff.; vgl. auch Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 198.

3. Privatheit, häuslich-familiäres Leben und bürgerliche Gesellschaft

156 Innerhalb der Auseinandersetzung mit dem *zweiten Dualismus*, dem Privaten im Privaten, und dem Aspekt der *räumlich-statischen Konzeptionierung*, die sich an der Metapher des Hauses orientiert, zeigt sich eine weitere Facette des Privaten: Das Haus schafft den *Abgrenzungsraum für die Familie und das häusliche Leben*, soll den Bereich des Schutzes vor den Rauheiten des öffentlichen Lebens liefern. Das familiäre und innerhäusliche System wird von Rössler als die quasi-natürliche Dimension des Privaten bezeichnet.[216] Den Konnex der Kategorien des Privaten und der Familie bildet in eindrücklicher Weise Art. 8 EMRK ab. Der Artikel vereint in sich die Garantien auf Schutz des Privat- und Familienlebens. Allerdings sind die beiden Schutzbereiche nur teilweise überlappend.[217]

157 Wenn nun der Terminus «privat» *auch den Bereich des Familiären* markiert, lohnt es sich, in diesem Raum etwas zu verweilen. Die Familie kehrt als eine Konstante von der Antike bis heute in zahlreichen Diskursen um das Private wieder.[218] Eine eigentliche Akzentuierung der *Familie als Institution des Privaten* bildet die bürgerliche Kleinfamilie der Vormoderne – sie ist entsprechend ebendieser Zeit der privilegierten Gesellschaftsschicht zuzuordnen, der auch Warren/Brandeis angehörten. Es ist die Epoche, in der sich die bürgerliche, eheliche Kleinfamilie mit geschlechtsstereotyper Arbeitsteilung zum Familienideal konsolidierte.[219] *Nota bene:* zum Familienideal erhoben bedeutet nicht, dass ebendiese Familie den herrschenden Familienrealitäten entsprach.[220] Die bürgerliche Kleinfamilie als real gelebte Familienform war ein «Privileg der Oberschicht», ebenso die Rückzugsmöglichkeit in einen geschützten räumlichen Bereich.

158 Fundament der bürgerlichen Einheitsfamilie bildete die Ehe zwischen Mann und Frau.[221] Auch insofern lässt sich eine ursprünglich eigentumsrechtliche Verwurzelung nachzeichnen, führt man sich die Definition von Kant zur Ehe zu Gemüte: Nach seinem Dafürhalten ist die Ehe die

216 Zur Natur vs. Kultur-Debatte anhand der Kategorien von männlich und weiblich, auch unter dem Titel des Privaten, Ortner, in: Landes (ed.), 21 ff.; Rössler, digma 2002, 106 ff., 108 f.; Nissenbaum, 90; zum Zusammenspiel der Kategorien auch Bartsch, in: Bartsch/Briner (Hrsg.), 31 ff.; Richards, Vand. L. Rev. 2010, 1295 ff., 1304 f.

217 Vgl. für eine vertiefte Auseinandersetzung mit dem Schutz des Privatlebens gemäss Art. 8 EMRK dritter Teil, IIX. Kapitel; dazu, dass Art. 8 EMRK weit ausgelegt wird und der ebenda verbürgte Schutz ebenso Relevanz im Arbeitsverhältnis hat, Pärli, EuZA 2020, 224 ff., 225 f.; Ders., EuZA 2015, 48 ff., 52 ff.

218 Vgl. Ariès, 7.

219 Peukert, 20 ff.; Büchler/Cottier, m. w. H., 37 ff.

220 Vgl. namentlich die Beiträge von Schwenzer, Familie und Recht sowie z. B. FamPra.ch 2014, 966 ff.; sodann haben sich mit Familienbildern vonseiten der Schweizer Rechtswissenschaft sowie den familiären Realitäten insb. Büchler, Cottier, aber auch Cantieni, Fankhauser oder Pfaffinger befasst.

221 Schwenzer, FamPra.ch 2014, 966 ff., 973 f.

> «Verbindung zweier Personen verschiedenen Geschlechts zum lebenswierigen wechselseitigen Besitz ihrer Geschlechtseigenschaften […].»[222]

159 Die eine Person kann sich – im Geschlechtsgenuss – unter der Bedingung zur Sache machen, dass die andere sich ihr ebenfalls als solche gibt; denn auf diese Weise gewinnt sie wieder ihre Persönlichkeit. Das Verhältnis der Verehelichten ist nach KANT ein Verhältnis der Gleichheit des Besitzes sowohl der Personen als auch der Güter. In der Ehe liegt ein «auf dingliche Art persönliches Recht» vor.[223]

160 Später wird die Familie mit der bürgerlichen Kleinfamilie zum Hort der Geborgenheit und Liebe, Emotionalität, Körperlichkeit, Sexualität, Fortpflanzung und Intimität erhoben.[224] Ihre konstitutiven Elemente sind Ehe zwischen Mann und Frau, Leben unter einem gemeinsamen Dach, gemeinsame leibliche Kinder, wobei der Mann in der öffentlichen Sphäre das Geld verdient und die Frau im Innenbereich Kinder und Haushalt versorgt.[225] Die bürgerliche Familie als Nukleus des Privaten im Privaten wird damit von einer «naturgegebenen Dualität» beherrscht.[226]

161 Mehrere familienrechtliche und familieninformationsrechtliche Regelungen schütz(t)en dieses Familienideal.[227] Im Vordergrund stehen hierbei namentlich gesetzgeberische *Blockierungen von Informationsflüssen*, welche auf den Schutz des Ideals der ehelichen Einheitsfamilie abziel(t)en und diese von angrenzenden oder einbettenden Bezugssystemen hermetisch abzuschirmen versuchen. So werden beispielsweise im Konzept der geheimen Volladoption oder im System der ehelichen Vaterschaftsvermutung Informationsflüsse unterbunden, um Verletzungen der Normerwartungen zu kaschieren resp. zu verdrängen. Sie verfolgen Institutionenschutz.[228]

---

222 KANT, Metaphysik der Sitten, Rechtslehre, Eherecht, § 25; vgl. insofern auch AUER, AcP 2016, 239 ff.

223 DERS., a. a. O., §§ 24 ff.; vertiefend weiter zu Eigentum und Herrschaft bei KANT vgl. HELD, 114 ff.

224 PFAFFINGER, N 106 ff.

225 Vgl. z. B. WERSIG, in: FOLJANTY/LEMBKE (Hrsg.), 173 ff.; RÖSSLER, 41 ff.

226 Aktuell wird die Überwindung der (biologischen) binären Geschlechterordnung auch im Rahmen des Registerrechts der Schweiz thematisiert, vgl. Schweizer Parlament, Drittes Geschlecht im Personenstandsregister, Dezember 2017, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174121> (zuletzt besucht am 30. April 2021).

227 Vgl. zum Institutionenschutz namentlich zahlreiche Beiträge von SCHWENZER, z. B. zu Frauenbildern im Familienrecht, 1 ff.; ein modernes Familienrecht müsse sich u. a. von der Vorgabe leiten lassen, keinen Institutionenschutz zu betreiben, vgl. DIES., Grundlinien eines modernen Familienrechts, 109 ff., 115; inwiefern das Familienrecht des ZGB Institutionenschutz betreibt, wurde namentlich von BÜCHLER, COTTIER und PFAFFINGER thematisiert; zum Begriff des Informationsrechts mit seiner Themenvielfalt vgl. BURKERT, in: MEIER-SCHATZ/SCHWEIZER (Hrsg.), 155 ff., 157 ff.; eine Übersicht zu den zahlreichen Rechtsgrundlagen, die dem Schutz der Information dienen, findet sich bei DRUEY, in: WEBER/HILTY (Hrsg.), 7 ff.

228 Vgl. SCHWENZER, FamPra.ch 2014, 966 ff., 973 f.; mit Fokus auf familieninformationsrechtliche Regelungen PFAFFINGER, 116 ff.; DIES., Ancilla Iuris (anci.ch) 2016, 49 ff. sowie FamPra.ch 2014, 604 ff.

162 In Bezug auf die Bedeutung der *Kategorie der (bürgerlichen) Familie für das Private* darf denn auch eine Anekdote nicht unerwähnt bleiben: Sie liefert die Hintergrundszenerie für den Beitrag von Warren/Brandeis. Und sie wurde nahezu ebenso intensiv rezipiert wie die wissenschaftliche Argumentation der beiden Autoren im Harvard Law Review. Am Anfang des Right to Privacy stand ein familiärer Anlass im Kreise eines der Autoren – die Verehelichung der Tochter von Warren. Sie wurde mit einem der Gesellschaftsschicht entsprechend lukullischen Hochzeitsmahl gefeiert. Nicht nur darüber, sondern darüber hinausgehend wurden das mondäne Leben sowie der Lebenswandel des Brautvaters in der Yellow Press thematisiert. Es ging einem der beiden Autoren mit seinem Plädoyer in Gestalt eines wissenschaftlichen Artikels damit ebenso um ein ganz persönliches Anliegen.

163 Mit dieser Hintergrundinformation zur (familiären) Herkunft und zum gesellschaftlichen Milieu, in dem sich die «Urheber des Right to Privacy» bewegten, bahnt sich eine weitere *Dichotomie* an: die *Zweiteilung der Gesellschaft in eine Ober- und Unterschicht* (neben derjenigen der Geschlechterrollen). Die dem privilegierten Mann zugebilligten Freiräume, die Abweichung vom Ideal der lebenslangen monogamen ehelichen Beziehung, bedurften Schutzmechanismen, namentlich der Diskretion und Geheimhaltung. Mit seiner Diskretionsforderung ging es damit wohl ebenso um den Schutz eines Lebensstils, der dem Ehemann der bürgerlichen Gesellschaft quasi durch das Privileg der Doppelmoral eingeräumt wurde. Warren/Brandeis beklagten, dass in der Sensationspresse unter anderem Berichte über sexuelle Relationen verbreitet wurden. Aus der Veröffentlichung von «Gossip» über die «Bourgeoisie» würde auch noch finanzieller Profit geschlagen. Die Gesellschaft (die untere Gesellschaftsschicht resp. das «Proletariat») würde in niederen Bedürfnissen adressiert, die schnöde Neugierde befriedigt. Hierin wurde eine Gefahr für den Zerfall der Gesellschaft sowie Moral verortet.[229]

164 Neugier und wirtschaftliche Interessen erscheinen in dem Aufsatz unmissverständlich als *niedere Motive*, deren Befriedigung im Medienkontext als Beitrag zum Sittenzerfall taxiert. Weil die gesellschaftlichen Ausschweifungen des einen Autors – ein verheirateter Mann aus der Oberschicht – hinter dem Beitrag standen, wundert es kaum, dass die beiden selbst von wissenschaftlicher Seite gleichermassen Ruhm wie Häme erfuhren. Prosser präsentierte seine weiterfüh-

229 Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 196; zivilrechtliche Probleme der identifizierenden Berichterstattung am Beispiel der Presse für die Schweiz greift 1981 Lüthy in ihrer rechtswissenschaftlichen Dissertation auf. Die Autorin geht zum einen auf die öffentliche Aufgabe der Presse und die Pressefreiheit – vgl. 14 ff., 17 ff. und 35 ff. – sowie zum anderen auf das geschützte Rechtsgut der «Persönlichkeit» ein, vgl. 39 ff., und den Schutzbereich der Privatheit, vgl. 67 ff.

rende Analyse zum Right to Privacy und der Kategorisierung von vier *privacy torts* mit den süffisanten Worten:

> «All this is a most marvelous tree to grow from the wedding of the daughter of Mr. Samuel D. Warren.»[230]

Es ist somit die privilegierte Oberschicht,[231] die sich von der «primitiven Neugier der Unterschicht» abzugrenzen sucht und die massgeblichen Einfluss auf die Anerkennung des Right to be left alone resp. Right to Privacy nahm. Zugleich leisteten die Elemente der Scham und Beschämung, der Sexualität und Untreue einen Beitrag zur Herausbildung des zivilrechtlichen Privatheitsschutzes. Die *bürgerliche Ehrenordnung und der Schutz des Ansehens* gelten ihrerseits als *originäre Elemente zur Entwicklung des Persönlichkeitsschutzes*.[232] Eindrücklich beschrieben wird der Konnex des Ideals der bürgerlichen Ehe mit dem Ehrenduell infolge eines Ehebruches durch die Frau im berühmten Roman «Effi Briest» von Theodor Fontane.[233] 165

Die Ehre und das Ansehen als im Privatheitsschutz angelegte Schutzgedanken werden sodann im 1899 gefällten Urteil Vogelsanger des Bundesgerichts thematisiert. Der Entscheid anerkannte die Notwendigkeit des Schutzes des Einzelnen vor Datenbearbeitungen im privaten Sektor.[234] Ihm lag folgender Sachverhalt zugrunde: Ein Verband versandte an seine Mitglieder Listen mit «saumseligen oder böswillig und fruchtlos gepfändeten» Schuldnern. Diese sog. «Lumpenlisten» und die damit beabsichtigte gegenseitige Warnung beurteilte das Bundesgericht nicht als an sich widerrechtlich. Allerdings müssten die Informationen der *Wahrheit* entsprechen, wobei eine Verwechslung zwischen den Kategorien «saumselig» und «zahlungsunfähig» auszuschliessen sei. Sodann müssten für die Schuldner die Gründe ersichtlich sein, weshalb es zu einer Nennung auf der Liste kam. Da besagte Vorgaben der Rücksicht vom Verband nicht eingehalten worden waren, wurde der Verband wegen widerrechtlichen Verhaltens zu Genugtuung und Schadenersatz verurteilt.[235] In diesem Urteil deutet sich die Herausbildung datenschutzrechtlicher Grundprinzipien, wie dasjenige der Rich- 166

230 Vgl. Prosser, Calif. L. Rev. 1960, 383 ff., 423.

231 Dazu auch Simitis, in: Schlemmer (Hrsg.), 67 ff., 70 f.

232 Hierzu Vesting, in: Götting/Schertz/Seitz (Hrsg.), N 10 ff.; zum Zusammenhang des Right of Privacy mit dem Ansehen resp. der Reputation, wobei Informationen preisgegeben werden, welche die Reputation stärken, Murphy, Geo. L.J. 1996, 2381 ff., 2384 ff.

233 Fontane, 373.

234 BGE 25 II 621; weitere frühe Entscheide zum Schutz der Privatsphäre sind BGE 31 II 429, BGE 43 II 236, BGE 44 II 319, BGE 57 II 334; für eine Übersicht auch über die kantonalen Entscheide Schmid, ZBJV 1995, 809 ff., 813 ff.

235 Vgl. zu den Rechtsbehelfen wegen widerrechtlicher Persönlichkeitsverletzung gemäss Art. 28 ZGB den Art. 28a ZGB, dessen Abs. 1 die spezifischen Klagebehelfe und dessen Abs. 2 die allgemeinen Klagen auf Schadenersatz, Genugtuung und Gewinnherausgabe einräumt; zu den Rechtsbehelfen nach Persönlichkeitsverletzung vertiefend vgl. Inderkum, 3 ff.

tigkeit sowie der Transparenz an, wie sie später zum festen Bestandteil datenschutzgesetzlicher Erlasse werden.

167 Die wie illustriert bis ins 19. Jahrhundert zurückreichenden Wurzeln des Diskurses um die Notwendigkeit eines rechtlichen Schutzes des Menschen vor Informations- und Datenbearbeitungen wurden zunächst – wie der schweizerische Entscheid zeigt – durchaus, aber nicht nur von technischen Entwicklungen vorangetrieben. Geführt wurde diese frühe Debatte im amerikanischen Recht unter dem Right of Privacy, in der Schweiz resp. allgemein in Europa unter dem Schutz der Persönlichkeit, des Privatlebens oder der Privatsphäre, aber auch der Ehre.[236]

168 Zurück zum Beitrag von Warren/Brandeis: Die Autoren haben mit ihrem Aufsatz «The Right to Privacy» für die eigenständige und allgemeine Anerkennung des neuen subjektiven Rechts – abgelöst vom Eigentum und dem Ansehensschutz – plädiert. Gleichzeitig und in aller Deutlichkeit präsentiert sich ihr Beitrag als eine «gesellschaftspolitische Streitschrift». Warren/Brandeis waren, wie gezeigt, Angehörige einer Elite. «Eigene Rückzugsräume» – dessen ist man sich heute vielleicht mehr denn je bewusst – sind (und waren) ein *Privileg*.[237]

169 Denn im 19. Jahrhundert, in dem der spezifische und eigenständige Privatheitsschutz ausgebildet wurde, war für eine Vielzahl von Menschen an Orte des Rückzugs nicht zu denken; vielmehr hausten in den Grossfamilien mehrere Generationen auf engstem Raum unter einem Dach. Es ist wiederum die *bürgerliche Kleinfamilie* – in Realform eher die Ausnahme –, deren Mitglieder aufgrund potentiell grosszügiger Raumverhältnisse Rückzugsmöglichkeiten offenstanden. Um Raum für Privatheit zu beanspruchen, ist nicht zuletzt Wohlstand erforderlich. Das Privacy Right präsentiert sich damit im Ursprung *nicht* als «Recht des einfachen Mannes».[238] Die Tonalität der Überlegenheit und des Paternalismus lässt sich im Artikel von Warren/Brandeis kaum überhören.

170 Damit ging es in dem Beitrag keineswegs nur um die Verbürgung eines neuen, jedem Menschen verbürgten subjektiven Rechts. Vielmehr zielten die Bemühungen

236 Für die Schweiz zum Schutz von Personendaten im System des zivilrechtlichen Persönlichkeitsschutzes und zum Schutz der Privatsphäre sowie zur Sphärentheorie, welche von Hubmann entwickelt und von Jäggi in die Schweiz transferiert wurde, vgl. vertiefend Aebi-Müller, N 512 ff.; dazu, dass sich der Schutzbereich des US-amerikanischen Right to Privacy und des deutschen allgemeinen Persönlichkeitsrechts weitgehend decken, Buchner, 8 – gewährleistet würden namentlich die informationelle Selbstbestimmung, der Schutz vor Überwachung, Verhören und Durchsuchungen sowie der Ehre.

237 Zur Bedeutung des «eigenen Zimmers», gerade für die Frau als Schriftstellerin, Woolf, A Room of one's own, mit dem berühmten Satz auf der ersten Seite des ersten Kapitels: «A woman must have money and a room of her own if she is to write fiction.» — Virginia Woolf, A Room of One's Own, 29. Insofern könnte vom Privaten (eigenes Zimmer als Rückzugsort für selbstbestimmte Handlungen der Frau und Entfaltung ausserhalb der Rolle der Mutter und Hausfrau, hier als Schriftstellerin) im Privaten (im häuslichen Bereich als Sphäre der Frau und Mutter gemäss bürgerlichen Leitvorstellungen) des Privaten (als Gegensphäre des staatlichen Bereichs) gesprochen werden.

238 Simitis, in: Schlemmer (Hrsg.), 67 ff., 70 f.

der beiden Autoren bei Lichte betrachtet ebenso auf eine Forderung ab, wonach eine *obere Schicht* «in Ruhe zu lassen» und von den übrigen Gesellschaftsschichten abzugrenzen sei: auch, indem keine Informationen zwischen den Schichten zur Befriedigung der Neugierde der unteren Schichten transferiert werden sollten. *Informationsflüsse resp. deren Unterbindung zeigen sich als Instrument zur Segregation* der Gesellschaft.[239] Die Unterbindung von Informationsflüssen ist damit eine effiziente Strategie zur Abgrenzung nicht nur von Individuen, sondern auch von Gesellschaftsstrukturen und -systemen.

4. Privatheit und Kommerzialisierung – der Wert von Informationen

Die Relevanz gesellschaftlicher Strukturen innerhalb des Privatheitsschutzes wird 171
in einem zusätzlichen Aspekt der Studie von Warren/Brandeis deutlich. Die Autoren thematisieren eine *Kommerzialisierung des «Privaten» durch die Regenbogenpresse*. Sie beschreiben damit die *Kollision des ökonomischen Kontextes mit dem familiären und persönlichen Lebensbereich*, indem die *Medien* – anstatt die Aufgaben und Ziele einer «seriösen Sachpresse» zu erfüllen – *primitive Unterhaltungsbedürfnisse* befriedigen würden. Bis heute bildet die Vermarktung von Lebensgeschichten von Eliten und Prominenten ein Kernthema juristischer Auseinandersetzungen zum Persönlichkeitsschutz, Immaterialgüter-, Informations- sowie Datenschutzrecht.[240] Der Kommerzialisierung eines – in Abgrenzung zum Eigentumsrecht – zusehends ideell gedachten Rechtsgutes, der Persönlichkeit, wurde allem voran in Deutschland ab Ende des 20. Jahrhunderts beachtliche Aufmerksamkeit geschenkt.[241]

Einer historischen Betrachtung, welche die faktische Entwicklung der Kommer- 172
zialisierung von Personen und Informationen vor Augen führt, fällt eine bestimmte Person in den Blick: Erasmus von Rotterdam. Er ist ein frühes Beispiel für die Kommerzialisierung der eigenen Person; Vervielfältigung und

239 Die Diskriminierung qua Personendatenverarbeitungen ist bis heute gerade im Zusammenhang mit AI und Profiling ein bedeutsames Datenschutzthema, vgl. m. w. H. Heuberger, N 29; zum Problem der Hierarchisierung aufgrund von Profiling m. w. H. auch Schwartz, Wis. L. Rev. 2000, 743 ff., 747.

240 Vgl. grundlegend und einleitend zur Bedeutung des Ehrenschutzes und des 19. Jahrhunderts Ladeur, Ökonomie der Aufmerksamkeit, 11 ff.; Ahrens, *passim*; Büchler, AcP 2006, 300 ff.; Dies., in: Honsell/Portmann/Zäch/Zobl (Hrsg.), 177 ff.; Emmenegger, in: Gauch/Pichonnaz (Hrsg.), 209 ff.; nicht spezifisch mit Blick auf Prominente, sondern allgemeiner zur Kommerzialisierung von Identitätsmerkmalen Ahn Byung, 20 ff.; Beuter, 63 ff.; Meyer, 9 ff.; Biene, 3 ff.; vgl. auch die zahlreichen Beiträge von Beuthien; zu kommerziellen Interessen an Politikerpersönlichkeiten Ehmann, AfP 2007, 81 ff.; dazu, dass das Informationsrecht um die Frage der Zuordnung von Rechten an Informationen versus den freien Zugang zu diesen kreist, Hoeren, 9.

241 Büchler, AcP 2006, 300 ff., 302.

Verbreitung seines Bildnisses und seiner Schriften am Ende des 15. Jahrhunderts trugen dazu bei, dass sich ein eigentlicher Nimbus um seine Person aufbaute.[242]

173 Durch die Beschäftigung mit dem Plädoyer von Warren/Brandeis wird bereits für frühere Zeiten offensichtlich, dass Informationen mit Personenbezug grosse *ökonomische Relevanz* haben.[243] Bereits ihr Beitrag am Ende des 19. Jahrhunderts hatte sich der Frage zu widmen, wie das Recht nicht nur auf technische Entwicklungen (Möglichkeit des massenhaften Druckes und der Verteilung von Unterhaltungspresseerzeugnissen) umgeht, sondern auch mit dem Anreiz der wirtschaftlichen Verwertung persönlicher Informationen. Dass Informationen, die sich auf Personen beziehen, einen wirtschaftlichen Gehalt und Wert haben ist – wie gezeigt – keineswegs erst ein Phänomen dieser Tage. Informationen haben in unzähligen Facetten *wirtschaftliche Bedeutung*.[244]

174 Beim Zusammenspiel zwischen *Informationen und Gütern, namentlich Geld* stehen zwei Mechanismen im Vordergrund: Zum einen dienen Informationen indirekt zur Generierung von (Geld-)Werten – so gezeigt anhand des Märchens von Ali Baba zu Beginn dieses Teils. Der Zugriff auf ein Gut erfolgt über eine Information (quasi der informationelle Schlüssel, der Code). Zum anderen können Mechanismen beschrieben werden, bei denen Informationen zum Gut transformiert werden (so wie beim verwerteten «Gossip» der Sensationspresse). Dass Informationen an und in sich Werte tragen («Informationen als Güter») resp. die Kontrolle über Informationsflüsse und (monetäre, aber auch nicht monetäre) Werte sichern können, ist folglich keineswegs ein Phänomen des digitalen Zeitalters.[245] Das Phänomen soll an dieser Stelle in diesem historischen Teil um einige weitere Fragmente angereichert werden:

175 Personenregistrierungen erfolgten schon früh nicht nur zur Wahrnehmung *fiskalischer Interessen*, sondern ermöglichten auch anderweitig die Füllung der *Staatskassen*: Dürer beispielsweise beklagte die *Gesundheitsbriefe*, die nach seinem Dafürhalten weniger der Seuchenbekämpfung, sondern vielmehr dazu dienten, den Menschen das Geld aus der Tasche zu ziehen. Auch weitere Dokumente wie Geleitbriefe oder Pilgerscheine kosteten Geld.[246]

242 Groebner, 188; unter Integration einer Geschichte der Persönlichkeitsvermarktung grundlegend ebenso zur Kommerzialisierung der Persönlichkeit im 20. Jahrhundert Seemann, 33 ff.

243 Vgl. vertiefend dritter Teil, VII. Kapitel, B.1. und B.2., wo diese Schrift sich mit zwei faktischen Herausforderungen – Kommerzialisierung sowie technischer Fortschritt – auseinandersetzt, mit denen das Datenschutzrecht konfrontiert ist.

244 Vertiefend zur Kommerzialisierung dritter Teil, VII. Kapitel, B.2.

245 Vgl. zur Herausbildung einer eigenständigen Industrie dritter Teil, VII. Kapitel, B.; zum monetären Wert des Privaten statt vieler Dörflinger, 116 ff.

246 Groebner, 115 ff. und 127 ff.; zum Aufbau einer administrativen Ordnung mit unzähligen Registern, Listen und Dokumenten auch von Lewinski, in: Arndt/Augsberg (Hrsg.), 196 ff., 202 f.

176 Es waren keineswegs nur die obrigkeitlichen Stellen, die in diesem Zusammenhang gutes Geld verdienten: Gutenberg und seine beiden Mitgesellschafter hatten ca. 30'000 in Blei geprägte Pilgerzeichen hergestellt und erzielten mit dieser Massenfabrikation beträchtlichen kommerziellen Erfolg.[247] Die Pilgerzeichen dienten dem Nachweis, dass die städtischen Gebühren entrichtet worden waren. An den Stadttoren wurden den Fuhrleuten Marken als Quittung für Torgelder und Gebühren ausgestellt. Nur gegen Abgabe der Marke durften sie die Stadt wieder verlassen.

177 Zur Eintreibung von Geldforderungen kamen die aus dem 14. Jahrhundert bekannten Schuldnerlisten zum Einsatz, wobei die juristischen Identifikationsstrategien auch zu diesem Zweck selbst über grosse Entfernungen wirksam wurden.[248] Eine bemerkenswerte Zweckänderung, die sich im Informationstransfer aus dem Strafverfolgungskontext in den privaten Bereich vollzieht, wird für das 18. Jahrhundert beschrieben: Gaunerlisten dienten eines Tages nicht mehr nur der Auffindung von Übeltätern. Vielmehr wurden sie als aufregender Lesestoff auch an Private verkauft.[249]

178 Rund um die bereits vorgestellte mediale Hauptfigur – den Diener – wurde die Entwicklung einer *spezifischen Logik der Ökonomie* nachgezeichnet. Auf dem Markt wurden bereits vor Jahrhunderten neben Gemüse und weiteren Waren auch Informationen feilgeboten.[250] Offensichtlich hatte die *Diskretion der Bediensteten* einen nicht minder hohen (Stellen-)Wert für die Herrschaften.

179 Als Konsequenz konnte mit der *Rekrutierung und Vermittlung von Informationen über treue Bedienstete Geld* verdient werden: Gesindevermittlungsagenturen waren in London ab dem 18. Jahrhundert fest etablierte Institutionen; für Deutschland ist das Gesind-Vermietungscomptoir in Berlin überliefert.[251] Solche Vermittlungsagenturen wurden auch als «Verdinger/Hindinger» bezeichnet, womit das stellensuchende Individuum selbst sprachlich vom Subjekt in ein Objekt überführt wurde, das seinen Herrschaften mechanisch zur Hand gehen sollte.[252] Die Hindinger erhoben Vermittlungsgebühren, womit das ökonomische Interesse zugleich ein Interesse inkludierte, dass das vermittelte Arbeitsverhältnis nicht zu lange währte. Entsprechend wurde der fragliche Vermittlungskanal eher für das weniger qualifizierte Gesinde gewählt, wohingegen die wichtigen Bediensteten in aller Regel über Mund-zu-Mund-Propaganda vermittelt wurden. Letztere waren

247 Groebner, 44.
248 Ders., 51.
249 Ders., 164.
250 Zum Ganzen Krajewski, 176 f.
251 Ders., 183.
252 Ders., 185.

in Netzwerken organisiert, in denen ein reibungsloser Informationsaustausch gewährleistet werden sollte.[253]

180 In den *frühneuzeitlichen Adressbüros* wurden allerdings keineswegs bloss Bedienstete vermittelt, sondern auch Ärzte und ganz allgemein Arbeitssuchende, Waren, Kapital und Immobilien.[254] Diese Adressbüros in Europa im 17. resp. 18. Jahrhundert werden als erste Suchmaschinen und gewissermassen als Vorläufer von Google beschrieben, so das Bureau d'Adresse in Paris, das intelligence oder registry office in London, das Fragamt in Wien usf. Die Erhebung, Organisation und Koordination von Informationen und Wissen, Angebot und Nachfrage wurde institutionalisiert, professionalisiert und spezialisiert.[255]

181 Das von Renoudet bereits 1630 in Paris gegründete Vermittlungsbüro war Pfandbüro, Vermittlungsbüro für Ärzte oder Apothekerinnen sowie Verkaufsagentur in einem.[256] So konnten sich beispielsweise potentielle Käuferinnen resp. Verkäufer zwecks Angebot resp. Nachfrage einer Ware gegen eine Vermittlungsgebühr ins Register eintragen lassen resp. gegen Gebühr einen Auszug erhalten. Ein solcher Auszug informierte über Ort und Person, wo die jeweilige Nachfrage gedeckt werden konnte.[257] Besagte Auskunfteien illustrieren nicht nur die frühe Kommerzialisierung von (personenbezogenen) Informationen, indem die Betreiber mit der Informationsvermittlung wirtschaftliche Gewinne erzielten,[258] weshalb man durchaus von einer Informationsindustrie sprechen könnte. Sie dienten gleichzeitig dem Auf- und Ausbau von Handels- und Arbeitsmarktbeziehungen. Von der Entwicklung jener lukrativen Geschäftspraktiken wollten wiederum die obrigkeitlichen Stellen profitieren. Entsprechend bedurfte es für die Einrichtung eines Adressbüros in aller Regel eines Privilegs resp. einer gebührenpflichtigen Konzession.[259] Anhand des Aufbaus dieser Adressbüros und Auskunfteien zeigt sich, dass die Kommerzialisierung von Informationen mit Personenbezug kein neues Phänomen ist.[260] Bereits früh beginnt sich hier eine Betrachtungsweise

253 Krajewski, 183, wobei Dienstmädchen meist der Gemüsestand als Informationsforum diente und sich dort ausgetauscht wurde, wo man sich besser nicht verdingen sollte.
254 Herwig/Tantner, 20 f.
255 Vgl. Tantner, Adressbüros, 20 ff., 49 ff., 130 ff.
256 Ders., a. a. O., 34 ff.; zum Adresshandel heute, der datenschutzrechtlich wiederholt kritisiert wurde und der die expansive Kraft ökonomischer Rationalitäten veranschaulicht, vgl. dritter Teil, VII. Kapitel, 2.
257 Herwig/Tantner, 21.
258 Vgl. zu den Gebühren für Eintragungen Tantner, Adressbüros, 30 und 49.
259 Ders., a. a. O., 40 ff.; wie bereits für die Verdingbüros beschrieben, galt auch hier, dass die öffentliche Hand ebenso in den Geldtopf greifen wollte. Entsprechend bedurfte es für die Einrichtung von Adressbüros eines Privilegs, das zunächst in Renoudets Familie verblieb, alsdann aber gegen Entgelt verpachtet wurde.
260 Eine lebhafte Schilderung der frühen Partnerschaftsvermittlung findet sich etwas später im Roman von Alice Berend, Die Bräutigame der Babette Bomberling; zur Optimierung auch des Privaten «Liebe aus Nullen und Einsen. Der Computer als Kuppler: Das ist keine Erfindung der Internetära. Seit den 1950er Jahren versucht man, das Glück zu programmieren», NZZ vom 10. Juli

zu etablieren, wonach *Information als Quasi-Objekt, das zwischen Subjekten transferiert wird,* wahrgenommen wird.[261]

Gleichwohl findet sich auch die *kontextuelle Dimension* des ökonomischen The- 182
mas adressiert, insb. bei Warren/Brandeis.[262] Die Autoren beklagten, dass die Yellow Press Informationen aus den *heiligen Zirkeln des privaten Lebens* einzig und allein aus *wirtschaftlichem Profitstreben* und zur Befriedigung der primitiven Neugier der Allgemeinheit (Gossip) verbreiten würde.[263] Zwar richtete sich ihr Fokus auf die Ableitung und Herausbildung eines *subjektiven Rechts,* eines Right to Privacy. In ihrer Analyse wird indes die systemische Herausforderung dergestalt sichtbar, als dass diese als *Kollision des ökonomischen Kontextes mit dem Kontext der privaten Lebenswelt* beschrieben wird. Das Presseerzeugnis zielte gemäss den Autoren gerade nicht darauf ab, ein legitimes öffentliches Informationsinteresse zu erfüllen.

Warren/Brandeis bezogen sich für ihre Ableitung, wonach ein Right to 183
Privacy bereits im Recht angelegt sei, namentlich auf Entwicklungen in Frankreich: Frankreich war das erste Land, das die Privatheit gesetzlich gegenüber der Presse schützte.[264] Mit der *Loi Relative à la Presse* wurde die Veröffentlichung von Fakten aus der «vie privée» in periodisch erscheinenden Medien unter Strafe gestellt. Im deutschsprachigen Raum problematisierte der Preussische Strafrechtler Klein das Thema 1788 mit den Worten:

> «Da es nicht von sonderlichem Nutzen sein kann, Thatsachen aus dem Privatleben eines Menschen auszuheben, und öffentlich zu jedermanns Wissenschaft zu bringen, so wird eine dergleichen Bekanntmachung nicht leicht zu entschuldigen seyn; es ware den, dass ein überwiegender Nutzen für das Publicum zu erwarten ware.»[265]

2018, 36; Auskunfteien, insb. Kreditauskunfteien, wurden immer wieder kritisch vor dem Hintergrund des Datenschutzrechts diskutiert, vgl. hierzu vertiefend dritter Teil, VII. Kapitel, B.2.

261 Zu einer solchen Idee resp. Konzeptionalisierung, der rechtlich namentlich das Eigentumsrecht verpflichtet ist, vgl. dritter Teil, VIII. Kapitel, B.4.

262 Anknüpfend an die Bedeutung von Informationen für den Schutz des Ansehens ist anzunehmen, dass mit der Herabsetzung des Ansehens der gesellschaftliche Fall auch dramatische wirtschaftliche Folgen haben konnte.

263 Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 196; hierzu auch Richards, Vand. L. Rev. 2010, 1295 ff., 1299; interessant Odlyzko, Int. J. Commun. 2012, 920 ff., 925 mit dem Hinweis zum Effekt von Preissenkungen betreffend Zeitungen und dem damit einhergehenden intensivierten Informationsfluss im England des 19. Jahrhunderts; dazu, dass je ungewöhnlicher intime Informationen sind resp. je berühmter die betroffenen Personen sind, desto grösser das mediale Interesse, Harvey, U. Pa. L. Rev. 1992, 2385 ff., 2386 f.; zur Abwägung zwischen Gossip-Begehrlichkeiten und dem Schutz von Prominenten zugunsten der letzteren im Zusammenhang mit dem Verunfallen von Prinzessin Diana vgl. m. w. H. Allen, Harv. L. Rev. Forum 2013, 241 ff., 243.

264 Dazu Warren/Brandeis, Harv. L. Rev. 1890, 193 ff., 214.

265 E. F. Klein, Preussischer Strafrechtler, 1788, zit. nach Balthasar, Fn 56; vgl. zum kommunikationsbezogenen Strafrecht im 19. Jahrhundert Ladeur, Ökonomie der Aufmerksamkeit, 11 ff.; zur Relevanz der Abgrenzung der Unterhaltung von anderen Gehalten verbreiteter Informationen Ders., ZUM 2000, 879 ff., 884 ff.

184 Die «Presse» ist ein *Medium*, das der Informationsvermittlung dient. Allerdings kann diese *Informationsvermittlung ganz unterschiedliche Ziele* verfolgen: Die Verbreitung von «Gossip» zur Generierung von Geld und Befriedigung eines Unterhaltungsinteresses wird anders beurteilt als die Verbreitung von «berichterstattungswürdigen Nachrichten», die gerade für den politischen Kontext und die Demokratie von Bedeutung sind.[266] Beschrieben wird von den Autoren folglich die Kollision einer tief verwurzelten Institution – der private resp. familiäre Lebensbereich – mit dem Profitstreben der Presse und damit dem ökonomischen Kontext, aber auch einer Presse, die dem demokratischen System dient. Die Regenbogenpresse konterkariert scharf eine Presse, die in ihrer Funktion für die Demokratie und unter ebendiesem Titel der Pressefreiheit gelesen wird.[267]

5. Resümee und Überleitung

185 Die vorangehenden Ausführungen lassen sich wie folgt *zusammenfassen*: Gezeigt wurde, dass die *informationelle Erfassung des Menschen* insb. als *Herrschaftstechnologie dient(e)*.[268] Entsprechend kommt Personendatenerfassungen zentrale Bedeutung im Rahmen der Herausbildung obrigkeitlicher resp. staatlicher Institutionen und Systeme zu.

186 Exzessive Herrschaftspraktiken durch informationelle Personenverarbeitungen blieben allerdings nicht ohne Reaktion. Neben Torpedierungen brachte insb. die Anerkennung von Freiheitsrechten, die der invasiven Macht des Staates Schranken setzen sollten, eine *erste Zweiteilung der Welt*: ein *Dualismus*, in dem eine *öffentliche Sphäre im Sinne einer staatlichen Sphäre vom Bereich des Privaten* abgegrenzt wurde. Die *Freiheitsrechte* sind als konstitutiv für die Kategorien des öffentlichen und privaten Bereiches zu qualifizieren.[269] Es geht um die Etablierung eines *ersten Dualismus*.

---

266 Eine Schlüsselfigur zwischen den Bereichen bildet später bekanntermassen die relative und absolute Figur der Zeitgeschichte, anhand der beschrieben wird, inwiefern Informationen zur persönlichen Lebensführung von öffentlichen Figuren von allgemeinem Interesse sind oder nicht, vgl. BGE 127 III 481, E 2.a.; Lüthi, *passim*; kritisch unlängst Zulauf/Sieber, medialex 2017, 20 ff.; zur Unterscheidung von Gossip und berichtwürdigen Tatsachen Richards, Vand. L. Rev. 2010, 1295 ff., 1310 ff.; zur Einordnung der Unterhaltung und zur Staatsfixierung des Bundesverfassungsgerichts auch in seiner Rechtsprechung zum Medienrecht Ladeur, ZUM 2000, 879 ff., 881.

267 Vgl. Buchner, 20 ff.

268 Für unsere Zeit wird dies z. B. beschrieben durch Whitaker, 47 f., mit Blick auf die Überwachung von Gefangenen, die damit diszipliniert werden.

269 Vgl. Rössler, 27 ff.; sie zeigt zunächst, inwiefern für die Zweiteilung zwischen dem öffentlichen Bereich im Sinne des Staates gegenüber eines von seinem Handeln freigehaltenen Bereiches, dem Privatbereich, der Liberalismus und die Freiheitsrechte relevant sind; zum entsprechenden Dualismus von Personendatenverarbeitungen durch den Staat (Bundesbehörden) und Privatpersonen als erstes Strukturmerkmal des schweizerischen DSG zweiter Teil, IV. Kapitel; zur Freiheit und Selbstbestimmung als Kernelemente der absolut geschützten Rechtsgüter und damit auch der Persönlichkeit Ehmann, in: Stathopoulos/Beys/Philippos/Karakostas (Hrsg.), 113 ff., 138 f.

187 Unter dem Titel «Das Private im Privaten» folgte ein genauerer Blick aus einer historischen Perspektive auf den Bereich des Privaten, der jenseits der öffentlichen i. S. v. staatlichen Sphäre liegt. Im Zentrum stand die Entwicklung und Ausdifferenzierung von subjektiven Rechten. Für das *Private im Privaten* wurden schlaglichtartig verschiedene Ursprünge und Ingredienzen beleuchtet. Eine Auseinandersetzung mit dem berühmten Beitrag von Warren/Brandeis war hierbei von besonderem Interesse.

188 Als Quellrecht des Right to Privacy zeigte sich im Artikel von Warren/Brandeis zunächst das *Eigentumsrecht*. Prominent taucht die *räumlich-statische Metapher* des Hauses zur Konstituierung des Privaten auf. Eine solche Symbolisierung zeigte sich schon an früherer Stelle in Redewendungen, aber auch literarischen Erzählungen. Zugleich präsentiert sich das Right to Privacy als ein Recht der Privilegierten und der bürgerlichen Oberschicht, denen auch die beiden Juristen angehörten, die mit ihrem Aufsatz Rechtsgeschichte schrieben. Damit wurde gleichzeitig sichtbar, dass die Entwicklung des Privatheitsschutzes eng mit den Privilegien einer Elite sowie dem Ehrenschutz zusammenhängt.

189 Mit diesen Komponenten eines Right to Privacy untrennbar verbunden ist die *Kategorie der Familie*. Sie gilt bis heute als Kerndimension des Privaten. Das Ideal der bürgerlichen Kleinfamilie geht mit geschlechtsspezifischen Rollenzuweisungen einher: Der häuslich-familiäre Bereich wird der Frau zugewiesen, die Aussenwelt, wo Ehre, Ruhm und Geld zu verdienen waren, dem Mann. Damit lässt sich von einer *zweiten Dichotomie* sprechen, dem Privaten im Privaten.

190 Im Zeitalter von Warren/Brandeis verengte sich der informationsrechtliche Fokus auf den Schutz der subjektiven Rechte. Zwar konzentrierten sich die Autoren auf die deduktive Begründung eines *Individualrechts*, des Right to Privacy als subjektives Recht. Gleichwohl erfolgte in ihrer Analyse die Beschreibung einer Kollision zwischen *Gesellschaftsstrukturen* (zwischen Ober- und Unterschicht) und *Gesellschaftsbereichen resp. Kontexten*, namentlich des *wirtschaftlichen Kontextes mit dem Privat- und Familienleben*. Ausgangslage ihres Beitrages war eine Situation, in welcher die Presse nicht mehr (nur) darauf abzielte, «höherrangige» Informationsinteressen zur Gewährleistung von Rechtsstaatlichkeit, Freiheit und Demokratie umzusetzen. Vielmehr diente die Publikation von persönlichen Informationen einzig der Befriedigung der Neugierde des «einfachen Volkes». Hierfür wurde eine Invasion in die «heiligen Bezirke des persönlichen Lebens» vorgenommen und gleichzeitig eine Quelle für den finanziellen Profit erschlossen, worin die Juristen auch ein Risiko für die allgemeine Moral verorteten. Im Zuge der Entwicklung der Yellow Press war es somit eine *Veränderung des Informationszweckes*, der auf Widerstand stiess. Die Presseunternehmen verfolgten nicht mehr nur das Ziel, die politisch-demokratische Willensbildung zu gewährleisten. Stattdessen handelten sie zusehends im eigenen wirtschaftlichen

Interesse, das vom Unterhaltungsinteresse der Allgemeinheit genährt wurde. Dabei griffen die Presseunternehmen in den privaten Lebensbereich ein, wodurch dieser untergraben wurde.

191 Erneut wurde illustriert, dass Personendaten seit Langem *wirtschaftliche Relevanz* haben, sowohl im öffentlichen als auch im privaten Bereich. Die Kommerzialisierungsbestrebungen der Yellow Press konfrontierten den privaten Bereich in den Augen von Warren/Brandeis in einer Weise, welche die Anerkennung eines Right to Privacy gebiete. Die sich vollziehende Transformation von Informationen in Wirtschaftsgüter durch den Einsatz neuer Techniken und Praktiken – die heute als Hauptherausforderungen für das Datenschutzrecht diskutiert werden – stellte das Recht bereits im 19. Jahrhundert auf die Probe. Noch weiter zurückreichend konnte anhand verschiedener Schlaglichter auf gebührenpflichtige Gesundheitsbriefe, insb. aber die Errichtung sog. Frageämter und die damit geschuldeten Gebühren sowie Konzessionen, gezeigt werden, dass Informationen schon früh wertvolle Güter waren und in bares Geld umgesetzt wurden.

192 Die Emanzipation eines individualrechtlichen Subjektschutzes durch die Anerkennung eines eigenständigen, vom Eigentumsrecht und Ehrenschutz losgelösten Right to Privacy als juristische Antwort auf faktische Entwicklungen (Stichworte Yellow Press und Kommerzialisierung) war unbestritten eine Errungenschaft: Von nun an konnte sich der Einzelne gegen Eingriffe in das Privatleben durch «invasive informationelle Vorgehensweisen», unter Umständen technisch unterstützte Personendatenverarbeitungen, sowohl gegenüber staatlichen Stellen als auch Privatpersonen zur Wehr setzen. Damit war der Weg für die künftigen Entwicklungen gewiesen.

193 An dieser Stelle erfolgt der Sprung in die jüngere Vergangenheit sowie Gegenwart. Nachfolgend geht es vorab um die in gebotener Kürze vorzunehmende Auseinandersetzung mit der Entwicklung der *ersten Datenschutzgesetze*. Solche spezifische Datenschutzerlasse waren die Reaktion auf eine Erkenntnis, wonach das bisherige rechtliche Instrumentarium – für den privaten Bereich, insb. das allgemeine Persönlichkeitsrecht – den faktischen Entwicklungen und namentlich den Fortschritten im Zuge der Informationsverarbeitungstechnologien nicht hinreichend wirksam begegnen konnte.[270]

194 Ein Herzstück der frühen datenschutzrechtlichen Debatte bildete die Frage, ob und wie Normierungen mit Blick auf Personendatenverarbeitungen durch den Staat und durch Private ausgestaltet werden sollen.[271] In der Schweiz war die

270 Vgl. zur Beziehung von Technik und Recht aus allgemeinerer und geschichtswissenschaftlicher Perspektive, wobei die Frage der Technik im Recht zum Kardinalproblem der Moderne erhoben wird, Dommann, SZG 2005, 17 ff., 18; sodann die Beiträge in Ruch (Hrsg.), Recht und neue Technologien; spezifischer Cottier, Forum Europarecht 2018, 25 ff.

271 Zu dieser Diskussion insb. für Deutschland Buchner, 26 ff.

Notwendigkeit einer spezifischen Gesetzgebung mit Regeln für Personendatenverarbeitungen durch Bundesbehörden weit weniger umstritten als diejenige für den privaten Bereich.[272] Gleichwohl wurde für den privaten Bereich ebenso früh der Standpunkt vertreten, dass die basierend auf dem Persönlichkeitsrecht gemäss Art. 28 ZGB entwickelte *Sphärentheorie* keinen hinreichenden Schutz mehr gewähren könne.[273] Die Sphärentheorie geht auf den deutschen Rechtswissenschaftler Hubmann und das 20. Jahrhundert zurück. Sie wurde auch in der Schweiz rezipiert.[274] Die Theorie sollte das so schwer zu definierende Schutzobjekt der Privatheit im Rahmen des Persönlichkeitsschutzes konkretisieren. In diesem Sinne geht es um eine Auslegung im Zusammenhang mit dem Persönlichkeitsschutz. Die Sphärentheorie, die für das 20. Jahrhundert prägend ist, wirkt im 21. Jahrhundert – jeglichem datenschutzgesetzlichem Fortschritt zum Trotz – fort.[275] Sie geht von der Unterscheidung dreier Lebenskreise aus, welche die rechtlich geschützten Persönlichkeitsbereiche voneinander abgrenzen und mit einem jeweils differenzierten Schutzniveau versehen.[276] Den innersten Kreis bildet die sog. Geheim- oder Intimsphäre; diese

> «umfasst darnach Tatsachen und Lebensvorgänge, die der Kenntnis aller andern Leute entzogen sein sollen, mit Ausnahme jener Personen, denen diese Tatsachen besonders anvertraut wurden […].»[277]

Zur Privatsphäre 195

> «gehört der übrige Bereich des Privatlebens; es sind ihr also alle jene Lebensäusserungen zuzurechnen, die der einzelne mit einem begrenzten, ihm relativ nahe verbundenen Personenkreis teilen will, so mit Angehörigen, Freunden und Bekannten, jedoch nur mit diesen. Was sich in diesem Kreis abspielt, ist zwar nicht geheim, da es von einer grösseren Anzahl von Personen wahrgenommen werden kann. Im Unterschied zum Geheimbereich handelt es sich jedoch um Lebenserscheinungen, die nicht dazu bestimmt sind, einer breiteren

272 Vertiefend insofern nachfolgend zweiter Teil, IV. Kapitel, A. und B.

273 Vgl. zu den Grundlagen und Ursprüngen der Sphärentheorie mit Hinweisen auf die Arbeiten von Hubmann aus dem Jahr 1953 für Deutschland und Jäggi für die Schweiz aus dem Jahr 1960 insb. Aebi-Müller, N 408 ff., N 423, N 512 ff.; sodann namentlich auch BGE 97 II 97; zur Sphärentheorie auch Ehmann, in: Stathopoulos/Beys/Philippos/Karakostas (Hrsg.), 113 ff., 141 ff.; zum Ungenügen der Sphärentheorie und insb. Art. 28 ZGB zur Bewältigung der Herausforderungen im Kontext von Personendatenverarbeitungen BBl 1988 II 414 ff., 428 f.; zum Ungenügen des geltenden Rechts als Grund für die Entwicklung eines spezifischen Datenschutzrechts Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 34 ff.; zu Schwächen des Sphärenkonzeptes in Deutschland bereits früh und mit Hinweis auf die Entwicklungen zum Autonomieschutz Schmidt, JZ 1974, 241 ff., 243 ff.; zur Sphärentheorie gemäss Art. 28 ZGB in der Zeit vor dem DSG Page, 213 ff.; zum Recht auf Privatsphäre auch Schrepfer, 31 ff.

274 M. w. H. Aebi-Müller, N 408 ff. und N 512 ff.; nicht spezifisch juristisch zur wirkungsmächtigen «Privatsphäre» Güntner, Privatsphäre, Schriftenreihe der Vontobelstiftung, Zürich 2011.

275 In dieser Arbeit wird an mehreren Stellen sichtbar gemacht werden, inwiefern das Konzept selbst im DSG nach seiner Totalrevision fortwirkt, obschon die Datenschutzgesetze ihre Defizite überwinden wollten.

276 Vgl. insb. BGE 97 II 97 mit Hinweis auf das einschlägige Schrifttum und insb. die Beiträge von Jäggi, Hubmann, Grossen und Hotz; BBl 1988 II 414 ff., 428 f.

277 BGE 97 II 97, E 3.

> Öffentlichkeit zugänglich gemacht zu werden, weil die betreffende Person für sich bleiben und in keiner Weise öffentlich bekannt werden will.»[278]

196 Die Gemein- oder Öffentlichkeitssphäre umfasse dagegen

> «Tatsachen [, die] von jedermann nicht nur ohne weiteres wahrgenommen, sondern grundsätzlich auch weiterverbreitet werden dürfen […].»[279]

197 Das Ungenügen einer im (allgemeinen) Persönlichkeitsschutz angelegten Sphärentheorie wurde im Zuge des 20. Jahrhunderts immer deutlicher. Entwickelt und erlassen wurden die ersten spezifischen Datenschutzgesetze. Die Schweiz nahm in dieser *ersten datenschutzgesetzlichen Entwicklungsetappe keine Vorreiterrolle* ein. Im Gegenteil – sie setzte aufgrund einer «élaboration pénible» als eines der letzten Länder in Europa ein allgemeines Datenschutzgesetz auf Bundesebene in Kraft.[280] Im Rahmen der jüngsten kontinentaleuropäischen datenschutzrechtlichen Neuerungswelle wiederholte sich diese (datenschutzrechtliche) Positionierung und Geschichte: Erneut geriet die Eidgenossenschaft ins Hintertreffen, weil die Verabschiedung der Totalrevision zeitlich immer wieder nach hinten verschoben und damit teilweise um einen sog. Angemessenheitsbeschluss, vgl. Art. 45 DSGVO, gebangt wurde. Die nationalrätliche Differenzbereinigung fand in der Frühjahrssession 2020 statt. Am 25. September 2020 wurde die Totalrevision des DSG vom Parlament verabschiedet. Das Inkrafttreten ist mittlerweile auf 2023 festgelegt. Doch bevor über eine Charakterisierung anhand dreier Strukturmerkmale auf das DSG in seiner noch geltenden Form wie auch nach Totalrevision eingegangen und damit der Fokus auf die datenschutzrechtliche Gegenwart und Zukunft gerichtet wird, nochmals eine kurze Rückblende in die Vergangenheit: auf die Zeit, in der die ersten Datenschutzgesetze entwickelt wurden.

C. Entstehung der ersten Datenschutzerlasse

198 Die *datenschutzrechtlichen resp. -gesetzlichen Entwicklungen* sind Reaktionen auf die Fortschritte der Datenverarbeitungs- und Kommunikationstechnologien, wie sie durch den *Computer* möglich und symbolisiert werden.[281] An dieser Stelle ist der Name des Computerpioniers Konrad Zuse zu nennen, der die erste

278 BGE 97 II 97, a. a. O.
279 BGE 97 II 97, a. a. O.
280 Zur wechselvollen Geschichte der Arbeiten zum ersten DSG auch Kleiner, in: Brem/Druey/Kramer/Schwander (Hrsg.), 397 ff., 397 f.
281 Simitis, Symposium, 1 ff., 1; Ders. zu den Nutzungsmöglichkeiten elektronischer Anlagen 1970 mit seiner Schrift zur Informationskrise des Rechts und Datenverarbeitung; vgl. für das Schweizer DSG Belser, in: Datenschutz-Forum Schweiz (Hrsg.), 1 ff., 2; zur Geschichte des Informationsrechts als Rechtsinformatik, dem Computerrecht sowie dem Recht der neuen Medien vgl. Hoeren, 12 ff.; zur Informatik, die das Recht herausfordert, Schweizer, digma 2003, 58 ff.; in drei Etappen wird der Übergang vom Privatheitsschutz zum Datenschutzrecht beschrieben von Cottier, SRIEL 2016, 255 ff., 257 ff.

Rechenmaschine entwickelte. Als Mutterland der Computertechnologien gelten die USA und ebenda das Silicon Valley.

199 Die besagten technologischen Entwicklungen lösen erste Debatten über die Notwendigkeit des Schutzes von Personen und Daten aus. Drei Episoden trugen zur steigenden Aufmerksamkeit in der amerikanischen Öffentlichkeit bei:[282] Erstens war der Wahl von Präsident John F. Kennedy im Jahr 1961 eine über viele Jahre hinweg vorgenommene, rechnergesteuerte Analyse des Wählerverhaltens vorausgegangen. Zweitens scheiterte der Plan der US-Regierung unter Kennedy im Jahr 1965, ein nationales Datenschutzzentrum zu errichten, am Widerstand des Kongresses. In diesem hätten sämtliche Bürgerinnen und Bürger registriert werden sollen, womit dem Staat ein umfassendes Informationssystem zur Verfügung gestanden hätte. Die Diskussion um den Schutz des Menschen und seiner Privatsphäre wurde indes, drittens, durch eine andere Praxis wesentlich angetrieben: Es waren Presseberichte darüber, dass computerbasierte Kreditvergaben auf fehlerhaften Berechnungen basierten und infolge davon zu Unrecht als kreditunfähig Eingestuften der Strom oder das Wasser abgestellt wurde.[283]

200 Der *Ursprung* der Diskussionen rund um eine datenschutzrechtliche Regulierung wird folglich in den *USA der 1960er Jahre* verortet.[284] In den USA wurde alsdann der *Federal Privacy Act* im Jahr 1974 in Kraft gesetzt, der Prinzipien zur *fairen Personendatenverarbeitung* durch die Bundesbehörden vorsieht. Die Bundesstaaten setzten ihrerseits entsprechende Erlasse in Kraft.[285] Der Fokus der ersten Datenschutzgesetzgebungen richtete sich auf die Personendatenverarbeitungen durch den *Staat* – so auch wenig später in Kontinentaleuropa.[286]

201 Die Verarbeitung personenbezogener Informationen war, wie gezeigt, seit jeher eine *Herrschaftsmethode* und wurde zur Konsolidierung staatlicher Macht nutzbar gemacht. Die Abkehr von den Karteikarten und die Hinwendung zur automatischen Datenverarbeitung mittels *staatlicher Grossrechenanlagen* eröffnete

282 M. w. H. Schiedermair, 42; vgl. zu den Anfängen der Entwicklung der Computertechnologien in den USA und den hier beginnenden juristischen Auseinandersetzungen Bull, Computer, 73 ff.

283 Vgl. zum Ganzen m. w. H. Schiedermair, 42; zu skandalösen Missständen im Kreditwesen in den USA als Ursprung für die Datenschutzdiskussion in den 1960er Jahren Fiedler, in: Podlech/Steinmüller (Hrsg.), 179 ff., 180; vgl. die Hinweise auf die Vorläufer in Gestalt der Schuldnerlisten erster Teil, II. Kapitel, A.; vertiefend zu den Kreditauskunfteien im Kontext der expansiven Tendenzen ökonomischer Rationalitäten dritter Teil, VII. Kapitel, B.2.

284 Vgl. Buchner, 7; Garstka, in: Schulzki-Haddouti (Hrsg.), 49 f.; zum weiteren Paradigmenwechsel mit seiner Abkehr von diesen staatlichen Grossrechnern zu Kleinstcomputern Rudin, digma 2001, 126 ff., 126.

285 Buchner, 11; vgl. den Ansatz der Anerkennung der fair information practices spezifisch für das Internet Schwartz, Wis. L. Rev. 2000, 743 ff., 745 ff.

286 Für Deutschland Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff.; für die USA Nissenbaum, 1; für die Schweiz Bründler, SJZ 89, 129 ff., 129; zur automatisierten Verwaltung auch Simitis, Informationskrise, 57 ff.; zu den Entwicklungen in Kontinentaleuropa Evans, Am. J. Comp. L. 1981, 571 ff.; Fiedler, in: Podlech/Steinmüller (Hrsg.), 179 ff., 181.

ganz neue Dimensionen der Personendatenerfassungen.[287] Zugleich beanspruchte der Staat als Sozial- und Wohlfahrtsstaat, zwecks Steuerung seiner Handlungen und Massnahmen, mehr denn je auf die weitgehende Erfassung seiner Bürgerinnen und Bürger angewiesen zu sein. Der Staat als Machthaber ist es, der, ab den 1960 resp. 70er Jahren informationstechnologisch aufgerüstet, eine Art Orwellsches «Big Brother»-Syndrom auslöste.[288] Ausgangspunkt datenschutzrechtlicher Regulierungen ist folglich der *Schutz des Bürgers vor der massenhaften Informationsverarbeitung durch den Staat*.[289]

202 In Europa nahm *Deutschland eine Vorreiterrolle* in Bezug auf die Entwicklungen des Datenschutzrechts ein, wobei gerade auch das Bundesverfassungsgericht markante Impulse gab.[290] Insofern ist vorab auf den *Mikrozensus-Entscheid* aus dem Jahr 1969 hinzuweisen, der einen ersten richtungsweisenden Anstoss für die Entwicklung des Datenschutzrechts im öffentlichen Bereich gab.[291] Die Anleihen des Urteils aus der historischen und hierbei namentlich der US-amerikanischen Argumentation zum Privatheitsschutz sind unverkennbar: Das Gericht hält im Rahmen der Überprüfung der Verfassungsmässigkeit einer statistischen Bevölkerungserhebung fest, dass

> «dem Einzelnen um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum" verbleiben muß, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit geniesst" […].»[292]

203 Vonseiten des Gesetzgebers war es *das Bundesland Hessen*, das 1970 ein erstes Datenschutzgesetz unter ebendieser Bezeichnung erliess.[293] Verankert wurden darin Vorgaben für die Datenbearbeitung durch die Landesverwaltung. Es folgte 1974 Rheinland-Pfalz mit seinem Datenschutzgesetz, das sich gemäss der Kompetenzausscheidung ebenso auf die Datenbearbeitung durch öffentliche Stellen auf Länderebene konzentrierte.

204 Wie in Deutschland wurde ebenso in der *Schweiz* das erste Datenschutzgesetz nicht auf Bundesebene geschaffen. Vielmehr war es der Kanton *Genf*, der 1976

287 Hierzu Vesting, in: Ladeur (Hrsg.), 155 ff., 165.
288 Bründler, SJZ 1993, 129 ff., 129; m. w. H. Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 4; für Deutschland Vesting, in: Ladeur (Hrsg.), 155 ff., 163; Forstmoser, digma 2003, 50 ff., 51; zu dieser (unzutreffenden) Metapher auch Solove, Stan. L. Rev. 2001, 1393 ff., 1396 ff.
289 Zur Brisanz des Staatsschutzes statt vieler Nabholz, in: Schweizer (Hrsg.), 1 ff., 5; Vischer, in: Datenschutz-Forum Schweiz (Hrsg.), 109 ff.; zur Staatszentriertheit des Datenschutzrechts in Deutschland Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff.; Buchner, 27; allgemein zu dieser Ausrichtung der ersten Datenschutzgesetze Mayer-Schönberger, 113 f.
290 Die hohe Sensibilität für den Datenschutz in Deutschland wird auch mit den Erfahrungen der beiden totalitären Überwachungsstaaten in Nazi-Deutschland sowie der DDR erklärt, vgl. Schaar, 27 und 34 f., mit Hinweis auf den Einsatz der durch IBM entwickelten Lochkarten durch das NS-Regime.
291 Dazu Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff.
292 BVerfGE 27, 1 ff., 6 f.
293 Hierzu Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 1.

als erstes Gemeinwesen im Rahmen seiner gesetzgeberischen Kompetenzen ein Datenschutzgesetz für die kantonalen Behörden erliess. Auf Bundesebene gab es in der Schweiz ab 1971 mehrere Vorstösse mit dem Ziel einer Spezialgesetzgebung zum Datenschutz, die sich auf den öffentlichen Bereich bezogen.[294] Die erste Motion war von Nationalrat Bussey ausgegangen, der eine Gesetzgebung verlangte, die den *Bürger und dessen Privatsphäre gegen missbräuchliche Datenverarbeitung* schütze. Kurt Furgler zielte in der Folge als Antwort und ersten Schritt auf eine Bundesdatenschutzverordnung ab, die sich auf die Datenbearbeitung in der *Bundesverwaltung* konzentrieren sollte. Ein im Frühling 1976 vorgelegter Verordnungsentwurf konnte allerdings nicht verabschiedet werden. Erst am 16. März 1981 erging eine Richtlinie zur Datenbearbeitung in der Bundesverwaltung.[295] Der Fokus der ersten Datenschutzerlasse liegt in der Verhinderung *missbräuchlicher Verarbeitungen* personenbezogener Daten durch den *Staat*. Sie werden als *Datenschutzgesetze der ersten Generation* bezeichnet.[296]

205 Datenschutzgesetzgebungen, die sowohl den öffentlichen als auch den privaten Bereich erfassen, werden als jene der *zweiten Generation* beschrieben.[297] Schweden hatte ein solches Datenschutzgesetz bereits 1973 in Kraft gesetzt.[298] Auf Bundesebene erliess Deutschland 1977 nach mühevollen Diskussionen als zweites Land der Welt ein Bundesdatenschutzgesetz.[299] Es regelte ebenso die Datenverarbeitung durch Private.

206 In der Schweiz setzte die Auseinandersetzung mit dem Datenschutz und seiner Regulierung in den 1970er Jahren ein. Die Diskussionen wurden von einer wissenschaftlichen Thematisierung begleitet, die massgeblich vom amerikanischen und deutschen Geschehen und Diskurs beeinflusst war.[300] Gleichzeitig wurde das Land zu jener Zeit von der Cincera-Affäre erschüttert:[301] FDP-Nationalrat Cincera hatte 1976, wenn auch in selbstgestelltem politischem Auftrag und als Privatperson, sowohl privaten Unternehmen als auch Behörden Informationen über linksstehende Personen und Gruppierungen zugespielt. Ziel dieser Aktionen war, diesen als «politisch Subversive» denunzierten Personen den Zugang zu politischen Ämtern und privatwirtschaftlichen Stellen zu verwehren. Die

294 Dazu Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 12 ff.
295 Danioth, in: Schweizer (Hrsg.), 9 ff., 10.
296 Mayer-Schönberger, 113 f.; vgl. für Schweden als gesetzgeberischer Vorreiter mit der Frage, wie staatliche Überwachung kontrolliert werden könne, Flaherty, 104; Bäumler sieht in der anfänglichen Fokussierung auf den «Täter Staat» ein schweres Defizit der damaligen Lösungen, Interview vom April 2009, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/baeumler/index.html> (zuletzt besucht am 30. April 2021); zu den Entwicklungen des Datenschutzrechts mit den Argumentationsmustern m. w. H. auch Boehm, 19 ff.
297 Mayer-Schönberger, a. a. O.; Flaherty, a. a. O.
298 Flaherty, 104.
299 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 1.
300 Vgl. Forstmoser, SJZ 1974, 217 ff.
301 Belser, in: Datenschutz-Forum Schweiz (Hrsg.), 1 ff., 2.

Cincera-Affäre gilt als Vorläufer des Fichenskandals von 1989, welchen die Schweiz mit dem Titel «Schnüffelstaat» in ihre eigene Geschichte eingehen liess: Die Bundesanwaltschaft hatte rund 900'000 Karteikarten über Personen und Organisationen angelegt, mit vergleichbarer Zielsetzung wie in der Cincera-Affäre. Ausgerechnet die Schweiz, die als «Musterknabe» der Demokratie beschrieben wird, dokumentiert für die moderne Geschichte, dass «staatsschnüffelnde Aktivitäten» mit invasiver und extensiver Bürgerkontrolle bereits ohne hochautomatisierte Datenverarbeitungstechnologien möglich waren.[302]

207 Zusätzlich zu diesen brisanten Vorkommnissen wurde die Verabschiedung eines Datenschutzgesetzes von internationalen Entwicklungen angetrieben: Die informationstechnologischen Fortschritte hatten bereits dazumal zu stark intensivierten wirtschaftlichen Aktivitäten geführt, mit einer zusehenden Verdichtung nicht nur der staatlichen Kooperationen. Entsprechend bemühte man sich um völkerrechtliche Regelungen für den internationalen Datenschutz. Am weitreichendsten und bedeutsamsten war das Europarat-Übereinkommen Nr. 108 vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Der Erlass eines Datenschutzgesetzes durch die Schweiz sollte die Ratifikation besagten Übereinkommens ermöglichen.[303] Die Konvention wurde unlängst geändert, wobei die Anpassungen des DSG mittels Totalrevision von den internationalen Entwicklungen (namentlich auch der Verabschiedung der DSGVO) angestossen wurden.[304] Die Teilhabe an einem grenzüberschreitenden Markt, der mit einem grenzüberschreitenden Transfer von Personendaten einhergeht, gab seit jeher Anlass, harmonisierte datenschutzrechtliche Vorgaben zu erlassen.

208 Während die Notwendigkeit einer Datenschutzgesetzgebung für die Personendatenverarbeitung durch *Bundesbehörden* weitestgehend anerkannt war, zeigte sich ein anderes Bild betreffend den privaten Bereich. Für den Schutz der Person vor Datenbearbeitungen durch Private wurde in den 1970 resp. 1980er Jahren auf Art. 28 ZGB zurückgegriffen. Im Rahmen der Erwägungen zur Änderung von Art. 28 ZGB schlug bereits die insofern eingesetzte Expertenkommission unter Lüchinger in ihrem Vorentwurf einen lit. k vor, der in minimaler Weise Datenschutzbelange aufgreifen sollte. In der Folge erarbeitete die nach den Vernehmlassungsergebnissen eingesetzte Expertenkommission unter Tercier weiterfüh-

302 Vgl. hierzu Aiolfi, NZZ vom 28. März 1990, 65; auch Deutschland kannte Datenskandale: Legendär insofern die Berichte des Journalisten Günter Wallraff, der sich inkognito in Callcentern hatte anstellen lassen, woraufhin eine Welle der Empörung durch die Öffentlichkeit ging, vgl. m. w. H. Bull, ZRP 2008, 233 ff., 233.

303 BBl 1988 II 414 ff., 423 f.

304 Zur Stärkung des Datenschutzes, veranlasst nicht nur von den technologischen Entwicklungen, sondern namentlich auch den rechtlichen Entwicklungen auf supra- resp. europarechtlicher Ebene, vgl. <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.htm> (zuletzt besucht am 20. September 2021).

rend mehrere ZGB-Bestimmungen, welche den Datenschutz im Privatrecht gewährleisten sollten. Allerdings wurde der Schluss gezogen, dass das Anliegen im Rahmen des ZGB nicht zu bewältigen sei.[305] Was folgte, war ein über zwanzig Jahre andauerndes Ringen um die erstmalige Verabschiedung des eidgenössischen Datenschutzgesetzes, das Vorgaben sowohl für die Personendatenverarbeitung durch Bundesbehörden wie auch für Private vorsehen wollte.[306] Ebendiesem Gesetz – allerdings aus einer kontextuellen und systemischen Betrachtung – widmet sich diese Studie. Entsprechend werden auch spezialgesetzliche Erlasse eine spezifische Bedeutung für diese Untersuchung haben. Die Untersuchung beschränkt sich indes nicht auf das Schweizer Recht, sondern integriert Vorgaben und Entwicklungslinien namentlich in der EU, aber auch des US-amerikanischen Rechts. Von besonderem Interesse werden sodann Art. 8 EMRK und die Rechtsprechung des EGMR sein.

209 Um die regulatorische Landkarte übersichtshalber zu vervollständigen, seien am Rande zwei weitere für die Schweiz relevante Felder erwähnt: *Erstens* sind entsprechend der verfassungsmässigen Kompetenzausscheidung in der Schweiz seit jeher die *Kantone* zum Erlass *kantonaler Datenschutzerlasse* bezüglich der Normierung von Personendatenverarbeitungshandlungen durch die kantonalen Behörden zuständig. Solche Vorgaben z. B. im Kanton Zürich finden sich im sog. IDG, dem Gesetz für die Information und den Datenschutz, das seit dem 12. Februar 2007 in Kraft steht. Es regelt allgemeine Grundsätze im Umgang mit Informationen sowie solche im Umgang mit Personendaten. Gemäss § 30 ff. IDG gibt es die Funktion eines kantonalen Datenschutzbeauftragten, den zahlreiche weitere Kantone ebenso in ihren kantonalen Datenschutzerlassen vorsehen. Damit wird sowohl im DSG als auch in den kantonalen Datenschutzgesetzen eine spezifische Funktion installiert, die über die Einhaltung des jeweils einschlägigen Datenschutzgesetzes zu wachen hat. Die kantonalen Datenschutzbeauftragten haben, wie der EDÖB, die Debatte um den Datenschutz wesentlich mitgestaltet. Die föderalistische Struktur in der Schweiz sowie die verfassungsmässige Kompetenzausscheidung prägen das Datenschutzrecht. Für eine Regelung der Personendatenverarbeitung durch Private sowie durch Bundesbehörden war seit jeher der Bund kompetent.[307] *Zweitens* geht mit der Entwicklung von Datenschutzerlassen eine Ausbildung von sog. Öffentlichkeitsgesetzen einher. Beide Typen von Gesetzgebungen dienen der Kontrolle und Rückbindung staatlicher Macht, wie sie über Informationsverarbeitungen und namentlich Verarbeitungen von Personendaten möglich werden. Die Öffentlichkeitgesetze zielen darauf ab, Transparenz in Bezug auf staatliches und insb. verwaltungsrechtliches Handeln zu gewährleisten,

305 Zum Ganzen Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 17.
306 Vertiefend hierzu sogleich zweiter Teil, IV. Kapitel, B. zum Dualismus.
307 BBl 1988 II 414 ff., 424 f.

womit staatliches Handeln überprüfbar wird. Öffentlichkeitsgesetze finden sich – wie auch Datenschutzgesetze – in der Schweiz wiederum sowohl auf Bundesebene als auf kantonaler Ebene.[308]

210 Zurück zum eidgenössischen Datenschutzgesetz: Der langwierige Prozess bis zur Verabschiedung des DSG führte auch dazu, dass mangels spezifischer Datenschutzgesetzgebung das erste internationale Datenschutz-Übereinkommen Nr. 108 des Europarates aus dem Jahre 1981 von der Schweiz nicht ratifiziert werden konnte.[309] Das Übereinkommen verlangte in seinem Art. 3 Abs. 1, dass sowohl der öffentliche als auch der private Sektor zu regulieren seien. Als 1990 dem Ständerat ein datenschutzgesetzgeberischer Vorschlag vorgelegt wurde, der sowohl den öffentlichen als auch den privaten Bereich adressierte, geschah dies mit den Worten:

> «Die unrühmlichen Vorkommnisse in der Bundesverwaltung dürfen nicht zur Annahme verleiten, in der Wirtschaft und anderen Bereichen seien keine Irrtümer und Missbräuche denkbar. Die Bejahung einer Gesetzgebung hat auch einen gleichsam rechtspraktischen Grund. Experten der Wissenschaft und der Praxis haben überzeugend dargetan, dass eine datenschutzrechtliche Konkretisierung des Persönlichkeitsschutzes durch den Gesetzgeber nicht zuletzt im Interesse der Wirtschaft und aller privaten Datenbearbeiter selber liegt […]. [I]m öffentlichen Bereich, das heisst bei der Bundesverwaltung, einen griffigen Datenschutz zu begründen, bedeutete wohl, Wasser in die Reuss oder in die Aare zu tragen. Die Aktualität lässt sich angesichts der sich jagenden Fichen-Enthüllungen kaum mehr überbieten […].»[310]

211 Die Schweiz konnte ihr erstes Datenschutzgesetz, das Vorgaben für Personendatenverarbeitungen sowohl durch Bundesbehörden als auch durch Private formulierte, auf den 1. Juli 1993 in Kraft setzen. Es bezweckt(e) den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten verarbeitet werden, Art. 1 DSG. Adressiert wurde hierbei die Personendatenverarbeitung sowohl durch Bundesbehörden als auch durch Private, vgl. Art. 2 DSG. An diesem Konzept wird auch mit der Totalrevision festgehalten, vgl. Art. 1 f. nDSG.

212 Anders verliefen die Entwicklungen in den USA, wo der private Bereich *keiner* allgemeinen Datenschutzgesetzgebung zugeführt, stattdessen ein sektorieller Ansatz implementiert wurde.[311] Insofern ist allem voran der *Fair Credit Reporting Act* von 1970 einschlägig, der das Kreditinformationswesen reguliert, dessen Erschaffung auch mit dem allgemein stark ausgebauten Konsumentenschutz erklärt

308 Vgl. zum Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung <https://www.fedlex.admin.ch/eli/cc/2006/355/de>; die kantonalen Öffentlichkeitsgesetze lassen sich abrufen unter <https://www.oeffentlichkeitsgesetz.ch/deutsch/die-kantone/> (zuletzt besucht am 20. September 2021); in diesem Zusammenhang auch Cottier, in: Métille (ed.), 139 ff.

309 Nabholz, in: Schweizer (Hrsg.), 1 ff., 2.

310 Danioth, AB 88.032, 13. März 1990, 126.

311 Hierzu Buchner, 15; in seiner Studie mit Fokus auf das Auskunftsrecht auch mit Blick auf das US-amerikanische Recht mit seiner sektoriellen Gesetzgebung Page, 213 ff.

wird.[312] Sein Ziel ist die Gewährleistung eines akkuraten und fairen Kreditreportings und damit der Schutz des Vertrauens der Allgemeinheit, das für einen funktionierenden Finanzsektor unverzichtbar ist, was in einen bemerkenswerten Kontrast zur individualrechtlichen Anknüpfung der Datenschutzgesetzgebungen in Europa tritt. Zwar wurden in den USA wiederholt die Abkehr vom sektoriellen Regulierungsansatz und eine allgemeine Datenschutzgesetzgebung gefordert – allerdings erfolglos.[313] Der *sektorielle resp. bereichsspezifische Ansatz* in den USA wird mit dem tief verwurzelten Misstrauen gegenüber staatlichen Eingriffen in private Verhältnisse begründet, wie es auch mit der *state action doctrine* artikuliert werde.[314]

213 Der Frage, ob der bereichsspezifische Ansatz *sachlich und spezifisch aus datenschützerischen Erwägungen* – namentlich auch Zweckerwägungen – überzeugend ist, wird im Laufe dieser Arbeit vertieft analysiert. Die Differenz zwischen dem Regulierungsansatz in den USA und den kontinentaleuropäischen Erlassen für den privaten Bereich beschränkt sich damit nicht nur darauf, dass derjenige in den USA ein sektorieller ist, womit auf eine Querschnittsgesetzgebung verzichtet wird, wohingegen in Kontinentaleuropa allgemeine Datenschutzgesetzgebungen erlassen wurden, die sowohl den öffentlichen als auch den privaten Bereich normieren.[315]

214 Sodann präsentiert sich der Schutzzweck der Erlasse zumindest auf den ersten Blick unterschiedlich. Bemerkenswert sind in Bezug auf den Schutzzweck die Entwicklungen, wie sie die DSGVO bringt. Ebenda lässt sich eine Diversifizierung des Schutzzwecks verzeichnen. Anders richtet sich in der Schweiz *der Schutzzweck gemäss Zweckartikel des DSG bis heute ganz auf das Subjekt*, vgl. Art. 1 DSG und Art. 1 nDSG. In den USA steht *der systemische Schutzgedanke* im Vordergrund.[316] So statuiert der *Fair Credit Report Act* in seiner ersten Bestimmung, § 602 (a) (1), dass das *Banksystem* (und nicht nur die einzelne Bankkundin) auf die faire und akkurate Verarbeitung von Informationen angewiesen sei. Umgekehrt würden unfaire Verarbeitungshandlungen das *öffentliche Vertrauen in den Bankensektor erodieren.* Auf das Vertrauen allerdings sei der Banksektor für seine Funktionstüchtigkeit angewiesen.

312 Buchner, 16 f.
313 Simitis im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt besucht am 30. April 2021); vgl. illustrativ zu den (dazumal) freien Bereichen der Personendatenverarbeitung Bibas, Harv. J.L. & Pub. Pol'y 1994, 591 ff., 595 f.
314 M. w. H. Buchner, 9 und 19 ff.
315 Zum Begriff «Querschnittsgesetz» BBl 1988 II 414 ff., 444; Brunner, Jusletter vom 4. April 2011, N 8; für Deutschland und das BDSG Wolff, in: Mehde/Ramsauer/Seckelmann (Hrsg.), 1071 ff., 1071; zum Datenschutzrecht als Querschnittsmaterie und zur Kategorisierung von öffentlichem und privatem Recht auch Brühwiler-Frésey, 99 ff.
316 Vertiefend hierzu für den Subjekt- und Persönlichkeitsschutz gemäss DSG zweiter Teil, VI. Kapitel und zu den Schutzzwecken gemäss DSGVO sowie DSG, wie sie in den Zweckartikeln beschrieben werden, dritter Teil, VIII. Kapitel, A.2.2.

215 Die Entwicklungen im Anschluss an die Schaffung der Datenschutzerlasse erster und zweiter Generation sind hinsichtlich der Frage der Bereichsdifferenzierung im Datenschutzrecht von besonderem Interesse. In diesem Punkt bestand keineswegs Konsens. Vielmehr lassen sich entgegenlaufende Strategien feststellen – einerseits die *Verstärkung der Differenzierung der Normen für die beiden Sektoren, andererseits deren Harmonisierungen*.

216 In Deutschland wurde mit den Novellierungen des ersten Datenschutzgesetzes 1990, zudem über die Rechtsprechung des Bundesverfassungsgerichts eine sukzessive Angleichung des Datenschutzrechts für den öffentlichen und den privaten Bereich eingeleitet.[317] Selbst eine Vereinheitlichung datenschutzrechtlicher Normen für die beiden Bereiche wurde in Anbetracht der «umfassenden elektronischen Eigenaufrüstung der Gesellschaft»[318] bereits im 20. Jahrhundert gefordert.[319] Ausschlaggebend hierfür war eine Überzeugung, wonach die Bedrohungen, die durch Personendatenverarbeitungen von Privaten ausgehen, denjenigen durch den Staat um nichts (mehr) nachstünden.[320]

217 Den Schritt zu einem *monistischen System*, das Personendatenverarbeitungen durch Behörden wie Private einem identischen Regime unterstellt, wird im 21. Jahrhundert durch die seit dem 25. Mai 2016 in Kraft stehende Europäische Datenschutz-Grundverordnung (DSGVO) umgesetzt. Sie vollzieht damit nicht nur unter dem territorialen Aspekt, sondern auch dem materiellrechtlichen Aspekt, mithin bereichsspezifisch betrachtet, eine «Harmonisierung» der Vorgaben für Personendatenverarbeitungen im EU-Raum. Die DSGVO dient, so die einleitenden Erwägungen, dazu, einen Raum der Freiheit, Sicherheit und Prosperität zu gewährleisten und einen Beitrag zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarktes sowie zum Wohlergehen der Personen zu leisten. Der Schutz der natürlichen Person bei der Verarbeitung von Personendaten ist ein Grundrecht, vgl. Art. 1 DSGVO.

218 Die DSGVO löste einen datenschutzrechtlichen Handlungsdruck und Anpassungsbedarf auf die Schweiz aus, vgl. insb. zum Angemessenheitsbeschluss Art. 44 ff. DSGVO. Das DSG wurde einer Totalrevision unterzogen, die 2020 verabschiedet wurde und 2023 in Kraft tritt.[321] Das totalrevidierte DSG (nDSG) integriert mehrere neue datenschutzrechtliche Instrumente, wie sie die DSGVO

317 Vgl. zu diesen Entwicklungen vertiefend Buchner, 26 ff.

318 So Vesting, in: Ladeur (Hrsg.), 155 ff., 161, der indes die Übertragung des Bildes des machtüberlegenen Staates im Kontext von Personendatenverarbeitungen auf gesellschaftliche Beziehungen kritisiert.

319 Vgl. Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 56.

320 M. w. H. Buchner, 26, der für einen zweigeteilten Datenschutz, nicht dagegen für ein divergierendes Schutzniveau eintrat; kritisch zur Übertragung eines herkömmlich staatszentrierten Leitbildes auf gesellschaftliche Beziehungen Vesting, in: Ladeur (Hrsg.), 155 ff., 162 ff.

321 In dieser Studie wird das DSG vom 19. Juni 1992 (Stand am 1. März 2019) als DSG, das totalrevidierte DSG vom 25. September 2020 als nDSG bezeichnet; als diese Habilitationsschrift begonnen

vorsieht.[322] Keineswegs aber übernimmt das neue DSG die DSGVO eins zu eins oder setzt diese umfassend um. Früh stand fest, dass *prägende strukturelle Leitprinzipien*, die im Rahmen *der Verabschiedung des ersten eidgenössischen Datenschutzgesetzes installiert wurden, beibehalten werden*.[323] Entsprechend bleiben zahlreiche der konzeptionellen Erwägungen sowie Entscheidungen, wie sie sich im DSG sowie in den Gesetzesmaterialien zum ersten DSG finden, auch nach der Totalrevision relevant.

Dieser erste Teil, der sich den Informationspraktiken und Informationsvorgaben sowie dem Datenschutz (in zeitgenössischer Terminologie) aus einer geschichtlichen Perspektive widmete, soll nun abgerundet werden – mit einer Überleitung in den zweiten Teil. Ebenda werden *Strukturmerkmale des eidgenössischen Datenschutzgesetzes* freigelegt werden, um diese im dritten Teil einer Effektivitätsprüfung zu unterziehen und, bei festgestellten Defiziten, einen Vorschlag zur Rekonzeptionalisierung – über die Totalrevision hinaus – zu entwickeln. 219

Mit Blick auf die *Funktionsweise* und die *Strukturmerkmale* des eidgenössischen Datenschutzgesetzes ist eine Textpassage zu den damaligen parlamentarischen Beratungen im Rahmen seiner erstmaligen Verabschiedung aufschlussreich: 220

> «Herr Onken hat beanstandet, dass die Gewichte ungleich verschoben worden sind und dass vor allem der Ausdruck „überwiegende Interessen" diffus sei. Dieser Ausdruck ist aber dem Zivilgesetzbuch entnommen. Es geht nicht um eine Abkehr von den Grundsätzen von Artikel 28 des Zivilgesetzbuches, sondern es geht um eine Konkretisierung dieser Grundsätze, damit der Richter eine klarere Marschrichtung aufgezeigt erhält und nicht im grossen unbestimmten Bereich des jetzigen Artikels 28 Recht setzen soll. Wir wehren uns als Parlament mit Recht dagegen, dass die Gerichte bis hinauf zum Europäischen Gerichtshof in einer dynamischen Fortentwicklung des Rechtes in die Kompetenzen des Gesetzgebers eingreifen; das ist bei uns dem Parlament und dem Souverän vorbehalten. Jeder, der eigentlich will, dass seine Auffassung von Datenschutz verwirklicht werden kann, gerade auch im Privatrecht, sollte an einer vernünftigen Gesetzgebung interessiert sein. Das Datenschutzgesetz ist nicht ein Rezeptbuch, sondern enthält grundsätzliche Regeln über die Anwendung. Es ist falsch, wenn man einfach den öffentlichen und den privaten Datenschutz vergleicht. Im öffentlichen Recht hat der Staat Aufgaben zu erfüllen, für deren Erfüllung er auf Personendaten angewiesen ist. Er tritt dem Bürger hoheitlich gegenüber. Der Bürger hat diese Aufgabe hinzunehmen, hat Daten zu liefern. Hier besteht ein ganz klares Bedürfnis für einen verstärkten Rechtsschutz, währendem im privaten Recht die Grundsätze von Artikel 28, die Grundsätze der Freiheitsrechte,

wurde, war eine Totalrevision des DSG nicht in Sicht und das erste DSG führte ein eher stiefmütterliches Dasein auch im Schrifttum.

322 So neuerdings namentlich das Verarbeitungsverzeichnis, vgl. Art. 12 nDSG und Art. 30 DSGVO, die Datenschutz-Folgeabschätzung, vgl. Art. 22 nDSG und Art. 35 DSGVO, das Rollenkonzept von Auftragsverarbeiter und (gemeinsam) Verantwortlichen, vgl. insb. Art. 9 nDSG und Art. 24 ff. DSGVO; zum fehlenden Konzept betreffend die Frage, welche Instrumente der DSGVO in der Totalrevision übernommen werden sollten, kritisch Baeriswyl, digma 2020, 6 ff., 6; eine gute Übersicht zu den Kernelementen der DSGVO findet sich bei Räther, ZHR 2019, 94 ff.

323 Ihnen widmet sich der zweite Teil dieser Schrift.

> generell gelten und die Gerichte tätig werden sollen, während der Datenschutzbeauftragte als Ombudsmann Ratschläge, Empfehlungen abgeben und damit auch für den Rechtsweg wertvolle Hinweise geben kann.»[324]

221 Die Passage deutet *drei Leitgedanken resp. Ordnungsprinzipien des DSG* an. Sie leisten einen zentralen Beitrag zur *Charakterisierung des DSG*, die über seine Totalrevision hinaus Bestand hat. Entsprechend haben sie massgeblichen Einfluss auf die Funktionsweise, Funktionstüchtigkeit, aber auch auf die funktionalen Defizite des DSG. Die Totalrevision verleiht dem DSG zwar durch die Einführung verschiedener neuer Instrumente, wie namentlich dem Verzeichnis der Verarbeitungstätigkeiten oder der Datenschutz-Folgenabschätzung, neue Charakterzüge.[325] Gleichwohl hält es an seinen von Anfang an definierten Grundcharakteristika fest. Sie sind für diese Studie, die einen Vorschlag zur Weiterentwicklung des Datenschutzrechts entwickeln will, von zentralem Interesse. Anhand dieser Passage zeigen sich in Kürze die *folgenden drei Strukturmerkmale – sie werden im zweiten Teil vertieft analysiert – als konzeptionell prägend*:

222 *Erstens:* Die Schweiz sieht in ihrem als «Einheitsgesetz» titulierten DSG den *Dualismus* der datenschutzrechtlichen Vorgaben für den *öffentlichen und den privaten Sektor* vor – jener wird als *erstes Strukturmerkmal* im zweiten Teil dieser Arbeit im IV. Kapitel genauer beleuchtet werden.[326] Selbstredend ist der Dualismus nicht in radikaler Weise verwirklicht in dem Sinne, wonach für den öffentlichen Bereich des Bundes gänzlich andere Vorgaben gälten als für den privaten Bereich. Vielmehr sieht das DSG ein durchaus differenziertes Gefüge vor, was das Verhältnis der Vorgaben für den öffentlichen Bereich des Bundes und derjenigen für den privaten Bereich angeht. Eklatant ist die Annäherung über das sog. Verhältnismässigkeitsgebot als Verarbeitungsgrundsatz. Gleichwohl ist das Regime des DSG – bis heute und auch nach seiner Totalrevision – als (differenziert) *dualistisches Regelungsregime* zu beschrieben. Es nimmt insb. – anders als die DSGVO – keinen Wechsel zu einem *monistischen System* mit identischen und konsequent vereinheitlichten Vorgaben für die Personendatenerarbeitung durch staatliche Stellen und Private vor.[327] Wenn nun das DSG von einem *dualistischen System* ausgeht, das für den öffentlichen und den privaten Bereich differenzieren-

---

324 Danioth, AB 88.032, 13. März 1990, 135; zur Aufsicht über private Datenbearbeiter vgl. Schweizer, in: Schweizer (Hrsg.), 91 ff.

325 Vgl. Art. 12 und Art. 22 nDSG; vertiefend zu den historisch fest verankerten Grundzügen vgl. zweiter Teil, IV.–VI. Kapitel; vertiefend zu den neuen Instrumenten und Elementen, die mit der DSGVO und dem totalrevidierten DSG eingeführt wurden/werden und die den Charakter des DSG weiterentwickeln, ohne ihn allerdings gänzlich zu verändern, vgl. dritter Teil, VIII. Kapitel, A.1. und A.2.

326 Zum Begriff «Einheitsgesetz» Kohler, AB 88.032, 5. Juni 1991, 948; Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 20, N 26, N 34; Danioth, in: Schweizer (Hrsg.), 9 ff., 11 ff.

327 Zur dualistischen Regelungsstruktur des DSG Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.8; als föderalistische Ordnung umschrieben von Schweizer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 1 N 13; zum Dualismus als erstem Strukturmerkmal des DSG resp. nDSG nachfolgend zweiter Teil, IV. Kapitel.

de Vorgaben vorsieht, die DSGVO ein monistisches Modell wählt und die USA an ihrem sektoriellen Ansatz für den privaten Bereich festhalten, dann zeigt sich deutlich, dass die *Frage nach der Relevanz kontextueller resp. bereichsspezifischer Differenzierungen unterschiedlicher denn je beantwortet wird*. Der Frage kommt, wie anhand des historischen Teils schlaglichtartig beleuchtet, ein zentraler Stellenwert zu. Selbstredend ist auch in einem Modell, für welches eine dualistische Struktur beschrieben wird, dieser Dualismus nicht schwarz-weiss oder absolut rein. Ein solches Konzept der Reinheit der Trennung von privatem und öffentlichem Recht ist seit jeher eher theoretischer Natur. Gleichwohl gibt der Begriff des Dualismus ein wesentliches Charakteristikum des DSG wieder. Das klarste Beispiel für auflösende Schattierungen liefert das Verhältnismässigkeitsprinzip als Verarbeitungsgrundsatz, welches für den privaten wie den öffentlichen Bereich gleichermassen gilt, vgl. Art. 4 Abs. 2 DSG und Art. 6 Abs. 2 nDSG.[328]

223 *Zweitens:* Charakteristisch (auch) für das eidgenössische Datenschutzgesetz ist die *generalklauselartige Regelung*. Damit sollte der Tatsache Rechnung getragen werden, wonach Datenschutz als *Querschnittsmaterie* gilt: Durch ein offenes Regelungsregime sollte es in unterschiedlichen Feldern operationalisierbar werden – ein Punkt, der ebenso von hoher Bedeutung für diese Schrift ist. Darüber hinaus sollten durch eine generalklauselartige Regelung die Chancen, die in den Entwicklungen der Datenbearbeitungstechnologien verortet wurden, nicht durch ein starres Regelwerk vereitelt werden.[329] Die Normierung mittels Generalklauseln war in den 1970er Jahren sodann zumindest teilweise eine Verlegenheitslösung: *Dass* Datenschutzregulierungen unverzichtbar seien, hatte sich als Erkenntnis weitgehend durchgesetzt.[330] *Worauf* man allerdings rechtlich reagieren und *wie* reguliert werden sollte, das blieb weitgehend im Dunkeln.[331] Denn das, was in den Rechenmaschinen passierte, war namentlich für Juristinnen und Juristen kaum zu durchschauen. Zudem bereitete seit jeher nicht nur die Umschreibung der Verarbeitungsprozesse und Gefahren resp. Risiken, die mit den Informationstechnologien einhergingen, Probleme. Auch das Schutzobjekt der «Privatheit» erwies sich als definitionsresistent. An diesem Punkt erfolgt teilweise eine Verengung und Isolierung der Perspektive auf den Technologieaspekt – zum Ausdruck

328 Vertiefend zum Grundsatz im Datenschutzrecht in seiner öffentlich-rechtlichen Trias zweiter Teil, V. Kapitel, B.3.

329 Vgl. Meier, N 5 ff.; Belser, in: Datenschutz-Forum Schweiz (Hrsg.), 1 ff.; in diesem Zusammenhang ebenso Pohle, 57, 77, 181 auch mit Hinweis auf Simitis, der sich seit jeher kritisch zu den Generalklauseln äusserte, allerdings in erster Linie wegen der ungenügenden Berücksichtigung der Verarbeitungszusammenhänge.

330 So die mehrheitlichen Stellungnahmen im Vernehmlassungsverfahren im Jahr 1984 auf den nach rund fünf Jahren Ausarbeitungszeit vorgelegten Expertenentwurf, BBl 1988 II 414 ff., 428.

331 Simitis im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt besucht am 30. April 2021).

gebracht wird dies mit einer *Beschreibung des Datenschutzrechts als Technikfolgerecht*.[332]

224 Dass eine Gesetzgebung mittels Generalklauseln mit Defiziten einhergeht, wurde nicht nur für den Bereich des Datenschutzrechts beschrieben.[333] Der Schweizer Datenschutzgesetzgeber liess denn auch die mit einer solchen materiellrechtlichen Regelungsstrategie einhergehende Schwachstellen nicht unberücksichtigt. Die Schaffung der Position eines Datenschutzbeauftragten, der über die Einhaltung datenschutzrechtlicher Anliegen wachen sollte, müsste hier eine gewisse kompensatorische Wirkung entfalten.[334] Anders gewendet: Eine organisationale und prozedurale Normierung sollte Schwächen der materiellrechtlichen Normierung abfedern. Die generalklauselartigen Bearbeitungsgrundsätze nehmen auch nach der Totalrevision namentlich für den privaten Sektor die zentrale Schrankenfunktion wahr.[335] Zugleich allerdings werden die Kompetenzen des EDÖB und das Sanktionsregime mit der Totalrevision verschärft.[336] Das *generalklauselartige Regime* wird als *materiellrechtlich tragendes* und *zweites Strukturmerkmal des eidgenössischen Datenschutzgesetzes im V. Kapitel dieses zweiten Teils* analysiert.

225 *Drittens:* Für den Bereich der Verarbeitung von Personendaten durch *Privatpersonen* knüpft das DSG am *Persönlichkeitsrecht und Art. 28 ff. ZGB* – der berühmten schweizerischen Generalklauselregel – an.[337] Das DSG basiert folglich – ebenso nach der Totalrevision – auf den etablierten Regelungs- und Wirkungsmechanismen sowie der Struktur von Art. 28 ZGB. Dem *persönlichkeitsrechtlichen Ansatz für den «privaten Sektor»* widmet sich das *VI. Kapitel des zweiten Teils dieser Studie*.

226 Die umrissenen *drei Strukturmerkmale des DSG standen im Rahmen der Totalrevision* nicht ernsthaft zur Debatte. Verabschiedet wurde eine Totalrevision, die an den besagten *drei Strukturmerkmalen des DSG festhält*. Sie verleihen dem DSG damit auch seine charakteristische Funktionsweise. Dagegen wird die Totalrevision – ergänzend und weiterentwickelnd – diese Strukturmerkmale

332 Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 3 ff., N 12 ff.; Brunner, Jusletter vom 4. April 2011, N 9; zur Technologieneutralität des DSG Belser, in: Datenschutz-Forum Schweiz (Hrsg.), 1 ff.

333 Zum Problem der Generalklauseln Auer, Materialisierung, 1 ff.; spezifisch für das Datenschutzrecht Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 20, 45, 101 ff.; bezüglich des Datenschutzrechts vgl. auch Rosenthal, in: Datenschutz-Forum Schweiz (Hrsg.), 69 ff., der methodisch das Bauchgefühl als Bewältigungsinstrument vorschlägt.

334 Für Deutschland zu dieser kompensatorischen Rolle des Datenschutzbeauftragten Simitis im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt besucht am 30. April 2021).

335 Vgl. Art. 6 nDSG und Art. 30 ff. nDSG; Art. 4 DSG und Art. 12 ff. DSG; vertiefend zweiter Teil, V. Kapitel und VI. Kapitel.

336 Vgl. Art. 49 ff. nDSG und Art. 60 ff. nDSG.

337 Vgl. Art. 1 i. V. m. Art. 12 ff. DSG und Art. 1 i. V. m. Art. 30 ff. nDSG.

durch neue Instrumente flankieren und zumindest teilweise neu einbetten sowie ausrichten. In dieser Schrift wird sichtbar, inwiefern die datenschutzrechtlichen Entwicklungen weniger mit Anpassungen im Bereich der materiellrechtlichen Vorgaben einhergehen. Die grossen materiellrechtlichen Verarbeitungsgrundsätze, wie sie unter den Generalklauseln beschrieben werden, sind fester und unbestrittener Bestandteil der Datenschutzgesetze seit deren Anfängen bis heute. Diese materiellen Grundsätze werden neuerdings ergänzt durch prozedurale sowie organisatorische und damit formelle Ansätze. So obliegen den Verarbeitenden neu umfassende Pflichten in Bezug auf die Dokumentation, Risikoabwägung, die Organisation usf. Betont wird die Bedeutung technischer sowie organisatorischer Massnahmen zur Absicherung der materiellrechtlichen Vorgaben. Auch die staatlichen Durchsetzungskompetenzen werden markant ausgebaut. Bevor allerdings auf diese jüngsten Entwicklungen einzugehen ist, findet eine Auseinandersetzung mit den Kernstrukturmerkmalen des DSG statt – wie sie seit den Anfängen des DSG in diesem angelegt wurden und wie sie auch nach der Totalrevision weiterhin, wenn auch mit gewissen Modifikationen, Gültigkeit haben werden.

Der nachfolgende zweite Teil legt folglich vorab die drei das DSG vor und nach 227
der Totalrevision prägenden *Strukturmerkmalen* detailliert frei. Dies geschieht mit dem Ziel, diese nach ihrer Identifizierung und Beschreibung auf ihre Wirksamkeit und Tragfähigkeit hin zu untersuchen. Einfach gewendet: Die anschliessende Etappe dieser Studie widmet sich der Frage, «wie» das DSG funktioniert. Hierauf basierend kann sich alsdann ein dritter Teil den Fragen zuwenden, inwiefern die Revisionswellen die Strukturmerkmale neu ausrichten und «ob» das DSG auch in der Realität funktioniert. Die Funktionstüchtigkeit beurteilt sich hierbei nicht nur anhand der faktischen Einhaltung des Gesetzes in der Realität. Vielmehr ist ebenso zu fragen, welche Zwecke und Ziele das Datenschutzrecht absichern soll – und ob es diese (ggf. neu verstandenen) Schutzobjekte durch seine Normen angemessen und effizient zu garantieren weiss.

Zweiter Teil: Die drei Strukturmerkmale des DSG

Beim eidgenössischen Datenschutzgesetz handelt es sich um einen der wenigen Erlasse, der Antworten ebenso auf die *digitale Transformation* zu geben sucht. Eine Herausforderung, mit der sich neben dem Privatrecht ebenso das Urheberrecht, z. B. wegen Streamingdiensten, konfrontiert sieht.[338] Gleichwohl beschränkt sich das DSG weder auf spezifische Technologien der Personendatenverarbeitung noch auf spezifizierte (z. B. automatisierte) Verarbeitungshandlungen oder Technologien.[339] 228

Die Totalrevision setzt zwar neue Akzente. Anstoss zu dieser Totalrevision gaben zum einen die Entwicklungen in der EU.[340] Die Schweiz ist auf einen Angemessenheitsbeschluss vonseiten der zuständigen EU-Behörden angewiesen, vgl. Art. 45 DSGVO.[341] Zudem wurde die Totalrevision mit dem Aktualisierungsbedarf wegen des rasanten technologischen wie gesellschaftlichen Wandels begründet. Hinzu trat ein Attest, das der Wirksamkeit des geltenden DSG ein bescheidenes Zeugnis ausstellte.[342] Die jüngsten datenschutzrechtlichen Neuerungswellen erfolgen nicht nur in Anerkennung von Bedeutung, Chancen und Risiken moderner Datenverarbeitungstechnologien.[343] 229

338 Aufschlussreich z. B. die Beiträge in AcP 218 (2018), Heft 2–4, 151 ff.

339 Zum weit definierten Begriff des Verarbeitens (von Personendaten) vgl. Art. 5 lit. d (ff.) nDSG; Art. 3 lit. e und lit. f DSG.

340 Verordnung der EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, in Kraft seit dem 25. Mai 2016 mit einer Umsetzungsfrist bis zum 25. Mai 2018; abrufbar unter: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (zuletzt besucht am 30. April 2021); zur «Globalisierungswirkung» Birnhack, CLSR 2008, 508 ff.; zur Notwendigkeit der datenschutzrechtlichen Harmonisierung Cottier, SRIEL 2016, 255 ff.

341 Ausserdem hat die DSGVO extraterritoriale Wirkung, vgl. Art. 3 Abs. 2 lit. a und lit. b DSGVO. Dass die Vorgaben der DSGVO für manch ein Schweizer Unternehmen direkt gelten, wurde trotz des Ablaufes der Umsetzungsfrist am 25. Mai 2018 nur ungenügend zur Kenntnis genommen, vgl. NZZ, Was das neue EU-Datenschutzgesetz für die Schweiz bedeutet, Mai 2018, <https://www.nzz.ch/wirtschaft/strengerer-datenschutz-auch-in-der-schweiz-ld.1388558> (zuletzt besucht am 30. April 2021); zur Totalrevision auch mit Blick auf einen Angemessenheitsbeschluss Frei, Jusletter vom 17. September 2018, N 17 f.

342 Vgl. Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017 (17.059), 6941 ff.; Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011 (BBl 2012 335); vgl. weiter Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz vom 21. Dezember 2016, 5 ff.; zum Vorentwurf: <https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vorentw-d.pdf> (zuletzt besucht am 30. April 2021); zum Entwurf: <https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf> (zuletzt besucht am 30. April 2021); grundlegend zum sog. Vollzugsdefizit Buchner, 1; zum Vollzugsdefizit auch Spiecker genannt Döhmann, in: Epiney/Sangsue (Hrsg.), 1 ff., 7 ff.; vertiefend zum Vollzugsdefizit dritter Teil, VII. Kapitel.

343 Den Bedeutungswandel, den das Datenschutzrecht allerdings gerade auch mit der DSGVO vollzieht, auf diese starke Hand der Behörden zu reduzieren, greift indes zu kurz. Vertiefend zu den Entwicklungstrends der DSGVO vgl. dritter Teil, XIII. Kapitel, A.

230 Gleichwohl soll an dieser Stelle – wie bereits im historischen Teil, allerdings chronologisch nicht ganz so weit zurück – eine Rückblende insb. auf den Gesetzgebungsprozess im Rahmen der *Verabschiedung des ersten DSG* erfolgen. Die ebenda geführten Debatten und getroffenen Entscheidungen sind auch nach der Totalrevision relevant: Denn mit dieser wird von der *Grundstruktur, dem Basiskonzept sowie den prägenden Leitprinzipien des ersten DSG* nicht abgegangen.[344] Ebendiesen widmet sich dieser zweite Teil. In ihm werden *drei Strukturelemente* des eidgenössischen Datenschutzgesetzes genauer analysiert. Eine solche vertiefte Beschäftigung mit der *Wirkungsstruktur des DSG* ist nicht zuletzt der Tatsache geschuldet, dass das DSG in seiner Gesamtheit sowie für seinen privaten Bereich von wissenschaftlicher Seite bislang eher wenig Aufmerksamkeit erfahren hat.[345]

231 Seit jeher wird vertreten, dass das eidgenössische Datenschutzgesetz eine sog. *Querschnittsmaterie* regelt.[346] Gleichwohl werden zahlreiche der datenschutzrechtlichen Konzepte und Begriffe – nicht zuletzt dasjenige des Schutzobjektes resp. Schutzzweckes sowie damit zusammenhängend die Regelungsmechanik und die Ansätze des DSG – mit einem bemerkenswerten Facettenreichtum umschrieben.[347] Die Interpretationsvielfalt und damit eine gewisse Orientierungslosigkeit zeigt sich z. B. im Evaluationsschlussbericht, der im Zuge des zwanzigjährigen Bestehens des Datenschutzgesetzes veröffentlicht wurde und Anstösse für die Totalrevision lieferte:

> «Das Datenschutzgesetz konkretisiert den grundrechtlichen *Schutz der Privatsphäre*, wie er in Art. 8 Abs. 1 EMRK sowie in der Bundesverfassung verankert ist. Art. 13 Abs. 2 BV legt fest: „Jede Person hat Anspruch auf *Schutz vor Missbrauch ihrer persönlichen Daten*." Obwohl es aus dem Wortlaut der Norm nicht klar hervorgeht, wird mit dieser Bestimmung das *Grundrecht auf informationelle Selbstbestimmung* definiert. Damit wird ein Schutzniveau hinsichtlich der persönlichen Daten statuiert, das nur unter den Voraussetzungen von Art. 36 BV eingeschränkt werden kann, d. h. die Einschränkung muss auf einer gesetzlichen Grundlage beruhen, ein öffentliches Interesse oder den Schutz von Grundrechten Dritter bezwecken sowie den Grundsatz der Verhältnismässigkeit und den Kerngehalt des Grundrechts auf informationelle Selbstbestimmung wahren. Dem Recht auf informationelle Selbstbestimmung kommt horizontale Drittwirkung zu, d. h. eine Schutzpflicht besteht auch gegenüber Datenbearbeitungen durch Privatpersonen. Konkretisiert wird dieser Schutzbereich durch Art. 4 ff. und Art. 12 ff. DSG (Schweizer 2008: 326 (N 43) zu Art. 13). Das DSG bezweckt gemäss Art. 1 „den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden". Der *Schutz der Persönlichkeit* zielt dabei primär auf die Bearbeitungen durch Private, der Schutz der

344 Die Begleitgruppe schlug in ihrem Bericht vor, sich am geltenden Aufbau des DSG zu orientieren, vgl. Bericht der Begleitgruppe Revision DSG, Normkonzept zur Revision des DSG vom 29. Oktober 2014, 7.

345 Zur Unkenntnis des Rechtsgebietes und verwirrenden Interpretationen auch zum Schutzbereich vgl. Gamper, Jusletter IT vom 22. Februar 2011, N 2 f.

346 Vgl. den Hinweis des EDÖB: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/ueberblick/datenschutz.html> (zuletzt besucht am 30. April 2021); Bolliger/Féraud/Epiney/Hänni, 11.

347 Vertiefend hierzu insb. dritter Teil, VII. Kapitel, A.2.

Grundrechte auf die Bearbeitungen durch staatliche Behörden. Zur Motivation des Datenschutzes führte der Bundesrat in seiner Botschaft an, der Umgang mit Daten könne sich in verschiedener Weise nachteilig oder verletzend auf die betroffene Person auswirken: Verunsicherung, wenn man nicht mehr überblickt, wer Daten über einen bearbeitet; Anmassung durch indiskretes Auskundschaften; Benachteiligung oder unbillige Behandlung aufgrund unrichtiger, unvollständiger oder nicht mehr aktueller Informationen; lebenslänglicher Makel aufgrund dauerhafter Aufbewahrung und Verwendung negativer Angaben; Verletzung der Persönlichkeit durch übermässiges Bearbeiten, z. B. durch Anprangern in der Öffentlichkeit oder Erheben unnötiger Angaben bei einem Vertrag; Verletzung durch Zweckentfremdung der Daten (Bundesrat 1988: BBl 1988 II 416). Das DSG will somit verhindern, dass Personen durch *nicht konformes Bearbeiten ihrer Daten einen Schaden erleiden*; sie sollen also zum Beispiel nicht aufgrund bestimmter Informationen, die ein Arbeitgeber nicht ohne Wissen der Person beschaffen dürfte, ihre Stelle verlieren. Das DSG setzt aber bereits vor dem Schaden an, indem es – anknüpfend an den grundrechtlichen Schutz der Privatsphäre – die Personen generell vor einer informationellen Entblössung schützen will. Dabei ist es nicht die Absicht des Gesetzgebers, mit dem DSG Datenbearbeitungen generell zu unterbinden; vielmehr sollten diese so ausgestaltet werden, dass der informationellen Selbstbestimmung Genüge getan wird: „Ein Datenschutzgesetz hat nicht den Zweck, die Entwicklungsmöglichkeiten im Bereich der Informationstechnologien zu verhindern oder einzuschränken." Vielmehr seien *„gewisse Leitplanken* für die Datenbearbeitung zu setzen, die garantieren, dass die *Entfaltung der Persönlichkeit nicht durch unnötige und unerwünschte Informationstätigkeiten beeinträchtigt wird"* (BBl 1988 II 417–418)».[348] [Hervorhebungen durch die Autorin]

«Informationelle Selbstbestimmung», «Missbrauchsverhinderung», «Schutz der Privatsphäre», «gewisse Leitplanken zum Schutz der Persönlichkeitsentfaltung vor unnötiger Informationstätigkeit», «Verhinderung eines Schadens» – zumindest teilweise scheint der Beitrag Begriffe «untechnisch» zu verwenden und nicht darauf abzuzielen, ebendiese fundiert zu durchdringen. Die kurze Passage führt in exemplarischer Weise das Vielerlei an Konzepten und Begriffen, die im Rahmen der Auseinandersetzung mit dem DSG oft differenzlos kursieren, vor Augen.[349] Sie bestätigt den Befund, der bereits für das Private gefunden wurde, mit welchem der Datenschutz untrennbar zusammenhängt, dass dieses ein schwer zu fassendes Konzept ist. Entsprechend vage bleiben für das Datenschutzrecht 232

348 Bolliger/Féraud/Epiney/Hänni, 7 f., Hervorhebung durch die Autorin; vertiefend und umfassend zu den in diversen Rechtstexten verankerten staatlichen Schutzpflichten mit Blick auf die Verbürgung der Privatsphäre im digitalen Zeitalter vgl. Kaufmann/Ghielmini/Medici/Pulver, 4 ff., mit einer Zusammenfassung bei 1 ff.; vgl. sodann Baeriswyl, digma 2008, 4 ff., 5, wonach das Recht auf Anonymität ein Aspekt des Grundrechts auf informationelle Selbstbestimmung und deshalb grundsätzlich gewährleistet sei, wobei seine Einschränkung, die Offenlegung der Identität, einer Rechtfertigung bedürfe; zur Drittwirkung der Grundrechte vgl. z. B. Bucher, SJZ 1987, 37 ff.

349 Zudem wird auf ein Missverständnis mit Blick auf den Datenschutz in der Allgemeinheit hingewiesen. Dieses artikuliert Gamper, Jusletter IT vom 22. Februar 2011, Einleitung, mit den Worten: «Datenschutz als Regelung des Rechts auf Privatsphäre in der (elektronischen) Datenverarbeitung wird in allgemeiner Unkenntnis der Materie überwiegend auf einen Geheimhaltungsanspruch reduziert, der rechtlich jedoch nur sehr eingeschränkt existiert»; nach Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 154 gehören zu den gesetzlich geschützten Persönlichkeitsrechten das Recht auf Privatsphäre, Ehre und informationelle Selbstbestimmung.

wesentliche Konzepte und Begriffe, was nicht nur der faktischen Verwirklichung, sondern auch der theoretischen Fortentwicklung im Wege steht. Immerhin – einige der über die Totalrevision eingeführten neuen Instrumente, wie beispielsweise das Verarbeitungsverzeichnis oder die Risiko-Folgenabschätzung, haben das Potential, eine gewisse strukturierende und damit kompensierende Wirkung zu erzielen.

233 Bei einer Auseinandersetzung mit dem DSG *gerade auch vor seiner Totalrevision* (die zu einer besseren Durchdringung der Materie auch in der Schweiz führte), präsentiert sich die Situation fast so, als ob die «Black Box» der Technik auch in das Recht transportiert würde. Das Recht des Privaten zeigt sich in einer für das Recht irritierenden Weise diffus. Als symptomatisch bezeichnet es denn auch Simitis, dass bis heute an der missverständlichen Begrifflichkeit des Datenschutzrechts festgehalten wird.[350]

234 Drei Strukturmerkmale prägen die Funktionsweise des DSG in beiden seiner Fassungen. *Erstens:* Der *Dualismus* im Sinne einer differenzierenden Regelung für den öffentlichen Bereich des Bundes und den privaten Bereich.[351] *Zweitens:* Ein generalklauselartiges Regime, in dessen Zentrum die allgemeinen Verarbeitungsgrundsätze stehen. *Drittens:* Die Anknüpfung des Datenschutzes für den privaten Sektor am Subjektschutz, genauer am *zivilrechtlichen Persönlichkeitsschutz*. Die Regelung des DSG für den privaten Bereich orientiert sich folglich an der Struktur von Art. 28 ZGB.[352]

235 Der zweite Teil will einen Beitrag zur besseren dogmatischen und konzeptionellen Durchdringung des DSG – in seiner Fassung vor, aber auch nach seiner Totalrevision – leisten. Die *Charakterisierung* des DSG anhand seiner *Strukturmerkmale* macht seine *Funktionsweise* («Wie funktioniert das Gesetz?») sichtbar. Alsdann wird es möglich, die Angemessenheit der Regelungsstruktur angesichts der Herausforderungen des Datenschutzes zu diskutieren («Funktioniert das Gesetz?»).[353] Eine solche mittel-, zweck- und zielorientierte Betrachtungsweise

350 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 f. und N 26; ebenso zur falschen Beschreibung des Rechtsgebietes Rossnagel, digma 2011, 160 ff., 160; vgl. Forstmoser, digma 2003, 50 ff., 51; als unglücklicher Begriff bezeichnet von Bull, Computer, 3; Drechsler sprach in seinem Beitrag anlässlich der Konferenz zum Titel «Neue EU-Datenschutzgrundverordnung: Herausforderungen für Schweizer Unternehmen bei der Umsetzung», Europa Institut an der Universität Zürich, Donnerstag, 24. Mai 2018, Zürich, von weit verbreiteten «fake news», also Missverständnissen resp. Fehlinformationen, was die Beschreibung und Interpretation des Datenschutzgesetzes und weiter des schweizerischen Datenschutzrechts anbelangt; eine ähnliche Einschätzung findet sich bei Bull, Vision, Vorwort und 1 ff., der die publizistische Darstellung der Rechtsmaterie und unbegründete Behauptungen beklagt; zur Fehlbezeichnung auch Gächter/Werder, in: Epiney/Fasnacht/Blaser (Hrsg.), 87 ff., 88 f.; zum Ganzen vgl. dritter Teil, VII. Kapitel.

351 Den Begriff einer dualen Rechtsnatur des DSG verwendet in seinem Beitrag zur Rechtsanwendung bei internationaler Datenbearbeitung durch Private zutreffend Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.8.

352 Vgl. Art. 12 f. i. V. m. Art. 4 ff. DSG; Art. 1 i. V. m. Art. 30 ff. nDSG.

353 Hierzu dritter Teil, VII. Kapitel.

scheint geeignet, zumindest teilweise Definitionsdefizite bezüglich des Terminus des Privaten abzumildern. Eine solche Analyse wird zu Tage fördern, dass es nicht nur der rasante technische Fortschritt und die Kommerzialisierung von Personendaten als quasi-exogenen Faktoren sind, die das Datenschutzrecht auf den Prüfstand stellen.[354] Vielmehr sind die Ursachen für das Vollzugsdefizit sowie die Schwächen der heutigen Datenschutzgesetzgebung teilweise *endogen und rechtskonzeptioneller Natur*. Die Wirksamkeitsdefizite des DSG liegen teilweise in seinen Anknüpfungspunkten und den Strukturmerkmalen selbst. Dass dieser Teil sich eher am Rande mit der Totalrevision befasst, ist keineswegs bloss den Faktizitäten der Zeit geschuldet. Vielmehr finden sich hierfür starke inhaltliche Argumente, zumal die Strukturmerkmale auch in Zukunft dem DSG seine Charakteristika vermitteln. Gleichwohl werden diese – auch wenn sie beibehalten werden – teilweise in einem neuen Licht erscheinen durch die Einführung neuer Instrumente qua Totalrevision.

Der Entscheid, den *Dualismus als primäres Strukturmerkmal* des DSG in seiner Entstehungsgeschichte zu präsentieren, vermag als erneuter Anachronismus erscheinen und etwas Selbstverständliches zu adressieren: Die Zweiteilung des Rechts in einen «öffentlichen» und einen «privaten» Bereich prägt bis heute die Vorstellungen des kontinental-europäischen Rechts.[355] Allerdings: Die markanteste konzeptionelle Differenz zwischen dem DSG auch nach Totalrevision und der DSGVO ist diesem thematischen Aspekt zuzuordnen. Die DSGVO geht zu einem Monismus über; das DSG hält allerdings weitgehend diskussionslos an seinem Dualismus fest. Mit diesen Entwicklungen wird sichtbar, dass den Fragen rund um die *bereichsspezifischen Differenzierungen im Datenschutzrecht* herausragende Bedeutung zukommt.[356] Die Relevanz *systemischer Bezüge* für das Datenschutzrecht rückt allerdings in einem subjektivrechtlich geprägten Ansatz in den Hintergrund. Die Auseinandersetzung mit kontextuellen Herausforderungen des Datenschutzrechts ist bereits in der Debatte im Rahmen der Verabschiedung des ersten DSG ausgeprägt. Ihr widmen sich die nächsten Seiten. 236

354 Vgl. zu den Herausforderungen auch Bischof/Schweizer, digma 2011, 152 ff.
355 So auch sichtbar anhand der universitären rechtswissenschaftlichen Curricula.
356 Grundlegend hierzu m. w. H. bereits Buchner, 7 ff.

IV. Kapitel: Erstes Strukturmerkmal – Dualismus

> «L'élaboration longue et chaotique d'une loi fédérale sur la protection des données est à plus d'un titre exemplaire de ce qui se passe au niveau du processus législatif, lorsque des intérêts privés et économiques sont en jeu.»[357]

A. Die Gretchenfrage nach dem Ausgangspunkt

237 Die (gesetzgeberische) Geschichte wiederholt sich – in die Länge zogen sich ebenso die Arbeiten im Zuge der Totalrevision des DSG, nicht nur diejenigen im Zusammenhang mit der Verabschiedung eines ersten eidgenössischen Datenschutzgesetzes. Im historischen Teil wurde die Etablierung der Idee eines Zweikammersystems bezüglich der Kategorie des Privaten beschrieben.[358] Sie geht von einem Dualismus von öffentlich und privat aus. Dass dieses Zweikammersystem nicht schwarz-weiss und absolut etabliert ist, wird an verschiedenen Stellen, insb. anhand einer Auseinandersetzung mit dem Verhältnismässigkeitsprinzips sichtbar werden.[359] Gleichwohl lässt sich für das DSG – selbst nach seiner Totalrevision – die dualistische Struktur als ein Charakteristikum beschreiben.

238 Wie aber wurde und wird dieses Verhältnis aus datenschutzrechtlicher Perspektive insb. in der Schweiz thematisiert? Für eine Annäherung an den Datenschutz und damit auch das Verhältnis der Normgestaltung im Datenschutzrecht für Verarbeitungshandlungen durch Private einerseits und durch öffentlich-rechtliche Stellen andererseits war eine literarische Metapher prägend: «big brother is watching you».[360] In Orwells Worten klingt ein übermächtiger Staat als grosser Bruder an, der den kleinen, zerbrechlichen, machtunterlegenen Bürger durchleuchtet, überwacht und zum gläsernen Bürger degeneriert.[361] Ihm galt in den Anfängen die volle Aufmerksamkeit, ging man doch in der Zeit des Erlasses der ersten Datenschutzgesetze nicht davon aus, dass Private in gleichem Masse Personendatenbestände generieren und verarbeiten würden können.[362] Es

357 Jeanprêtre, AB 88.032, 5. Juni 1991, 944.
358 Erster Teil, III. Kapitel, A.
359 Zweiter Teil, V. Kapitel, 3.; zur Neueinbettung und Verblendung des Dualismus durch den Ausbau von Vorgaben, welche gemeinsam für beide Bereiche gelten, mit der Totalrevision vgl. dritter Teil, VIII. Kapitel, A.
360 Für die Schweiz seit der Veröffentlichung des PUK-Berichts schon Rüesch, AB 88.023, 13. März 1990, 132; Bründler, SJZ 1993, 129 ff., 129; vgl. Buchner, 26.
361 Vgl. beispielsweise Vesting, in: Ladeur (Hrsg.), 155 ff., 164; zum gläsernen Steuerpflichtigen vgl. Broger, zsis Monatsflash 7, 1 ff.
362 Hierzu der Hinweis von Simitis im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt besucht am 30. April 2021); Hoffmann-Riem, AöR 1998, 513 ff., 524 ff.; Vesting, in: Ladeur (Hrsg.), 155 ff., 165.

waren staatliche Stellen, die erste Grossrechenanlagen zum Einsatz brachten.[363] Die Diffundierung des Computers in die Gesellschaft hatte noch nicht stattgefunden.[364] Immerhin: Mit der Referenz auf den grossen Bruder Staat und der damit erfolgenden Anknüpfung an Verwandtschaftsbeziehungen wird bereits «ein (kleineres) Geschwister» impliziert. In der datenschutzrechtlichen Debatte sind damit Private, die Personendaten verarbeiten, gemeint.[365]

Die stark bildhafte Rhetorik unter diesem Aspekt – die für den rechtlichen Diskurs, der sich gerne fachlich-neutral präsentiert, so gar nicht passen will und gleichwohl in kaum einem juristischen Beitrag fehlt – lädt zu einigen Gedanken ein: 239

Chronologisch betrachtet ist es vorab der grosse Bruder als staatliche resp. amtliche resp. obrigkeitliche Stelle, dessen Personendatenverarbeitungen Widerstand und im Ergebnis auch die Forderung nach rechtlichen Beschränkungen auslösen. Wie im ersten Teil gezeigt, widmeten sich die Datenschutzgesetze der ersten Generation einzig der Regulierung von Datenbearbeitungen durch den Staat. Das erste Schweizer Datenschutzgesetz von 1993 dagegen reiht sich – nach einem langen Ringen um die Verabschiedung eines Normkomplexes auch für den privaten Bereich – in die zweite Generation ein:[366] Es formuliert Vorgaben für die Personendatenverarbeitung durch öffentliche Stellen des Bundes wie durch Private, vgl. Art. 2 Abs. 1 lit. a und lit. b DSG und Art. 2 Abs. 1 lit. a und lit. b nDSG. 240

Die *kognitive Annahme*, wie sie in der *Orwellschen Metapher* mitschwingt, hat im DSG Niederschlag gefunden: Das Hauptaugenmerk gilt der staatlichen Datenbearbeitung, die als grössere Bedrohung beurteilt und somit einer strengeren Regelung zugeführt wird als Personendatenverarbeitungen durch Private. Hierzu vertiefend was folgt: 241

Das DSG bleibt auch nach seiner Totalrevision ein *duales Gesetz* – ein Gesetz, das die Vorgaben für den öffentlichen Bereich des Bundes gegenüber dem privaten Bereich unterschiedlich gestaltet. Die besagte Differenzierung erfolgt sowohl in materiellrechtlicher wie auch verfahrensrechtlicher Hinsicht. Entsprechend war und bleibt die *bereichsspezifische Differenzierung ein charakteristisches Element* des schweizerischen Datenschutzgesetzes. Angelegt wurde sie im Zuge der Verabschiedung des ersten DSG. Eine komplette Vereinheitlichung i. S. der Identität der Normen für die Verarbeitung von Personendaten durch Private und 242

363 Simitis im Interview, abrufbar unter: <https://www.datenschutzzentrum.de/interviews/simitis/interview-simitis.mp3> (zuletzt besucht am 30. April 2021); Hoffmann-Riem, a. a. O.; Vesting, in: Ladeur (Hrsg.), a. a. O.

364 Von einer «Demokratisierung der Informationstechnologien» spricht Nissenbaum, 24, 1.

365 Ähnlich Buchner, 5.

366 Zur Generationeneinteilung Mayer-Schönberger, Information und Recht, 113 ff.; vgl. auch Weichert, in: Bäumler (Hrsg.), 158 ff., 160.

öffentliche Stellen des Bundes wurde – soweit ersichtlich – in der Schweiz bislang nicht dezidiert gefordert, auch nicht im Zuge der Totalrevision.[367]

243 Ein Bericht zur Totalrevision hält denn auch fest, dass das «einheitliche» Gesetz für den privaten und öffentlichen Bereich beibehalten, allerdings die Bestimmungen *soweit wie möglich* vereinheitlicht werden sollten.[368] Umgesetzt wird diese Annäherung über mehrere neue Instrumente, die *für beide Bereiche* gelten sollen: Exemplarisch zu nennen sind insofern die Vorgaben für den Datenschutz durch Technik und Voreinstellungen, Art. 7 nDSG; die Pflicht zur Erstellung eines Verarbeitungsverzeichnisses nach Art. 12 nDSG, die (annähernden) Vereinheitlichungen bezüglich der Informationspflichten nach Art. 19 nDSG oder die Datenschutz-Folgenabschätzung, Art. 22 nDSG.

244 Anders wurde die Vereinheitlichung der beiden Bereiche namentlich in Deutschland bereits im letzten Jahrhundert als richtungsweisend für die *Modernisierung des Datenschutzrechts* beschrieben.[369] Denn die sog. kleine Schwester – die Datenbearbeitung durch Private –, so wurde attestiert, sei längst ihren Kinderschuhen entwachsen: Im 21. Jahrhundert, für welches von der «elektronischen Eigenaufrüstung der Gesellschaft mit Datenverarbeitungstechnologien»[370] resp. der «Demokratisierung der Informationstechnologien»[371] gesprochen wird, werde das Individuum nicht nur von Datenbearbeitungen durch den grossen Bruder Staat bedroht, sondern auch und gerade durch Private wie Google, Facebook usf.[372] Die Forderung auf eine Vereinheitlichung wird nicht zuletzt mit der *Vergleichbarkeit der Bedrohungslage* begründet, die von Personendatenverarbeitungen durch staatliche Behörden und Private, insb. den Internetgiganten, ausgeht.[373] Zudem wurde der *Zugriff der Behörden auf die infolge eines Regimes mit niedrigerem Schutzniveau erlangten Personendaten der privaten Akteure pro-*

367 Vgl. immerhin Baeriswyl in: Baeriswyl/Rudin (Hrsg.), 47 ff., 59, demgemäss sich die ursprüngliche Unterscheidung zwischen Datenbearbeitungen im öffentlichen gegenüber dem privaten Bereich kaum mehr durchführen lasse.

368 Bericht der Begleitgruppe Revision DSG vom 29. Oktober 2014, Normkonzept zur Revision des Datenschutzgesetzes, 8.

369 M. w. H. Buchner, 36 f.

370 So Vesting, in: Ladeur (Hrsg.), 155 ff., 157 ff., insb. 161 f.

371 So Nissenbaum, 24, 1; vgl. auch zur Digitalisierung des Alltags Richter, in: Mehde/Ramsauer/Seckelmann (Hrsg.), 1041 ff.

372 Vgl. Hassemer, in: Simon/Weiss (Hrsg.), 121 ff., 126 f.; Buchner, 1 und 26 ff.; heute sind es nicht mehr nur Informations- und Kommunikationstechnologien, die in die Gesellschaft diffundiert sind. Vielmehr sind unzählige Alltagsgegenstände wie Autos, Kühlschränke usf. mit Informationsverarbeitungstechnologien ausgerüstet – vgl. zum Phänomen des Internet of Things mit einem Fokus auf vertragsrechtliche Fragestellungen z. B. Eggen, AJP 2016, 1131 ff.; zum weiteren Phänomen der Informatisierung des Alltags, insb. durch ubiquitous computing, die Beiträge gesammelt von Friedemann (Hrsg.), *passim*; zum Paradigmenwechsel mit seiner Abkehr von Grossrechnern in staatlicher Hand hin zu Kleinstrechnern Rudin, digma 2001, 126 ff., 127 f.; zur Durchdringung des Alltages der Informations- und Kommunikationstechnologien Mattern, in: Mattern (Hrsg.), 11 ff.

373 M. w. H. und kritisch zu dieser kognitiven Annahme Vesting, in: Ladeur (Hrsg.), 155 ff., 156 ff., insb. 160 ff.; ebenso kritisch Buchner, 44 ff.

blematisiert.[374] Eine mögliche regulatorische Schlussfolgerung könnte sein, die Personendatenverarbeitung durch Behörden wie Private identischen Vorgaben zu unterwerfen.[375]

245 Ebendiesen Schritt hat die Europäische Datenschutz-Grundverordnung, in Kraft seit dem 25. Mai 2016, vollzogen. Ihre Vorgaben sind gleichermassen auf öffentliche wie private Verantwortliche anwendbar. Ungeachtet dessen, dass die Totalrevision von diesen Entwicklungen in der EU mitangestossen war – die Implementierung eines Monismus stand nicht zur Debatte.[376]

246 In der Schweiz sind die datenschutzrechtlichen Auseinandersetzungen bis heute von einer starken Position zugunsten privatwirtschaftlicher Erwägungen geprägt. Ihr gemäss sollen Personendatenverarbeitungen durch Private resp. der private Bereich datenschutzrechtlich so weit wie möglich als freier Bereich gestaltet werden.[377] Illustrativ hierfür ist das im Zuge der Schaffung des ersten eidgenössischen Datenschutzgesetzes erfolgte Ringen, *überhaupt* einen Normkomplex für den privaten Bereich verabschieden zu können. Die Schaffung eines Normenkomplexes, auch für Personendatenverarbeitung durch Private, war während des gesamten Prozesses strittig; die Debatte prägte den gesamten Gesetzgebungsprozess.

247 Es lohnt sich, *Relevanz und Argumente dieser bereichsspezifischen Debatte im Rahmen der Verabschiedung eines ersten eidgenössischen Datenschutzgesetzes* genauer nachzuvollziehen. In der Schweiz bezog namentlich Tercier zur Notwendigkeit einer Datenschutzgesetzgebung, die sich auch auf den privaten Bereich erstrecken sollte, unmissverständlich Stellung:

> «Est-ce que les articles 28 ss ne suffisent pas? Ma réponse, et c'est ma conviction, est clairement non […]. Les articles 28 ss du Code civil ne donnent pas un arsenal suffisant. Pourquoi? Au moins pour deux raisons principales. La première, c'est que les articles 28 ss fonde sur des formulations à caractère très général. Or, nous sommes dans un domaine où les généralités ne suffisent pas. Il faut des notions claires, garantissant une sécurité juridique suffisante. Deuxièmement avec l'article 28, pour les ordinateurs en tout cas, on est dans un domaine où les armes du droit civil ne suffisent plus […].»[378]

248 Das Zitat dokumentiert, dass in der Schweiz von Anfang an Überzeugungsarbeit geleistet werden musste, um für den privaten Sektor *überhaupt* eine spezifische Datenschutzgesetzgebung erlassen zu können. Die Richtung, aus welcher sich der Schweizer Gesetzgeber der Datenschutzgesetzgebung annäherte, war damit vorgegeben.

374 Vesting, 72.
375 Grundlegend Ders., *passim*.
376 Hierzu dritter Teil, VIII. Kapitel.
377 BBl 1988 II 414 ff., 418 ff., insb. auch 428 ff.
378 Vgl. Danioth, AB 88.032, 13. März 1990, 125 ff., 126.

249 Eine Entscheidung, *dass* der private Sektor ebenso einer datenschutzrechtlichen Regelung zuzuführen sei, sagt noch nichts darüber aus, wie weit Schutzinstrumente und Schutzniveau für den privaten und den öffentlichen Bereich des Bundes einander angenähert werden sollen oder inwieweit die Normen für den öffentlichen gegenüber dem privaten Bereich im Datenschutzrecht differenziert oder (punktuell) einheitlich geregelt werden sollen.[379]

250 Das zumindest theoretisch markanteste und wirkungsmächtigste Instrument zur Gestaltung eines datenschutzrechtlichen Regimes ist die Fixierung des *Ausgangspunktes hinsichtlich der Personendatenverarbeitung: Freiheit der Datenbearbeitung als Grundsatz mit Schranken* einerseits oder *Verarbeitungsverbot als Grundsatz mit Erlaubnistatbeständen* andererseits.[380] Dass der Entscheid für den Ausgangspunkt ein leitendes Ordnungsprinzip des Datenschutzrechts ist, wurde in der Schweiz bislang ungenügend zur Kenntnis genommen. Erst im Zuge der Totalrevision wurde dieser Aspekt vermehrt thematisiert.[381]

251 Der gesetzgeberisch gewählte Ausgangspunkt stellt ein strukturelles Kernelement für die datenschutzrechtliche Konzeptionierung und für das Schutzniveau dar. Entsprechend dient er auch als Instrument zur bereichsspezifischen Differenzierung oder Angleichung.[382] Der Entscheid für einen bestimmten Ausgangspunkt ist anders gewendet ein *Kerninstrumentarium* zur Erreichung eines bestimmten Schutzniveaus, auch wenn sich die beiden Mechanismen annähern lassen: je grosszügiger die Erlaubnistatbestände im Grundsatz des Verarbeitungsverbotes, je schärfer die Verarbeitungsverbote resp. -schranken im Grundsatz der Verarbeitungsfreiheit, desto deutlicher die Annäherungen zwischen den beiden «Extrempolen». Umgekehrt liegt die Extremlösung für ein maximal divergierendes Schutzniveau für den öffentlichen und den privaten Sektor theoretisch gesprochen darin, für einen Sektor ein Verarbeitungsverbot mit eng formulierten Ausnahmetatbeständen zu definieren und für den anderen Sektor die Freiheit der Datenbearbeitung mit rudimentären Verarbeitungsverboten festzulegen.[383]

252 Dem Entscheid dürfte *präjudizierende* Wirkung zugemessen werden in dem Sinne, dass sich nicht nur die weiteren Gesetzesnormen, sondern auch die Rechtsauslegung daran zu orientieren haben: Ein Bereich, der als prinzipiell freier resp. nicht durchregulierter Bereich konzipiert wird, sollte konsequent gestaltet

379 Grundlegend hierzu Buchner, 5 ff.
380 Vgl. hierzu ebenso Ders., 80 ff.; für die USA und den Beginn dieser Vision in den 1930er Jahren Regan, xii.
381 Rosenthal, Jusletter 16. November 2020, N 7 ff.; Glatthaar, 1.
382 Man könnte an dieser Stelle geneigt sein zu folgern, dass der Ausgangspunkt das Schutzniveau des Datenschutzrechts selbst ist. Dass dem nicht so ist, wird an späterer Stelle deutlich werden, wo auf weitere Instrumente, die das Schutzniveau mitgestalten, eingegangen wird.
383 Zum Ganzen Buchner, 80 ff.

werden. Zudem sind auslegungsbedürftige Bestimmungen systemkongruent zu interpretieren.[384]

253 Die nachfolgenden Ausführungen wollen vor diesem Hintergrund in Erinnerung rufen, wie zentral das Ringen um ein Datenschutzgesetz für den privaten Bereich und in der Folge die Frage nach der differenzierten Gestaltung der Vorgaben für den öffentlichen und den privaten Bereich in der Schweiz war. Im schweizerischen Schrifttum vermochte sich die grundlegende Bedeutung der Differenzierung resp. der Nichtdifferenzierung zwischen Privatrecht und öffentlichem Recht im Datenschutz, basierend auf einer Analyse stichhaltiger und sachlicher Argumente, bislang nicht abzubilden. Im Zuge der Totalrevision wurde das Konzept nicht ernsthaft verhandelt; immerhin thematisiert die Lehre den Ausgangspunkt gemäss DSG. Anhand des politischen Prozesses im Rahmen der Verabschiedung des ersten Datenschutzgesetzes lässt sich die Relevanz der bereichsspezifischen Auseinandersetzung herausarbeiten. Insofern soll auch beleuchtet werden, welche strukturellen Entscheidungen die Differenzierung dazumals prägten. Es geht insofern zum einen um den gewählten Ausgangspunkt für die Personendatenverarbeitungen für den privaten resp. den öffentlichen Bereich. Zum anderen sind weitere Elemente zu beschreiben, die dazu Anlass geben, das DSG – namentlich wegen des entgegengesetzten Ausgangspunktes – als *duales Regime* zu qualifizieren. Eine Charakterisierung, die für ein Gesetz, das gemeinhin als Einheitsgesetz beschrieben wird, nicht offensichtlich ist.[385] Verschiedenes gilt es bereits an dieser Stelle anzufügen: Erstens finden sich auch im DSG gemeinsame Schnittmengen der Normierung für den öffentlichen gegenüber dem privaten Bereich, insb. anhand der gemeinsamen Verarbeitungsgrundsätze. Das Verhältnismässigkeitsprinzip, das in seiner öffentlichen Natur auch für den privaten Bereich gilt, führt zu einer teilweisen Annäherung der beiden Regime: Ein öffentlich-rechtliches Prinzip annektiert quasi den privaten Bereich. Zudem bringt die Totalrevision gewisse Modifikationen durch Einführung neuer Instrumente, die für beide Bereiche gelten. Mit ihnen geht zwar keine Anpassung des materiellrechtlichen Grundsatzentscheides in Bezug auf den Ausgangspunkt einher. Gleichwohl stellen diese für beide Bereiche vorgeschriebenen Instrumente zur Umsetzung einer Datenschutz-Compliance den Dualismus in ein etwas anderes Licht.

384 Der Befund hat namentlich auch für ein Regelungsregime hohe Bedeutung, das generalklauselartig normiert; vgl. hierzu zweiter Teil, V. Kapitel.

385 Vgl. zur Titulierung als Einheitsgesetz durch Bundesrat Koller, AB 88.032, 5. Juni 1991, 948; Danioth, AB 88.032, 13. März 1990, 127; Ders., in: Schweizer (Hrsg.), 9 ff., 9.

B. Duales Einheitsgesetz

1. Von Titulierung und Inhalt

> «Die Notwendigkeit von datenschutzrechtlichen Regeln sowohl für den privaten wie den öffentlichen Bereich zu bejahen, warf die Frage – ich möchte sogar sagen: die Kontroverse – auf, ob es sinnvoll und angezeigt sei, die Bestimmungen der beiden Rechtsgebiete in je einem separaten Erlass zu behandeln oder in einem einzigen Erlass zusammenzufassen, wie es der Bundesrat vorschlägt. Die Kommission hat die Vorteile eines Einheitsgesetzes höher gewichtet als unbestreitbare Nachteile.»[386]

254 1992 trat auf eidgenössischer Ebene ein Datenschutzgesetz in Kraft, das die Verarbeitung personenbezogener Daten für den öffentlichen Bereich des Bundes wie auch im privaten Sektor normierte. Unter dem sog. *persönlichen Geltungsbereich* definiert das DSG seinen Adressatenkreis und verankert mit Art. 2 Abs. 1 lit. a DSG, dass das DSG für die Bearbeitung von Daten durch *Private* – gemäss lit. b auch für diejenige durch die *Bundesbehörden* – einschlägig ist.[387]

255 Diese Regelung in Bezug auf die Adressaten steht im Einklang mit der verfassungsrechtlichen Kompetenzausscheidung.[388] Aus der privatrechtlichen Regelungskompetenz ergibt sich ebenso die Kompetenz, im Bereich des privatrechtlichen Datenschutzes zu normieren.[389] Sodann ist der Bund zuständig, das öffentliche Recht des Bundes zu erlassen, worauf auch die Regulierung der Datenbearbeitung durch Bundesorgane basiert. Nicht anwendbar ist das DSG grundsätzlich auf Personendatenverarbeitungen durch kantonale und kommunale Behörden;

386 Danioth mit Verweis auf eine ähnliche, vereinte Regelung im UWG oder Kartellrecht, AB 88.032, 13. März 1990, 127.

387 Identisch nach Totalrevision Art. 2 Abs. 1 nDSG; Abgrenzungsschwierigkeiten können sich insb. im Rahmen der Wahrnehmung öffentlicher Aufgaben durch privatrechtlich angeknüpfte Unternehmen ergeben. Auf eine Vertiefung dieses Themas wird verzichtet.

388 Art. 3 BV sieht als Grundregel für die bundesstaatliche Kompetenzverteilung das Prinzip der Einzelermächtigung vor, wonach der Bund nur über jene Zuständigkeiten verfügt, die ihm die Bundesverfassung zuweist. Hierbei lautete Art. 3 BV 1848 und 1874: «Die Kantone sind souverän, soweit ihre Souveränität nicht durch die Bundesverfassung beschränkt ist, und üben als solche alle Rechte aus, welche nicht der Bundesgewalt übertragen sind.» Die aktuelle Version ist seit der Revision 1999 in Kraft, vgl. insb. auch Art. 42 BV: «Der Bund erfüllt die Aufgaben, die ihm die Bundesverfassung zuweist.» Art. 42 f. wurden mit der Revision 1999 eingeführt, die Subsidiaritätsklausel später gestrichen bzw. in Art. 5a und Art. 43a BV verschoben. Die einzelermächtigenden Kompetenzen des Bundes auf dem Gebiet des Privatrechts waren Art. 64 aBV sowie die Verfassungsnorm zur Erhaltung der Lauterkeit im Geschäftsverkehr, Art. 31 bis Abs. 2 aBV. Die Zivilrechtskompetenz des Bundes geht teils auf das Jahr 1874 zurück (BV 1874 Art. 64 Abs. 1: insb. wirtschaftsrelevante Bereiche; vgl. auch BV 1874 Art. 53 Abs. 1), teils auf das Jahr 1898 (BV 1874 Art. 64 Abs. 2: übrige Gebiete des Zivilrechts), teils auf das Jahr 1905 (BV 1874 Art. 64 Abs. 1: Patente, Muster und Modelle) zurück, vereinzelt sogar auf das Jahr 1848 (BV 1848 Art. 49: Vollstreckung rechtskräftiger Zivilurteile). Heute obliegt dem Bund die Regelung des Privatrechts aufgrund von Art. 122 Abs. 1 BV.

389 Zu diesem Anwendungsbereich Art. 2 Abs. 1 lit. a DSG; nach Totalrevision Art. 2 Abs. 1 lit. a nDSG.

insofern greifen die kantonalen Datenschutzgesetze. Deren Einhaltung wird von kantonalen Datenschutzbeauftragten überwacht.[390]

256 Das eidgenössische Datenschutzgesetz formuliert in den Art. 4 ff. DSG resp. nach Totalrevision gemäss Art. 6 nDSG unter den «allgemeinen Bestimmungen» *gemeinsame Verarbeitungsgrundsätze für beide Bereiche*. Diese allgemeinen Grundsätze, die Leitplanken für beide Bereiche setzen, weisen Parallelen zum Einleitungstitel des ZGB auf, und zwar in *zweifacher Hinsicht*: Es handelt sich zum einen um die grundlegenden Prinzipien des Datenschutzrechts, die für beide Bereiche Wirksamkeit entfalten sollen. Vergleichbare Grundsätze formuliert die Europäische Datenschutz-Grundverordnung in Art. 5 DSGVO. Die allgemeinen Verarbeitungsgrundsätze erfüllen anders gewendet eine Art Leitsternfunktion für beide Bereiche, ähnlich wie der Einleitungstitel des ZGB mit seinen fundamentalen Prinzipien für das gesamte Privatrecht (und keineswegs bloss für das ZGB) wirksam werden soll (oder gar darüber hinaus wirkt).[391] Zum anderen werden im Datenschutzgesetz zentrale Prinzipien des Einleitungstitels wie Treu und Glauben zu allgemeinen Verarbeitungsgrundsätzen gemacht.[392] *Materiellrechtlich* sind sie das Herzstück des Datenschutzgesetzes. Allerdings, so wird zu zeigen sein, sind die allgemeinen Verarbeitungsgrundsätze im DSG – anders als in der DSGVO – für den öffentlichen und privaten Bereich *in zwei unterschiedliche Systeme* eingebettet. Ebendies führt zu einer signifikanten Unterschiedlichkeit der datenschutzrechtlichen Regime.

257 Für das DSG hat sich, weil es die Personendatenverarbeitung durch Bundesbehörden wie Private normiert, die Beschreibung *Einheitsgesetz* etabliert.[393] Allerdings vermag diese Titulierung den strukturellen Gehalt des DSG nicht abzubilden – im Gegenteil wird mit dem Titel ein Rechtskonzept assoziiert und suggeriert, das sich im Gesetz gerade nicht findet. Dass nach DSG für den privaten und den öffentlichen Sektor beträchtliche Divergenzen gelten, rückt mit der Benennung und Qualifizierung des DSG als Einheitsgesetz aus dem Blickfeld. Die Titulierung überdeckt die eigentliche *materiellrechtliche Kernfrage* jeder datenschutzrechtlichen Regulierung und die hierzu getroffenen Entscheidungen:[394] diejenige nach der bereichsspezifischen Differenzierung oder auf deren Verzicht.

390 Vgl. zum föderalistischen System der Schweiz, das sich auch im Datenschutzrecht niederschlägt, Rudin, SJZ 2009, 1 ff.; zum datenschutzrechtlichen Regelungsgefecht, dem DSG, den kantonalen Datenschutzgesetzen sowie den Spezialgesetzen vgl. Epiney/Hofstötter/Meier/Theuerkauf, 221 ff.

391 Honsell, BSK-ZGB I, Einleitung vor Art. 1 ff. N 1.

392 Allerdings: Während dem Einleitungstitel des ZGB konkretisierende und ausgereifte Normenkomplexe mit erheblicher Regelungsdichte zu den einzelnen Verhältnissen folgen, bleiben die hoch abstrakten Grundsätze von Art. 4 ff. DSG resp. Art. 6 nDSG weitgehend ohne nähere Konkretisierung für den datenschutzrechtlichen Kontext.

393 Vgl. Art. 2 DSG und Art. 2 nDSG; s. EJPD, Bericht Begleitgruppe, 3; vgl. z. B. Danioth, AB 88.032, 13. März 1990, 127; BBl 1988 II 414 ff., 431; Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 6.

394 Dazu namentlich für Deutschland Vesting, in: Ladeur (Hrsg.), 155 ff., 156 ff.; Buchner, *passim*.

258 In der Entscheidung für eine vereinheitlichte resp. monistische Normierung schlägt sich die Überzeugung nieder, dass die Bedrohungen, die von Datenverarbeitungen durch den Staat und Private unter den Gegebenheiten moderner Verarbeitungstechnologien ausgehen, vergleichbar, ja identisch sind und folglich eine rechtliche Differenzierung nicht sachgemäss erscheint – so der Ansatz in der DSGVO. Im Entscheid für ein materiellrechtlich zweigeteiltes Datenschutzrecht manifestiert sich hingegen die Überzeugung, dass grundsätzliche Unterschiede zwischen den Bearbeitungskontexten bestehen.[395] In der Schweiz hat sich letztere durchgesetzt und gehalten. Die Differenzierung zwischen den beiden Bereichen im schweizerischen Datenschutzgesetz wurde zwar von fachlichen und sachlichen Argumenten mitgetragen, war allerdings bei Lichte betrachtet stark von *politischen Kräften* getrieben; namentlich die Interessen vonseiten der Privatwirtschaft nahmen massgeblichen Einfluss.[396]

259 Wer das eidgenössische Datenschutzgesetz als *Einheitsgesetz* in der Hand hält, realisiert wenig von der Brisanz, Virulenz und Spannungshaftigkeit, aus der es damals hervorging. Lässt man die Stellungnahmen vonseiten der Expertengremien sowie die Voten in den Räten Revue passieren, kommt schnell ans Licht, wie kontrovers über Schutzniveau und Regelungsinstrumente für den privaten und den öffentlichen Sektor sowie über das Verhältnis der Datenschutzgesetzgebung für die beiden Bereiche debattiert wurde. Die Gesetzgebungsmaterialien dokumentieren die *politischen Kräfte und Dimensionen*, die hinter dem eidgenössischen Datenschutzgesetz als Einheitsgesetz wirk(t)en.

260 Illustrativ insofern der strategische Entscheid, beide Sektoren formell in einem Gesetz zur Abstimmung zu bringen: Er erfolgte aus *politischem Kalkül*.[397] Denn während die Normierung für den öffentlichen Sektor Rückenwind genoss, sah sich diejenige für den privaten Sektor starkem Gegenwind ausgesetzt. Nur indem *ein* Gesetz für beide Bereiche vorgelegt wurde, konnte Schiffbruch und eine (partielle) Ablehnung einer Gesetzgebung für den privaten Sektor verhindert werden. Zwar wurde hinterfragt, ob dieses Vorgehen mit den politischen Rechten und namentlich dem Grundsatz der Einheit der Materie im Rahmen der Gesetzgebung im Einklang stand.[398] Das fusionierende Vorgehen schien – nicht zuletzt, weil es sich beim Datenschutz um eine sog. Querschnittsmaterie handle – gleichwohl als opportun und legitim.[399] Im Ansatz wurde eine Überzeugung dokumentiert, wonach es für das Individuum, dessen Schutz im Zentrum stünde, nicht relevant sei, ob Datenbearbeitung durch den Staat oder Private erfolge.[400] Wie aber gestaltete

395 Buchner, 5.
396 Hierzu sogleich 2., wo der Weg zum Zweikammersystem abgeschritten wird.
397 Forstmoser, digma 2003, 50 ff., 50 f.
398 Müller, LeGes 2013, 507 ff., 507.
399 Danioth, AB 88.032, 13. März 1990, 127; Nabholz, AB 88.032, 5. Juni 1991, 940.
400 Vgl. Küchler, AB 88.032, 13. März 1990, 128 f.

sich der Prozess des Austarierens datenschutzrechtlicher Normierung(en) für den privaten und den öffentlichen Sektor im Folgenden und Einzelnen?

2. Der Weg zum datenschutzgesetzlichen Zweikammersystem

Den langwierigen Gesetzgebungsprozess im Rahmen der Verabschiedung des ersten eidgenössischen Datenschutzgesetzes retrospektiv nachzuzeichnen, ist kein einfaches Unterfangen.[401] Eine solche Rückblende über das erst gerade abgeschlossene Gesetzgebungsprojekt der Totalrevision ist für diese Studie und ihre Forschungsfragen allerdings unverzichtbar. Sichtbar wird damit, welcher Stellenwert der Frage der bereichsspezifischen Differenzierung zugewiesen wurde und welche Argumente insofern vorgetragen wurden. Im Ergebnis wurde ein Gesetz verabschiedet, dessen *erstes Charakteristikum in seiner dualistischen Struktur* liegt. 261

Der Gesetzgebungsprozess, der zur Verabschiedung des ersten eidgenössischen Datenschutzgesetzes führte, war vom Druck und Widerstand vonseiten der *Wirtschaftsakteure* auf die datenschutzrechtliche Normierung für den privaten Bereich geprägt.[402] Unbestritten war, dass nicht nur für die moderne Leistungsverwaltung Personendaten unverzichtbar seien, sondern auch für private Versicherungsunternehmen, Kreditinstitute oder Arbeitgeber.[403] Dies reflektierend sollte eine Normierung für den privaten Sektor der Bedeutung von Informationsbeschaffungen und dem wirtschaftlichen Wettbewerb Rechnung tragen.[404] Die konkrete Ausgestaltung des Datenschutzgesetzes für den privaten Sektor gegenüber dem öffentlichen Sektor beschäftigte die involvierten Akteure während des gesamten Gesetzgebungsprozesses. Die Verhandlungen insofern waren mit hoher Ambivalenz belegt und sind als eigentlicher Brennpunkt der schweizerischen Datenschutzgesetzgebung zu bezeichnen. 262

In Bezug auf den Aspekt des *Dualismus* ist vorab relevant, dass der dazumal amtierende Vorsteher des EJPD, Altbundesrat Furgler, *im Vorfeld* richtungsweisende Entscheidungen traf: Einerseits sollte bundesgesetzlich sowohl die Personenbearbeitung durch Private wie durch Bundesbehörden geregelt werden, wohingegen die Bearbeitung durch kantonale und kommunale Behörden mangels einer allgemeinen Kompetenznorm im Bereich des Datenschutzes der kantona- 263

401 Von einer wechselvollen Geschichte, die ihren Anfang mit der Motion Bussey im Jahr 1971 nahm, spricht Kleiner, in: Brem/Druey/Kramer/Schwander (Hrsg.), 397.

402 Jaggi, AB 88.032, 13. März 1990, 161 f. mit Hinweis auf die Konzessionen in den Domänen Direktmarketing, Kreditauskunfteien und die Kompetenzen des EDÖB; der politische Druck vonseiten der wirtschaftlichen Kreise nahm seinen Anfang bei den Arbeiten der Kommissionen.

403 Forstmoser, SJZ 1974, 217 ff., 218.

404 BBl 1988 II 414 ff., 430 und 434; grundlegend zu Ansprüchen auf Informationsbeschaffungen vor der Verabschiedung des DSG vgl. Hauser, 19 ff.

len Normierung oblag. Andererseits wurde die Einsetzung zweier verschiedener Expertengruppen beschlossen: Die erste wurde 1977 mit der Ausarbeitung von Datenschutzvorschriften für die Bundesverwaltung beauftragt, die zweite 1979 mit derjenigen für den privaten Bereich. Beide Arbeitsgruppen standen unter der Leitung von Pedrazzini.[405] Vonseiten der mit der Ausarbeitung betrauten Stellen und Personen hielt man es von Anfang an für *sachgerecht*, eine differenzierende Regelung für beide Sektoren zu veranlassen. Man orientierte sich entsprechend an einem fest etablierten Konzept eines «Zweikammersystems», dessen eine Kammer der Privatrechtsbereich und dessen andere Kammer der öffentlich-rechtliche Bereich darstellt.[406]

264 Die erste Expertengruppe legte Ende 1981 einen Vorentwurf für ein Bundesgesetz über den Datenschutz im Bereich der Bundesverwaltung vor.[407] Die zweite Expertenkommission präsentierte ihren Gesetzesentwurf für den privatrechtlichen Sektor im Sommer 1982. Als die beiden Vorentwürfe vorlagen, erteilte der Vorsteher des EJPD den bemerkenswerten Auftrag, diese *in einem einzigen Gesetz zusammenzulegen*. In diese Fusion des Vorentwurfs für ein Bundesgesetz über den Datenschutz im Bereich der Bundesverwaltung von 1981 und des Vorentwurfs für den privatrechtlichen Bereich von 1982 wurden zudem die Ergebnisse des Berichts und die Empfehlungen für den Medizinalbereich integriert, deren Erarbeitung unter der Leitung von Jaggi stand. Das Ergebnis war der *Vernehmlassungsentwurf von 1983*.[408]

265 Mehrere Gründe standen hinter dem Entscheid, die verschiedenen Regelungsbereiche – obschon man von Anfang an einem differenzierten System zuneigte – in *einem* Gesetz zu fusionieren: Vorab sprach als *sachlogisches Argument* für die Zusammenlegung der beiden Bereiche der Befund, dass Datenschutz eine *Querschnittsmaterie* sei und entsprechend gesetzlich ein gemeinsames Fundament für beide Bereiche vorgesehen werden sollte.[409] So sollten Leitprinzipien der Datenverarbeitung, wie sie sich in Gestalt allgemeiner Bearbeitungsgrundsätze in ausländischen Rechtsordnungen Anerkennung verschafft hatten, auch im Schweizer Datenschutzgesetz gelten, und zwar für beide Bereiche. Dazu sollte ein prozedurales Instrumentarium gleichermassen in beiden Feldern zum Einsatz kommen, namentlich Auskunftsrechte, aber auch die Funktion eines Datenschutzbeauftragten. Gleichzeitig sollte mit der Zusammenlegung einer Kritik an der Gesetzesflut entgegengetreten werden: Der Verabschiedung eines einzigen

405 Seethaler, BK-DSG, Entstehungsgeschichte DSG, N 27 f.
406 Die in dieser Schrift als «pointierter Dualismus» beschriebene Rechtsgestaltung ist ein Element insofern.
407 BBl 1988 II 414 ff., 426 f.; zum Ganzen vertiefend Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 18.
408 BBl 1988 II 414 ff., 426.
409 Danioth, AB 88.032, 13. März 1990, 126.

Gesetzes wurden vor dem Hintergrund dieses Einwandes bessere Erfolgschancen zugemessen.[410]

Das Hauptargument für die Zusammenlegung lag allerdings – wie gezeigt – an anderer Stelle: Früh zeichnete sich ab, dass einer allgemeinen Datenschutzgesetzgebung für den privaten Sektor heftiger Widerstand erwachsen würde. Dass ein Gesetz für die Datenbearbeitung im öffentlichen Sektor Schiffbruch erleiden könnte, fürchtete angesichts der Vorkommnisse im EJPD und namentlich der Informationstätigkeiten der Bundesanwaltschaft kaum jemand. Der sog. Fichenskandal, der zur Einsetzung einer PUK geführt hatte, und der Bericht derselben, die dem Parlament zeitlich noch vor der Beratung des Datenschutzgesetzes vorgelegt worden war, hatte die Schweiz zutiefst erschüttert.[411] Ein Staat, der sich als Schnüffelstaat entpuppt hatte, gab einer Grenzen setzenden Gesetzgebung selbst den finalen Impetus. In der Folge galt als der neuralgischste Bereich der Datenbearbeitung derjenige durch Bundesorgane.[412] Die Zugkraft, die der politische Prozess zur Verabschiedung eines Datenschutzgesetzes für Datenbearbeitungen durch Bundesbehörden infolge des Fichenskandals entfaltete, konnte nun als starkes Vehikel für eine Normierung des privaten Sektors genutzt werden. Die Fusionierung war *primär politisches Kalkül.* 266

Mit der Zusammenlegung erfolgte sodann nicht nur eine *Reduzierung des Umfangs* auf rund die Hälfte der ursprünglich entworfenen Bestimmungen. Gleichzeitig wurden bereits erste Konzessionen bezüglich der Vorgaben für den privaten Bereich gemacht.[413] So sollte etwa das Auskunftsrecht nicht voraussetzungslos gelten – vielmehr sollte die Auskunft infolge eines überwiegenden Interesses verweigert werden können. 267

Zu diesem ersten Vernehmlassungsentwurf von 1983 hielt der von 2001–2015 amtierende Datenschutz- (und später Öffentlichkeits-)beauftragte Thür fest: 268

> «[A]ls das erste Vernehmlassungsverfahren durchgeführt wurde und der erste Expertenentwurf vorlag, war das Resultat vernichtend. Vor allem von wirtschaftlichen Interessengruppen wurde ein eigentliches Sperrfeuer entfacht.»[414]

Während die Bestimmungen zum öffentlichen Sektor in der Vernehmlassung grundsätzlich gut aufgenommen wurden, stiessen die Normen zum Privatbereich bei den Arbeitgeber- und Wirtschaftsorganisationen – vorbehältlich der Konsu- 269

410 M. w. H. Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 17 ff., N 28 ff. und N 34 ff.; Forstmoser, digma 2003, 50 ff., 52.
411 Vgl. hierzu Kreis, digma 2009, 56.
412 Hilty, NZZ 1994, 22.
413 Zu diesen Abschwächungen im Zuge der Vereinigung Jaggi, AB 88.032, 13. März 1990, 131.
414 Thür, AB 88.032, 5. Juni 1991, 945.

mentenverbände – auf gänzliche Ablehnung.[415] Eine privatrechtliche Normierung wurde nicht nur per se kritisiert. Bemängelt wurde die geplante gemeinschaftliche Regelung für die beiden Sektoren, womit den grundlegenden konzeptionellen Unterschieden, so hiess es, nicht gebührend Rechnung getragen würde. Darüber hinaus mache ein Einheitsgesetz den Erlass zu kompliziert.[416] Die Vorgaben für den privaten Sektor seien zu umfangreich, engmaschig und komplex.[417] In diesem Sinne wurden vonseiten der Privatwirtschaft zwei getrennte Gesetze sowie eine Abschwächung der rechtlichen Vorgaben für gewisse wirtschaftliche Tätigkeiten, beispielsweise diejenigen, welche Kreditauskunfteien vornähmen, gefordert.[418] Dieser Vorstoss war seinerseits strategisch motiviert: Die Vertreterinnen und Vertreter der Privatwirtschaft versuchten, den Normenkomplex für den privatrechtlichen Sektor wieder zu isolieren, um ihn später verhindern zu können. Nicht nur der Bundesrat sah sich damit in seiner ursprünglichen Einschätzung bestätigt, wonach es ein prioritäres Ziel bleiben musste, *überhaupt* eine Regulierung für den privatrechtlichen Bereich zur Verabschiedung zu bringen.

270 Nach Kenntnisnahme der Ergebnisse der Vernehmlassung setzte der Bundesrat erneut eine Arbeitsgruppe unter der Leitung von Pedrazzini ein. Trotz der Einwände zum Vernehmlassungsentwurf und namentlich zum Vorwurf vonseiten der Privatwirtschaft, die den Vernehmlassungsentwurf für den privaten Bereich als einen zu hohen Vollzugsaufwand auslösend beurteilte, hielt man an der Überzeugung fest, dass die Persönlichkeit auch vor Datenbearbeitungen im privaten Sektor geschützt werden müsse. Der Auftrag an die Arbeitsgruppe war, eine entsprechende Überarbeitung an die Hand zu nehmen. Es resultierte ein gestraffter Entwurf, der sich weiterhin sowohl auf den öffentlichen wie den privaten Sektor erstreckte, die Bereiche aber gleichwohl stärker trennte. Allerdings erschien auch diese gestraffte Version der damaligen Departementsvorsteherin Kopp als zu komplex. Eine verwaltungsinterne Arbeitsgruppe unter der Leitung von Steinlin wurde mit einer weiteren Überarbeitung betraut. 1988 – also elf Jahre nach der Einsetzung einer Expertengruppe zur Erarbeitung eines Datenschutzgesetzes – wurde der Gesetzesentwurf mit Botschaft vom 23. März 1988 vorgelegt.[419] Ergänzend erfolgten Gesetzgebungsaktivitäten für bereichsspezifische Regulierungen, namentlich für den Medizinal- und Sozialversicherungsbereich.[420]

415 BBl 1988 II 414 ff., 429; vgl. Forstmoser, digma 2003, 50 ff., 53; dies geschah ungeachtet der bereits im Jahr 1985 zu findenden wissenschaftlichen Einschätzung, wonach die private Informationsverarbeitung intransparenter und unberechenbarer sei als die staatliche.
416 BBl 1988 II 414 ff., 428 ff.
417 M. w. H. Nabholz, in: Schweizer (Hrsg.), 1 ff., 2.
418 Hinweise bei Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 26 ff.; vertiefend zur Praxis der Kreditauskunfteien dritter Teil, VII. Kapitel, B.2.2.
419 Vgl. Ders., a. a. O.
420 Ders., a. a. O.

Die *Botschaft* äussert sich prioritär – einleitend und eindringlich – zur Notwendigkeit, den öffentlichen *und* den privaten Sektor einer Regulierung zuzuführen. Gefahren würden sowohl in Informationstätigkeiten von Bundesbehörden wie in denjenigen von Privaten lauern.[421] Mehrere Argumente leisteten alsdann die notwendige Überzeugungsarbeit für die Verabschiedung des Regelungskorpus für den privaten Bereich: Zunächst werden bedeutsame Gerichtsentscheide, die sich mit Persönlichkeitsverletzungen durch private Informationstätigkeiten befassten, aufgeführt.[422] Dabei gab man zu bedenken, dass Verletzungen der Geheim- resp. Privatsphäre nur selten publik würden, weil Private meist gar nicht wüssten, wer über sie Daten bearbeite. Dort, wo eine Verletzung vermutet werde und feststellbar sei, werde allerdings in der Regel eine Auskunft über die Datenbearbeitung verweigert. Eine gerichtliche Beurteilung von Persönlichkeitsverletzungen wegen Informationsverarbeitungen durch Private sei zudem mit erheblichen Prozessrisiken verbunden.[423] Als Beleg für den Bedarf einer privatrechtlichen Regelung werden sodann vorhandene Instrumente der Selbstregulierung privater Organisationen in Gestalt von berufsethischen Normen oder Standesregeln genannt.[424] 271

In den parlamentarischen Beratungen setzte sich die Kontroverse um das Verhältnis datenschutzrechtlicher Vorgaben für den privaten und den öffentlichen Sektor indes weiter fort. Erstberatend war der Ständerat; er verhandelte die Vorlage 1990. Es seien insofern die Worte des berichterstattenden Vertreters der vorberatenden Ständeratskommission Danioth aufgeführt: 272

> «Die Kommission […] bejahte einhellig die Notwendigkeit einer gesetzlichen Regelung des Datenschutzes auch im Privatrechtsbereich. Die unrühmlichen Vorkommnisse in der Bundesverwaltung dürfen nicht zur Annahme verleiten, in der Wirtschaft und anderen Bereichen seien keine Irrtümer und Missbräuche denkbar. Die Bejahung einer Gesetzgebung hat auch einen gleichsam rechtspraktischen Grund. Experten der Wissenschaft und der Praxis haben überzeugend dargetan, dass eine datenschutzrechtliche Konkretisierung des Persönlichkeitsschutzes durch den Gesetzgeber nicht zuletzt im Interesse der Wirtschaft und aller privaten Datenbearbeiter selber liegt […]. Im öffentlichen Bereich, das heisst bei der Bundesverwaltung, einen griffigen Datenschutz zu begründen, bedeutete wohl, Wasser in die Reuss oder in die Aare zu tragen. Die Aktualität lässt sich angesichts der sich jagenden Fichen-Enthüllungen kaum mehr überbieten. Unweigerlich muss man bedauern, dass der Gesetzgeber nicht schon lange gehandelt hat. Denn Letzterem wurde

421 BBl 1988 II 414 ff.; dazu, dass international wie national kein Datenschutzgesetzgeber zögerte, sich an die Adresse privater wie öffentlicher Stellen zu wenden, Simitis, NJW 1984, 394 ff., 401.

422 BBl 1988 II 414 ff., 418 f.

423 BBl 1988 II 414 ff., 420.

424 BBl 1988 II 414 ff., 419; der Selbstregulierungsansatz wird im revidierten Datenschutzgesetz aufgenommen, vgl. Botschaft DSG 2003, 2101 ff., 2138; zur Forderung auf eine Stärkung des Selbstregulierungsansatzes bereits um die Jahrtausendwende Rossnagel/Pfitzmann/Garstka, in: Bundesministerium des Inneren (Hrsg.), 43 ff.; vgl. zur Selbstregulierung sowie Zertifizierung unter Darstellung der hierzu vertretenen Ansichten betreffend die (Un-)Tauglichkeit der Selbstregulierung als Ausweg aus der Datenschutzkrise Pärli, digma 2011, 67 ff.; zur jüngsten Stärkung deskriptiv und ohne Evaluierung Hofmann/Meyer, Expert Focus 2017, 424.

> aus Wirtschaftskreisen starkes Misstrauen entgegengebracht. […] Die Notwendigkeit von datenschutzrechtlichen Regeln sowohl für den privaten wie den öffentlichen Bereich zu bejahen, warf die Frage – ich möchte sogar sagen: die Kontroverse – auf, ob es sinnvoll und angezeigt sei, die Bestimmungen der beiden Rechtsgebiete in je einem separaten Erlass zu behandeln oder in einem einzigen Erlass zusammenzufassen, wie es der Bundesrat vorschlägt. Die Kommission hat die Vorteile eines Einheitsgesetzes höher gewichtet als unbestreitbare Nachteile, was bei einer solchen Gesetzgebung übrigens nicht erstmalig ist (ich verweise auf das UWG, das Kartellrecht). Mit einem Einheitsgesetz wird dem Umstand Rechnung getragen, dass es sich um eine sogenannte Querschnittsmaterie handelt. Datenschutz ist nicht an Rechtskategorien gebunden.»[425]

273 Im *Ständerat* wurde von verschiedener Seite betont, dass das Gefahrenpotential im staatlichen Bereich deutlich höher sei als im privaten.[426] Folglich hatten nicht nur der Berichterstatter der ständerätlichen Kommission, sondern auch die Ständeräte selbst wiederum Überzeugungsarbeit für die privatrechtliche Normierung zu leisten. Es waren vorrangig Ständerätin Jaggi und Ständerat Onken, die sich in der kleinen Kammer für den privatrechtlichen Datenschutz engagierten. Rhinow – zu jenem Zeitpunkt nicht nur ordentlicher Professor für Staats- und Verwaltungsrecht an der Universität Basel, sondern auch Ständerat – nahm eine differenzierte Position ein:

> «Der moderne Sozialstaat zeichnet sich nicht nur durch einen Normenhunger, sondern auch durch einen hohen Bedarf an gespeicherten Personendaten aus […].»[427]

274 Zugleich plädierte er für eine Verbesserung des Datenschutzes ebenso für den privaten Sektor, weil Menschen in ihrer Persönlichkeit auch durch den Datenhunger privater Wirtschaftsunternehmer bedroht werden könnten. Entsprechend sei es richtig, beide Gebiete zu regeln, allerdings ebenso richtig, die beiden Gebiete unterschiedlichen Regelungsregimen zu unterstellen.[428]

275 Ebendieses Konzept – Regulierung für beide Gebiete *ja*, identische Regelung allerdings *nein* – setzte sich durch. Es war auch der Ständerat, der zugunsten der Verabschiedung eines DSG für beide Sektoren die Differenz zwischen öffentlichem und privatem Sektor nochmals akzentuierte. Im Ständerat erfolgten Zugeständnisse mit Blick auf die datenschutzrechtlichen Vorgaben für den privaten Sektor, namentlich die Erschwerung des Auskunftsrechts, die Ausklammerung und Abschwächung von Schutzmechanismen für spezifische Felder wie beispiels-

425 Danioth, AB 80.032, 13. März 1990, 126.
426 Vgl. Hefti, AB 80.032, 13. März 1990, 139.
427 Rhinow, AB 88.032, 13. März 1990, 130; vgl. etwas allgemeiner Pedrazzini zum staatlichen Informationsbedarf zur Erfüllung seiner Aufgaben, Wirtschaft und Recht 1982, 27 ff., 28, auch mit dem Hinweis, dass trotz des Fokus auf den öffentlichen Bereich der private Bereich nicht aus den Augen geraten dürfe.
428 Rhinow, a. a. O., 131.

weise Kreditauskunfteien, Adresshandel oder das Arbeitsverhältnis sowie die Beschneidung der Kompetenzen des ED(Ö)B.[429]

Als das Geschäft die *zweite Kammer,* den Nationalrat, im Dezember 1991 erreichte, hatte die Vorlage eine früh ein- und sich kontinuierlich fortsetzende Absenkung des Schutzniveaus für den privaten Sektor hinter sich. Längst hatte sich bestätigt, dass die Einschätzungen und Entscheidungen von Altbundesrat Furgler klug gewesen waren: Von Sacherwägungen motiviert, erfolgte eine je separate Erarbeitung eines Datenschutzkomplexes für den privaten und den öffentlichen Sektor; aus politischem Kalkül erfolgte die Zusammenlegung in einem Gesetz. Ein Gesetz, für dessen öffentlich-rechtlichen Teil die Entrüstung über die Fichenaffäre das Wort redete und das damit die notwendige Kraft hatte, die «kleine Schwester», die Normierung für den privatrechtlichen Bereich, mitzuziehen: 276

> «Wir sind immer wieder erstaunt darüber – nicht zuletzt angesichts der erhaltenen Lobbyistenpost aus Wirtschaftskreisen –, wie sehr der für uns zentrale Grundrechtsaspekt dieses Datenschutzes hinter wirtschaftlichen Interessenüberlegungen zurücktreten soll.»[430]

Auch Nationalrat Thür beklagte, dass eine immer offenkundigere Verschiebung weg von einem tragfähigen Expertenentwurf durch die herrschenden politischen Mehrheitsverhältnisse erfolgt war. Die Durchschlagskraft wirtschaftlicher Interessen habe das Gleichgewicht aus dem Lot gebracht, wie er nicht ohne Zynismus bemerkte: 277

> «Natürlich kann man darüber erleichtert und erbaut sein, dass es gelungen ist, wenigstens das Einheitsgesetz zu retten, dass also ein Auseinanderbrechen des Datenschutzgesetzes in einen öffentlich-rechtlichen Teil, der gesetzlich normiert wird, und einen privatrechtlichen, der auf den Weg des Zivilgesetzbuches verwiesen wird, verhindert werden konnte. Ich will diesen Teilerfolg, um den sich namentlich der Kommissionspräsident sehr bemüht hat, keineswegs geringschätzen. Doch welch ein Katalog von Zugeständnissen musste dafür gemacht werden? Welch hoher Preis musste bezahlt werden, um dieses Auseinanderbrechen zu verhindern?»[431]

Wie im Ständerat Rhinow wies im Nationalrat Nabholz darauf hin, dass sachlogische, genauer: verfassungsrechtliche Gründe – namentlich der Grundsatz der Privatautonomie – durchaus Anlass für die Differenzierung gäben. Entsprechend bedeute ein Entscheid für ein Gesetz, das sowohl Datenbearbeitungen durch Private als auch durch Bundesorgane erfasse, nicht zugleich, dass beide Bereiche identisch geregelt werden müssten. Ein weniger restriktives Regime für 278

429 Onken, AB 88.032, 13. März 1990, 129 f.; vgl. zur Beschneidung der Kompetenzen des EDÖB im Parlament und namentlich die Beschränkung auf eine Beratungsfunktion für den privaten Sektor Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 42.

430 Vollmer, AB 88.032, 5. Juni 1991, 943.

431 Onken, AB 88.032, 13. März 1990, 130.

den privaten Sektor sei im Interesse der Privatautonomie und zur Vermeidung einer überbordenden Datenschutzbürokratie durchaus denkbar. Allerdings wies Nabholz darauf hin, dass der Ständerat den Entwurf des Bundesrates im privatrechtlichen Teil zu stark entschlackt habe.[432] So waren die Konzessionen im Nationalrat und die Reduktion des Schutzniveaus im privaten Sektor zwar vorhanden, aber doch weniger einschneidend als im Ständerat.

279 Die parlamentarischen Beratungen dokumentieren, dass *die beiden Kammern unterschiedliche Kursrichtungen* verfolgten. Sie lassen sich in den Worten Danioths wie folgt wiedergeben:

> «[A]uf einen Nenner gebracht, kann man die Unterschiede so qualifizieren, dass der Nationalrat zu vermehrter Regelungsdichte neigte und insbesondere den Datenschutz im Privatrechtsbereich verstärkte beziehungsweise sich dem öffentlichen Normenstand in der Bundesverwaltung stark annäherte. Die Kommission des Ständerates hält daran fest, dass die unterschiedliche Interessenlage eine differenzierte Datenschutzgesetzgebung erfordert, was auch in einem Einheitsgesetz zum Ausdruck kommen muss: *Missbrauchsgesetzgebung* im Privatbereich, Verhaltensnormen im öffentlichen Bereich».[433] [Hervorhebung durch die Autorin]

280 Im Differenzbereinigungsverfahren allerdings wurden weitere Konzessionen vonseiten des Nationalrates erforderlich.[434] Bis die Differenzen – wiederum nach intensivem Ringen – bereinigt worden waren und für die Schweiz ein erstes DSG in Kraft trat, wurde das Jahr 1993 geschrieben. Kurz vor der Zielgeraden war es Bundesrat Koller, der im Differenzbereinigungsverfahren und in der zweiten Lesung im Ständerat für ein «zügiges Abschliessen» des langwierigen Prozesses plädierte und nun auch auf den Zeitdruck und die Relevanz des eidgenössischen Datenschutzgesetzes für die internationalen Beziehungen hinwies.[435]

281 *Zusammenfassend* ist für die Schweiz festzuhalten, dass es die Debatte um eine Datenschutzgesetzgebung auch für den privaten Bereich war, die den Gesetzgebungsprozess so langwierig machte. Den eigentlichen *Brennpunkt* im Rahmen der eidgenössischen Datenschutzgesetzgebung bildete entsprechend die Frage nach der Differenzierung des Datenschutzrechts für den öffentlichen und den privaten Bereich bis hin zu Standpunkten, die eine allgemeine Datenschutzgesetzgebung für den privaten Sektor verhindern wollten. Es gelang zwar, ein Gesetz für beide Bereiche zu verabschieden. Allerdings wurde das Schutzniveau für den privaten Sektor bei der Ausarbeitung des DSG *sukzessive* und in jedem Verfahrensstadium abgesenkt. Davon betroffen waren bestimmte Verarbeitungskontex-

---

432 Nabholz, AB 88.032, 5. Juni 1991, 940 f.
433 Danioth, AB 88.032, 5. Dezember 1991, 1018.
434 Vgl. Ders., AB 88.032, 13. März 1990, 228.
435 In seinen Worten anlässlich der Sitzung vom 10. März 1992: «Die Zeit drängt für dieses Datenschutzgesetz. Wir brauchen dieses Datenschutzgesetz unbedingt auch im internationalen Bereich […]. Schliesslich muss ich Ihnen sagen: Es wäre schön, wenn wir einmal ein Gesetz ohne Referendum erlassen könnten»; vgl. Koller, AB 88.032, 10. März 1992, 393.

te sowie die Betroffenenrechte. Aber auch die prozeduralen Instrumente, namentlich die Kompetenzen des EDÖB, wurden für den privaten Bereich zurückgebunden, eine Verbandklage verworfen. Ebendiese Konzessionen im privaten Bereich erfolgten unter dem Druck effizient eingebrachter *Wirtschaftsinteressen*. Im Ergebnis wurde ein *duales Datenschutzgesetz* verabschiedet, wobei die Vorgaben für den privaten Bereich an erster Stelle durch den Einfluss ökonomischer Interessenvertreter geschwächt wurden.[436]

282 Im Rahmen der Totalrevision liess sich eine ähnliche Dynamik verzeichnen: Bereits bei den Vorarbeiten wurde, wiederum von Wirtschaftsvertretern, angeführt, dass das aktuell geltende Instrumentarium genüge, um die Rechte und Pflichten der betroffenen Personen zu gewährleisten. Allerdings befinden sie sich mit dieser Ansicht heute in der Minderheit.[437] An der Differenzierung zwischen dem privaten und dem öffentlichen Bereich wurde im Zuge der Totalrevision festgehalten; indes werden mehrere neue Instrumente für beide Bereiche gleichermassen vorgesehen. Auch hinsichtlich einer Totalrevision stand die Schweiz infolge der internationalen, namentlich der europarechtlichen Entwicklungen, unter Zugzwang. Von der Basisstruktur und damit namentlich von den im Rahmen der Erarbeitung des ersten Datenschutzgesetzes getroffenen Anknüpfungspunkten wurde in der Totalrevision nicht abgegangen. Obschon die Totalrevision auch von den Entwicklungen im Europäischen Recht und hierbei insb. der DSGVO angestossen wurde, stand die Übernahme des in der DSGVO implementierten *Monismus*, der die datenschutzrechtlichen Vorgaben für behördliche wie private Verantwortliche identisch formuliert, nicht zur Debatte. Vielmehr wird am dualistischen System festgehalten, das sich durch verschiedene Elemente konstituiert.

283 Was die Darstellung des politischen Ringens um die Verabschiedung des ersten Datenschutzgesetzes sichtbar werden liess und was mit der Titulierung des DSG als Einheitsgesetz[438] in keiner Weise ausgedrückt wird, ist die *Relevanz und Brisanz, welche der Frage nach einer bereichsspezifischen Differenzierung* (oder des Verzichtes auf diese) für die Datenschutzgesetzgebung zukam – und zukommt.

284 An erster Stelle steht die Vor- und Grundsatzfrage, ob es das dualistische oder das monistische Regime ist, das datenschutzrechtlichen Anliegen effizienter zum Durchbruch zu verhelfen vermag. Offensichtlich stellen sich für ein monistisches Regelungsregime gegenüber einem dualen Regime, das für die beiden Bereiche unterschiedliche Normen vorsieht, unterschiedliche Rechtsfragen. So präsentieren sich Fragen der Anwendbarkeit sowie der Koordination und Auslegung der für die beiden Bereiche nuancierten Normen. Zudem ist die Abgrenzung der bei-

436 Jaggi, AB 88.032, 13. März 1990, 131; vgl. zur Regelung des Datenschutzes für den öffentlichen und nicht-öffentlichen Bereich auch Epiney/Hofstötter/Meier/Theuerkauf, 19 f.
437 EJPD, Bericht Begleitgruppe, 6 f.
438 Dazu exemplarisch M. w. H. Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 6.

den Bereiche mit Blick auf Zugriffsbegehrlichkeiten des Sektors, der strengeren Vorgaben unterworfen wird, eine Herausforderung.

285 Dass die Bestimmung des einschlägigen Rechts schwierig sein kann, zeigte sich unlängst im Entscheid des Bundesverwaltungsgerichts A-3548/2018 i. S. Helsana+ vom 19. März 2019. Datenschutzrechtlich war das von der Zusatzversicherungs-AG betriebene, appbasierte Programm Helsana+ zu beurteilen. Nach diesem Programm sollten Nutzende über die App für bestimmte Aktivitäten, z. B. Sport, Pluspunkte sammeln können, wobei der Nachweis per Foto-Upload erfolgte. Später sollten die Pluspunkte in Barauszahlungen, Sachleistungen, Gutscheine von Partnerbetrieben umgewandelt werden können. Nutzungs- und Bonusberechtigt sollten Versicherungsnehmer einer Versicherungsgesellschaft der Helsana AG sein. Um die Teilnahmeberechtigung (i. e. die Eigenschaft, Versicherungsnehmerin resp. Versicherungsnehmer bei einer Helsana-Gesellschaft zu sein) sowie die Berechnung der Boni zu klären, holte die Helsana Zusatzversicherungs-AG bei den Antragstellenden die Einwilligung zu Personendatenverarbeitungsprozessen ein, um «Daten von der obligatorischen Krankenversicherung der Helsana-Gruppe zur Zusatzversicherung zu übertragen». Das Bundesverwaltungsgericht prüfte vorab, ob die Beklagte als Bundesorgan zu qualifizieren sei, da ein Zugriff auf Daten aus der obligatorischen Krankenpflegeversicherung im Rahmen des Registrierungsprozesses erfolge. Krankenkassen und private Versicherungsunternehmen, die dem BGG betreffend Aufsicht über Versicherungsunternehmen unterständen, gälten dann als Bundesorgane, wenn sie über eine Bewilligung zur Durchführung der sozialen Krankenversicherung nach Art. 4 VAG verfügen würden. Die Beklagte biete indes, so das Bundesverwaltungsgericht, unbestritten keine obligatorischen Krankenversicherungen an. Keine der Datenbearbeitungen, welche die Beklagte im Rahmen des Programms Helsana+ durchführe, beruhe auf solchen Personenangaben, die durch das Krankenversicherungsgesetz geregelt werden. Das Rechtsverhältnis zwischen den betroffenen Personen und der Beklagten sei entsprechend nicht öffentlicher Natur, die Beklagte handle nicht als Bundesorgan, womit es zur Anwendung der Bestimmungen des DSG für den privaten Bereich komme, Art. 12 ff. DSG.[439]

286 Weil die Schweiz, wie zu zeigen sein wird, einen pointierten Dualismus vorsieht, hat die Bestimmung des anwendbaren Rechts – des Normenkomplexes für den öffentlichen Bereich des Bundes resp. des Normenkomplexes für den privatrechtlichen Bereich – weitreichende Konsequenzen.

439 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 4.5.5.; zum Urteil s. auch Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; Vasella/Ziegler, digma 2019, 80 ff.; Pärli, SZS 2018, 107 ff. kritisch zur verordneten Selbstbestimmung; nach Totalrevision Art. 30 ff. nDSG.

3. Strukturierung des Dualismus

Nunmehr soll das dualistische Regime des DSG präziser erfasst werden. Von diesem wird auch mit der Totalrevision des DSG nicht abgegangen werden, ungeachtet der Tatsache, dass die DSGVO zu einem monistischen Modell übergegangen ist. 287

3.1. Gesetzessystematik – Überblick

Die duale Architektur des DSG wird nicht nur anhand des Schutzzweckartikels von Art. 1 DSG (das Gesetz soll die Grundrechte und die Persönlichkeit der Betroffenen schützen, vgl. Art. 1 nDSG) sowie des Anwendungsbereichs von Art. 2 DSG (Art. 2 nDSG), sondern auch anhand der Systematik des geltenden DSG deutlich. An den Anfang werden zwei Abschnitte gestellt, die für beide Bereiche gelten: Der 1. Abschnitt definiert *Zweck* sowie *Begrifflichkeiten* sowohl für den privaten als auch für den öffentlichen Bereich. Der 2. Abschnitt statuiert *allgemeine Datenbearbeitungsgrundsätze für beide Sektoren*. Anders noch hatte die Expertenkommission allgemeine Bestimmungen *je* für den privaten wie für den öffentlich-rechtlichen Datenschutz vorgesehen, was als die bessere, weil präzisere, Lösung galt.[440] Im Anschluss an den gewissermassen vor die Klammer gezogenen gemeinsamen Regelungskomplex des ersten und zweiten Abschnitts, der vereinzelte differenzierende Einzelnormen wie Art. 11a DSG beinhaltet, wird eine konsequente Zweiteilung vorgenommen: Im 3. Abschnitt folgt ein Korpus an Normen, der die Datenbearbeitung durch Private regelt. Der 4. Abschnitt sieht spezielle Regeln für die Datenbearbeitung durch öffentliche Stellen des Bundes vor. Die folgenden Abschnitte 5 ff. mit ihren Durchsetzungs- und Übergangsbestimmungen gelten dem Grundsatz nach für *beide Bereiche*. Sie enthalten gleichwohl bedeutsame Differenzierungen für den öffentlichen und den privaten Sektor. Exemplarisch ist der 5. Abschnitt, der den EDÖB für beide Bereiche als zuständige Behörde installiert. Allerdings kommen diesem unterschiedliche Kompetenzen für den jeweiligen Bereich zu. 288

Mit der *Totalrevision* finden sich die spezifischen Bestimmungen für den privaten resp. öffentlichen Bereich im 5. und 6. Kapitel. Unter dem Titel «Allgemeine Bestimmungen» steht das 2. Kapitel, dessen 1. Abschnitt sich den Begriffen und Grundsätzen, dessen 2. Abschnitt sich der Bekanntgabe von Personendaten ins Ausland, dessen 3. Abschnitt sich dem sog. postmortalen Datenschutz widmet. Dieser kennt in der DSGVO kein entsprechendes Pendant. Das 3. Kapitel regelt das Verhältnis von Verantwortlichem und Auftragsverarbeiter, das 4. Kapitel normiert die Betroffenenrechte, woraufhin das 5. und das 6. Kapitel mit den spe- 289

440 Pedrazzini, Grundlagen, 19 und 24.

zifischen Regeln für die Bearbeitung durch Private und Bundesbehörden folgen. Das 7. Kapitel befasst sich mit dem EDÖB.

290 Indem in den ersten vier Kapiteln Bestimmungen für beide Bereiche vorgesehen werden, wird der Normbestand, der für den öffentlichen wie den privaten Sektor gilt, ausgebaut. Das kommt durchaus einer Annäherung der beiden Systeme gleich. Immerhin: Es handelt sich um eine Angleichung, die in erster Linie *nicht* in der Überwindung der tradierten strukturellen und *materiellrechtlichen Differenzierung* besteht – namentlich nicht in Bezug auf den Ausgangs- sowie Anknüpfungspunkt. Im DSG gilt vor und nach Totalrevision das folgende Konzept: prinzipielles Verarbeitungsverbot und Legalitätsprinzip mit rechtlich definierten Erlaubnistatbeständen im öffentlichen Bereich, prinzipielle Verarbeitungsfreiheit mit Schranken im privaten Bereich.[441]

291 Die «Vereinheitlichung» wird mit der Totalrevision in erster Linie durch die Schaffung eines breiteren gemeinsamen Fundamentes von *prozeduralen und organisatorischen Datenschutzinstrumenten* vollzogen, die auf die faktische Verwirklichung und Implementierung des Datenschutzes abzielen (so namentlich das Verarbeitungsverzeichnis, das sowohl von privaten als auch von öffentlichen Verantwortlichen erstellt werden soll, vgl. Art. 12 nDSG). Die Totalrevision baut den Korpus an Vorgaben, die für beide Bereiche gelten, namentlich in diesem Aspekt aus.

292 Wie aber lässt sich die gesetzliche Differenzierung für den privaten und öffentlichen Bereich im geltenden DSG (und damit vor Totalrevision) strukturieren? Viele Umschreibungen finden sich, um das «zweigeteilte Einheitsgesetz» genauer zu charakterisieren, seine beiden Gesichter markanter und konkreter zu bezeichnen. Im Rahmen der Darstellung des historisch-politischen Prozesses fiel exemplarisch und trefflich eine Beschreibung des privaten Sektors als Missbrauchsgesetzgebung.[442] Später kursierten zusehends Charakterisierungen, die das Regime für den privaten Bereich als eines der *informationellen Selbstbestimmung* qualifizieren.[443] Zwar wurde seit 1993 erst die Bundesverfassung totalrevidiert, was auch

441 Hierzu bereits Forstmoser, digma 2003, 50 ff., 53; zum Legalitätsprinzip im Allgemeinen, aber auch spezifisch in Bezug auf die Verarbeitung von Personendaten Glass, 5 ff. und 91 ff.

442 Danioth, AB 88.302, 5. Dezember 1991, 1018; Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), 19 ff., 34 ff.

443 Ob das DSG ein Recht auf informationelle Selbstbestimmung insb. auch für den privaten Bereich verbürgt resp. was die Elemente eines solchen Rechts sind, wird im Zuge dieser Arbeit vertieft analysiert; vgl. insb. zweiter Teil, VI. Kapitel sowie dritter Teil; die Auffassung, wonach das DSG ein Recht auf informationelle Selbstbestimmung verbürge, vertritt mit einem Fokus auf den privaten Bereich z. B. Aebi-Müller, N 267 und m. w. H. N 529; Dies., in: Girsberger/Schmid (Hrsg.), 13 ff., 20; Rosenthal, HK-DSG, Art. 4 N 66; Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 5; Flückiger, PJA 2013, 837 ff.; aufschlussreich auch für die Schweiz die Ausführungen zur informationellen Selbstbestimmung mit der Einwilligungskonstruktion als zentrales Element Cavoukian, digma 2009, 20 ff.; hinterfragend dagegen zur Figur im Schweizer Rechtskorpus m. E. in zutreffender Weise, wenn auch mit einem Fokus auf den Grundrechtsschutz, Belser, in: Epiney/Fasnacht/Blaser (Hrsg.),

die Einführung eines neuen Art. 13 BV mit sich brachte. Zudem wurde das DSG seit seinem Inkrafttreten teilrevidiert.[444] Allerdings haben weder die bislang erfolgten Teilrevisionen noch die derzeit hängige Totalrevision einen Systemwechsel gebracht. Die Bedeutung der bis heute zugleich dezidiert wie nuanciert bereichsspezifischen Normierung, die das DSG für den öffentlichen gegenüber dem privaten Bereich vorsieht, wurde bislang nicht grundlegend thematisiert. Vielmehr wird man anhand zahlreicher Textstellen in eine andere Interpretationsrichtung verwiesen:

> «Das Datenschutzgesetz enthält *als gemeinsames Fundament* jeglicher Datenbearbeitung nebst den wichtigsten Begriffsumschreibungen die eigentlichen materiellen Grundsätze, ich möchte sie Spielregeln jeder Datenbearbeitung nennen […].»[445] [Hervorhebung durch die Autorin]

Die gemeinsamen Bestimmungen mit ihren generalklauselartigen, sehr allgemeinen Grundsätzen für die private wie die öffentliche Datenbearbeitung[446] wurden ebenso als das «ethische und rechtspolitische Fundament des Datenschutzgesetzes[447]» beschrieben. Allerdings verleitet die Referenz auf ein gemeinsames Fundament zu einer Fehlinterpretation in Bezug auf das Schutzniveau des Datenschutzgesetzes für den privaten gegenüber dem öffentlichen Bereich. Sie lässt die Assoziation mit einem *gemeinsamen und identischen Ausgangspunkt* entstehen. Doch das prägende Charakteristikum des DSG ist, wie bisher ansatzweise dargetan, dessen *Dualismus* mit *entgegengesetzten Ausgangspunkten* für den privaten und öffentlichen Bereich. Ebendies hat vorab bereits Rhinow mit folgenden Worten festgehalten: 293

> «Das Gesetz […] regelt zu Recht sowohl die Datenbearbeitung durch den Bund als auch durch private Personen. Trifft aber – ebenfalls zu Recht – unterschiedliche, differenzierte Normierungen, indem es bei den Bundesorganen das Legalitätsprinzip in den Vordergrund rückt, während es im privatrechtlichen Verhältnis die Mechanik des Persönlichkeitsschutzes von Art. 28 ZGB übernimmt.»[448]

---

19 ff.; auf Missverständlichkeiten hinweisend Meier, N 15 ff.; kritisch sodann Gächter/Egli, Jusletter vom 6. September 2010, N 19 ff.; Glass, 151 ff.; zutreffend mit dem Hinweis, dass ein Konzept der informationellen Selbstbestimmung bislang nicht ins Gesetz eingegangen ist, Ziegler/Vasella, digma 2019, 158.

444 Vgl. zur Teilrevision Wermelinger/Schweri, Jusletter vom 3. März 2008; zur Kritik an einer ersten Revision, wonach diese die Wirtschaft in ein zu enges Korsett schnüren würde, wobei die Autoren vertreten, dass ein starker Datenschutz auch der Wirtschaft diene, Baeriswyl/Rudin, Jusletter vom 28. Juni 2004; kritisch zur Revision, wie sie 2008 in Kraft trat, Brunner, in: Schaffhauser/Horschik (Hrsg.), 142 ff. und Ders., Jusletter vom 4. April 2011; Cottier, Jusletter vom 17. Dezember 2007, der die wichtigsten Neuerungen wie die Schärfung der Transparenzvorgaben darstellt und dafür plädiert, die Neuerungen nicht zu unterschätzen; Drechsler, AJP 2007, 1471 ff.; zur Teilrevision weiter Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 156 ff.

445 So Danioth, AB 88.032, 13. März 1990, 127.

446 Zu einer Darstellung der Grundsätze auch Schmid, ZBJV 1995, 809 ff., 820; Peter, 125 ff.

447 BBl 1988 II 414 ff., 459.

448 Rhinow, AB 88.032, 13. März 1990, 130.

294 Ebenso prägnant Forstmoser:

> «Im Rahmen des Privatrechts gilt: erlaubt ist, was nicht verboten ist, das ist der Ausgangspunkt im privaten Bereich, während im öffentlichen Recht gilt: Verboten ist, was nicht erlaubt ist […].»[449]

295 Diese akkurate Qualifizierung wurde in der späteren Rezeption und Interpretation des DSG allzu oft übersehen. Nachfolgend werden die Elemente vertieft, die zur Beschreibung des DSG als *duales Gesetz* Anlass geben.[450] Am Anfang steht der richtungsweisende Entscheid für *entgegengesetzte Ausgangspunkte für den privaten und den öffentlichen Bereich*. Darin allerdings erschöpft sich die *bereichsspezifisch differenzierende Regelung* nicht. Vielmehr setzt das DSG besagte Grundsatzentscheidung mit «gegenüberliegendem Startpunkt» durch weitere Gestaltungselemente konsequent fort.

3.2. Entgegengesetzte Ausgangspunkte für die beiden Bereiche

3.2.1. Darstellung

296 In der Schweiz zeigt sich folglich die datenschutzgesetzliche Situation dergestalt, dass die quasi als allgemeiner Teil vorangestellten Prinzipien in ein *ganz unterschiedliches, ja gegenläufiges Konzept* für den privaten und den öffentlichen Sektor eingebettet sind. Für den privaten und den öffentlichen Sektor gelten entgegengesetzte Ausgangspunkte: grundsätzliches Verarbeitungsverbot mit Erlaubnisvorbehalten qua gesetzlicher Grundlagen für den öffentlichen Sektor, grundsätzliche Verarbeitungsfreiheit mit Schranken für den privaten Sektor. Es ist Art. 1 DSG, der Zweckartikel, der bei einer streng der privatrechtlichen und öffentlichrechtlichen Terminologie wie Dogmatik verpflichteten Lesart die verschiedenen Mechaniken resp. unterschiedlichen Regelungskonzepte über das Schutzobjekt in das DSG einführt.

297 Entsprechend drängt es sich für den *öffentlichen Bereich* auf, an die Theorie der Grundrechte und ihrer Beschränkungen anzuknüpfen, womit auch das *Legalitätsprinzip* für das Datenschutzrecht installiert wird, vgl. Art. 17 DSG und Art. 34 nDSG. Für den öffentlichen Bereich des Bundes gilt das grundsätzliche Verarbeitungsverbot, jeder Umgang mit Personendaten – das Erheben, Speichern, Auswerten usf. – braucht eine spezifische Legitimation, wobei eine gesetzliche

449 Forstmoser, digma 2003, 50 ff., 53, spricht davon, dass das Gesetz nicht verleugnen könne, ein Fusionsprodukt zu sein, dessen Anwendungsbereich von verschiedener Tiefe sei; die Botschaft spricht von einer «eingehenden Regelung» für den öffentlich-rechtlichen Bereich des Bundes, vgl. BBl 1988 II 414 ff., 414.

450 Zu dieser Terminologie Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.8.; als föderalistische Ordnung umschrieben von Schweizer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 1 N 13.

Grundlage den wichtigsten der Erlaubnistatbestände liefert. Entsprechend ist aus der Perspektive des Datenschutzes der Verarbeitungsraum im öffentlichen Bereich kein freiheitlicher. Vielmehr bedarf *jede* Personendatenbearbeitung durch *Bundesbehörden*, um rechtmässig zu sein, *einer spezifischen rechtlichen Grundlage ausserhalb des DSG*. Das DSG selbst liefert eine solche allgemeine Rechtsgrundlage für die Datenbearbeitung durch Bundesbehörden gerade nicht.[451] Der Inhalt datenschutzrechtlicher Regulierungen lässt sich folglich für den öffentlichen Sektor auf Bundesebene nie isoliert anhand des DSG erschliessen. Zu beachten ist vielmehr eine ganze Reihe bereichsspezifischer Erlasse, die sich vorrangig spezifischen hoheitlichen Aufgaben des Bundes in der Verwaltung (vgl. z. B. AsylG, ANAG, BGÖ, IVG, UVG usf.) sowie der Strafverfolgung und Verbrechensbekämpfung widmen und in diesem Kontext Personendatenverarbeitungen normieren.[452] Sodann datenschutzrechtlich von besonderer Relevanz und Brisanz ist der steuerrechtliche Bereich, wobei das Bundesgesetz über die direkte Bundessteuer datenschutzrechtliche Regeln vorsieht, vgl. Art. 112a DBG.[453]

Die genannten *bereichsspezifischen Spezialgesetze* weisen entsprechend eine doppelte Funktion auf: Sie bilden zunächst die Legitimationsgrundlage zur Durchbrechung des nach DSG implementierten Grundsatzes des Verarbeitungsverbotes und erfüllen damit das verfassungsrechtliche Legalitätsprinzip für den öffentlichen Bereich, vgl. Art. 17 DSG und Art. 36 Abs. 1 sowie Art. 5 Abs. 1 BV. Sodann finden sich in den Spezialgesetzgebungen differenzierende, ergänzende und derogierende Datenschutzbestimmungen. Hieraus wird deutlich, dass der *öffentliche Bereich* aus datenschutzrechtlicher Perspektive *kein einheitlicher, monolithischer ist*. Vielmehr handelt es sich um einen facettenreichen Bereich, dessen Teilbereich jeweils unterschiedliche Ziele verfolgen. Über die jeweiligen Spezialgesetze werden jeweils verschiedene Verarbeitungszusammenhänge in die datenschutzrechtlichen Erwägungen integriert. Folglich kann bereits an dieser Stelle festgestellt werden, dass sich die Relevanz systemspezifischer Erwägungen selbst in einem Regime mit datenschutzrechtlichem Querschnittsgesetz keineswegs auf eine Zweiteilung in einen öffentlichen und privaten Bereich beschränkt. Vielmehr 298

451 Der Mechanismus ist ähnlich zu demjenigen von Art. 3 ZGB für das Privatrecht: Die Bestimmung selbst sieht keinen allgemeinen Gutglaubensschutz vor; vielmehr muss dieser in jeweiligen spezifischen Gesetzesnormen wie z. B. Art. 930 ZGB speziell verbürgt werden. Art. 3 ZGB knüpft an solche Sondernormen an («Wo das Gesetz […]») und formuliert allgemeine Modalitäten namentlich aus der Beweisperspektive.

452 Illustrativ mit Bezug auf den Datenschutz bei intelligenten Mess- und Steuersystemen und Netzbetreibern die Beschreibung des anwendbaren Rechts als dreistufiger Rechtsrahmen von DSG, kantonalem Datenschutzrecht und Spezialgesetzgebung wie das Stromversorgungsgesetz vgl. Rechsteiner/Steiner, Jusletter vom 11. Juni 2018, N 8 ff.

453 Für eine Übersicht: Seethaler, BSK-DSG, Entstehungsgeschichte DSG, N 62 ff., insb. N 65 ff.; weitere einschlägige Spezialgesetze finden sich beispielsweise für den biomedizinischen Kontext, dessen Erlasse ebenso datenschutzrechtliche Bestimmungen aufweisen: Zu nennen ist namentlich das Humanforschungsgesetz, Art. 2 Abs. 2 lit. c *e contrario*, Art. 3 lit. f. und Art. 32 f. HFG (vgl. auch Art. 119 BV) sowie das GUMG.

wird der öffentliche Bereich aufgrund *pluraler Verarbeitungszusammenhänge weiter ausdifferenziert*.

299 Damit präsentiert sich auch die Bezeichnung des Datenschutzgesetzes als Querschnittsgesetz in einem anderen Licht: Personendatenverarbeitungen durch Bundesbehörden werden über das Gebot der gesetzlichen Grundlage bereichsspezifisch rückgekoppelt. Man könnte hierfür den *Terminus der Akzessorietät des Datenschutzes* für die jeweiligen Bereiche und Verarbeitungskontexte verwenden. Insofern zeigt sich das Datenschutzrecht gerade nicht als unabhängiges Rechtsgebiet, wie man aus der isolierten Betrachtung des Datenschutzgesetzes als Querschnittsgesetz zu schliessen geneigt ist. Vielmehr weist es *systemrelative Bezüge* auf.

300 Für den öffentlichen Sektor liefert unbestrittenermassen die *gesetzliche Spezialermächtigung* den wichtigsten Erlaubnistatbestand zur Durchbrechung des grundsätzlichen Verarbeitungsverbotes.[454] Zwar sieht das DSG die Einwilligung als Erlaubnistatbestand namentlich in den Art. 17 Abs. 2 lit. c sowie Art. 19 Abs. 1 lit. b DSG vor (vgl. Art. 34 Abs. 4 lit. b, Art. 36 Abs. 2 lit. c nDSG). Dennoch kann der Einwilligung – systemkongruent – im Bereich der Datenverarbeitung durch öffentliche Stellen nur eine zurückhaltende Rolle zukommen: Die Verletzung des Legalitätsprinzips als Verarbeitungsprinzip soll nur beschränkt möglich sein.[455] Die datenschutzrechtliche Einwilligung kann ihr «Hauptanwendungsfeld» folglich nicht im öffentlichen Sektor finden, stattdessen ist sie, zumindest theoretisch betrachtet, im privaten Bereich zu verorten.[456] Entsprechend setzt das schweizerische Datenschutzgesetz für die Datenverarbeitung im öffentlichen Sektor durch Bundesorgane zumindest formell durch den Grundsatz des Verarbeitungsverbotes mit Erlaubnistatbestand und der bloss restriktiven Zulassung eines Rechtfertigungsgrundes auch bei Missachtung des Legalitätsprinzips – zumindest theoretisch oder ideal gedacht – ein *hohes Datenschutzniveau* fest. Dass diese Idee allerdings teilweise naiv bleibt, wird sich im Zuge dieser Schrift zeigen: Denn auch gesetzliche Grundlagen und Rechtssätze, die ihrerseits als Legitimation zur Bearbeitung von Personendaten dienen sollen, sollten durchaus kritisch betrachtet werden. Ebendies wird vertiefend im letzten Teil und letzten Kapitel

454 Zum Legalitätsprinzip mit seinem allgemeinen rechtsstaatlichen Rahmen sowie spezifisch im Kontext des Datenschutzrechts vgl. insb. Glass, 5 ff., auch mit Hinweis auf die Neuerungen im Zusammenhang mit den Kategorien von «Gesetz im formellen und materiellen Sinne».

455 Rosenthal, HK-DSG, Art. 4 N 4.

456 Fasnacht, N 191 ff. und N 215 ff.; Rogosch, 34; grundlegend zur datenschutzrechtlichen Einwilligung, allerdings teilweise ohne Vertiefung der Frage der Differenzierung für die beiden Bereiche Radlanski, *passim*; Liedke, *passim;* Schunke, *passim* sowie die Beiträge von Rosenthal, Vasella und Bühlmann.

dieser Schrift ausgearbeitet werden anhand der geheimen Observation im Versicherungskontext.[457]

Zur gesetzlichen Grundlage wurde in der Botschaft von 1988 vertreten, dass keine rechtliche Spezialermächtigung, die sich spezifisch auf die Datenbearbeitung beziehen müsse, erforderlich sei. Vielmehr sei die Bearbeitung von Daten zulässig, wenn sie für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist.[458] Eine solche Interpretation, die nicht zu überzeugen vermag, führt zu einer einschneidenden *Absenkung* des Datenschutzniveaus für den öffentlichen Bereich. Sieht das DSG als Ausgangspunkt für die Datenverarbeitung durch Bundesbehörden den *Grundsatz des Verarbeitungsverbotes mit Ausnahmetatbeständen* vor,[459] so deckt es sich insofern – in diesem Bereich – mit dem Regime der DSGVO, vgl. Art. 6 DSGVO. Allerdings gelten die Anforderungen an die Klarheit, Spezifizierung und Präzision ebenda als hoch.[460] 301

Wie aber präsentieren sich der im DSG implementierte Ansatz und das Schutzniveau für den *privaten Bereich*? Die im Rahmen der Gesetzgebungsarbeiten zur erstmaligen Verabschiedung des DSG gemachte Aussage, wonach das Datenschutzgesetz für den privatrechtlichen Sektor den Schutz der Persönlichkeit gemäss Art. 28 ZGB spezialgesetzlich gewährleisten solle, bedarf der Präzisierung. Die Worte in der Botschaft von 1988 zum Datenschutzgesetz von 1992 geben das später gesetzlich verabschiedete Regime prägnant wieder: 302

> «Gleichsam als Spiegelbild zum zivilrechtlichen Persönlichkeitsschutz besteht auch ein gewisser verfassungsrechtlicher Schutz gegen unzulässige und übermässige Datenbearbeitung.»[461]

Anders als im öffentlichen Bereich ist nicht jede Personendatenverarbeitung grundsätzlich verboten. Vielmehr implementiert Art. 12 ff. insb. i. V. m. Art. 4 DSG resp. Art. 30 ff. i. V. m. Art. 6 nDSG ein *System mit grundsätzlicher Freiheit der Datenbearbeitung, deren Schranken sich auf ein Prinzip der «Fairness»* beziehen.[462] Insofern aufschlussreich ist nochmals eine Passage aus der Botschaft von 1988, wonach die *Lauterkeit in der privaten Wirtschaftstätigkeit* auch im Umgang mit Personendaten gelte.[463] Die «Lauterkeit» wird in erster Linie durch die 303

457 Dritter Teil, IX. Kapitel; eindrücklich zur Problematik im Zusammenhang mit der verordneten Zwangsmedikation Bucher, ZBJV 2001, 764 ff.; seit jeher wird denn auch in der Schweiz die auf Bundesebene fehlende Überprüfung von Bundesgesetzen auf ihre Verfassungsmässigkeit hin diskutiert.

458 Vgl. auch BBl 1988 II 414 ff., 467; Ballenegger, BSK-DSG, Art. 17 N 18.

459 Vgl. Ballenegger, BSK-DSG, Art. 17 N 3.

460 Insb. bedarf es der spezifischen Zweckbestimmung mit Blick auf die Personendatenverarbeitung und die Gewährleistung der Vorhersehbarkeit der Verarbeitung, vgl. Buchner/Petri, Beck-Komm.-DSGVO, Art. 6 N 91.

461 BBl 1988 II 414 ff., 414; zum verfassungsmässigen Schutz und verfassungsmässigen Recht auf Privatsphäre im Zeitraum der Verabschiedung des ersten DSG Schrepfer, 19 ff.

462 Vertiefend hierzu zweiter Teil, VI. Kapitel, B.

463 BBl 1988 II 414 ff., 425.

allgemeinen Verarbeitungsgrundsätze gem. Art. 4 DSG resp. Art. 6 nDSG definiert. Erst der *qualifizierte Umgang mit Personendaten* – allem voran der Verstoss gegen die allgemeinen Verarbeitungsgrundsätze – begründet zugleich eine Persönlichkeitsverletzung, vgl. Art. 12 DSG resp. Art. 30 nDSG.[464]

304 Nach DSG liegen die *Schranken der grundsätzlichen Freiheit der Bearbeitung* vorab in den *allgemeinen Bearbeitungsgrundsätzen*, der Gewährleistung der Vorgaben an die *Datenrichtigkeit* sowie der Einhaltung der Datensicherheitsvorgaben, Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG.[465] Ein Verstoss gegen diese durch die Fixierung von Grundprinzipien gesetzten Schranken begründet eine Persönlichkeitsverletzung, die prinzipiell auch widerrechtlich ist, es sei denn, es liegt ein Rechtfertigungsgrund vor nach Art. 13 DSG resp. Art. 31 nDSG.[466]

305 Eine weitere Schranke der prinzipiellen Verarbeitungsfreiheit liegt in einer Widerspruchskonstellation: Die Verarbeitung von Personendaten entgegen dem ausdrücklichen Willen wird als qualifizierte Handlung taxiert, die – mangels Rechtfertigungsgrund – eine widerrechtliche Persönlichkeitsverletzung begründet, vgl. Art. 12 Abs. 2 lit. b i. V. m. Art. 13 DSG resp. Art. 30 Abs. 2 lit. b nDSG. In konsequenter Anlehnung des DSG für den privaten Bereich an Art. 28 ff. ZGB kann auch eine Verarbeitung gegen den ausdrücklichen Willen der Betroffenen zulässig sein, sofern hierfür ein Rechtfertigungsgrund angeführt werden kann gemäss Art. 13 DSG resp. Art. 31 nDSG.

306 Weiter begründet die *Bekanntgabe von besonders schützenswerten Daten oder von Persönlichkeitsprofilen an Dritte* eine widerrechtliche Persönlichkeitsverletzung, vgl. Art. 12 Abs. 2 lit. c i. V. m. Art. 3 lit. c, lit. d, lit. f. DSG. Auch hier besteht die Rechtfertigungsmöglichkeit gemäss Art. 13 DSG. Mit der Totalrevision wird das Konzept des Persönlichkeitsprofils aufgegeben. Neu geregelt werden stattdessen das Profiling sowie die automatisierte Einzelfallentscheidung, vgl. Art. 5 lit. f und lit. g nDSG und Art. 6 Abs. 7 nDSG und z. B. Art. 21, Art. 25 Abs. 2 lit. f. nDSG. Als Tatbestand der Persönlichkeitsverletzung gilt gemäss Art. 30 Abs. 2 lit. c nDSG einzig die Bekanntgabe besonders schützenswerter Personendaten an Dritte, vgl. zur Konkretisierung Art. 5 lit. c und lit. e nDSG. Eine Rechtfertigung ist nach Art. 31 nDSG möglich.

464 Vertiefend hierzu zweiter Teil, VI. Kapitel, A. und B.

465 Während der Grundsatz der Datenrichtigkeit noch in Art. 5 DSG eigenständig geregelt ist, wird er mit der Totalrevision in die allgemeinen Grundsätze gemäss Art. 6 nDSG, genauer in dessen Abs. 5 integriert. Separat finden sich in beiden Versionen die Vorgaben zur Datensicherheit, Art. 7 DSG resp. Art. 8 nDSG.

466 Zur Kontroverse mit Blick auf die unterschiedlichen Formulierungen betreffend die Rechtfertigungsgründe in den verschiedenen literae Rosenthal, HK-DSG, Art. 12 N 15 ff.; Auslegungshilfe des BJ vom 10. Oktober 2006, Ziff. 3.1.

Der Abriss hat gezeigt, wie eng das datenschutzgesetzliche System für den privaten Bereich an der Struktur von Art. 28 ZGB angelehnt ist. Es sind stets erst *qualifizierte Handlungen*, die als (persönlichkeits-)rechtlich relevant eingestuft werden.[467] Gleichzeitig wird damit ein *individualrechtlich sowie defensivrechtlich* gedachtes Regime im DSG implementiert. Die Totalrevision bringt, wie angedeutet und an späterer Stelle zu vertiefen, immerhin neue Akzente mit der Einführung eines Risiko- und Compliance-Ansatzes, die indes die persönlichkeitsrechtliche Anknüpfung nicht ersetzen, sondern ergänzen. 307

Damit ist erstellt, dass eine Behauptung, wonach das *DSG im privaten Bereich den Betroffenen ein Recht auf informationelle Selbstbestimmung in der Gestalt eines Herrschaftsrechts* einräume, aufgrund des gewählten Ausgangspunktes der grundsätzlichen Bearbeitungsfreiheit mit Schranken für den privaten Bereich im DSG *offensichtlich keine Grundlage* findet.[468] Das für den privaten Bereich gewählte Konzept, das an qualifizierte Verarbeitungshandlungen ansetzt, räumt dem Individuum kein «Herrschaftsrecht resp. Selbstbestimmungsrecht» an seinen Personendaten ein – auch nicht mit der Totalrevision.[469] Trefflicher dagegen ist die Charakterisierung des DSG für den privaten Bereich – namentlich vor der Totalrevision – als *Missbrauchsgesetzgebung*.[470] Diese Konzeptionierung wird anhand der Gestaltung des Massnahmenkatalogs, wie er dem EDÖB eingeräumt wird und wie gezeigt werden wird, bestätigt. Immerhin stärkt die Totalrevision seine Kompetenzen auch für den privaten Bereich. 308

Eine Folge der *persönlichkeitsrechtlichen Anknüpfung des Datenschutzgesetzes für den privaten Bereich* ist weiter, dass die Rechtsdurchsetzung resp. der Rechtsschutz – zumindest nach noch in Kraft stehendem DSG – weitgehend auf die Schultern der Datensubjekte gelegt wird.[471] Es obliegt in erster Linie den Datensubjekten, die Einhaltung des Datenschutzes sicherzustellen, sei es durch Ausübung der Betroffenenrechte, sei es weiter durch die Erhebung einer zivilgerichtlichen Klage gegen qualifizierte Personendatenverarbeitungen, was allerdings kaum je geschieht.[472] Die Totalrevision bringt insofern nicht nur über die 309

467 M. w. H. Haas, N 63 ff., N 70 ff. und N 80 ff.; vgl. unter Rückgriff auf das allgemeine Zivilrecht und damit das Persönlichkeitsrecht des ZGB in Bezug auf die Presseberichterstattung Lüthy, 59 ff.

468 Die Gewährleistung eines entsprechenden Rechts im DSG vertritt insb. Aebi-Müller, N 546 ff. und N 591 ff.; kritisch insofern zutreffend Gächter/Egli, Jusletter vom 6. September 2010, N 36; Belser, in: Epiney/Fasnacht/Blaser, 19 ff., 32 ff.; vgl. insofern die Botschaft von 1988, wo potentielle Risiken für den Menschen angedeutet werden, und: «er hat die Herrschaft über die Daten, die ihn angehen, weitgehend verloren»; BBl 1988 II 414 ff., 417.

469 Vertiefend hierzu zweiter Teil, V. Kapitel und VI. Kapitel.

470 Anders Aebi-Müller, N 546 ff. und N 591 ff.; zur Qualifikation auch Gächter/Egli, Jusletter vom 6. September 2010, N 36; Belser, in: Epiney/Fasnacht/Blaser, 19 ff., 32 ff.

471 Art. 12 ff. DSG und Art. 30 ff. nDSG; vertiefend zweiter Teil, VI. Kapitel sowie dritter Teil, VII. Kapitel, A.

472 Bolliger/Féraud/Epiney/Hänni, 4; sinngemäss Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.20 f.; vgl. auch Rudin, digma 2003, 4 f., wonach das Risiko für Unternehmen weniger in behördlichen resp. gerichtlichen Verurteilungen liegt als vielmehr in den Reaktionen der mün-

neuen Instrumente wie das Verarbeitungsverzeichnis oder die Datenschutz-Folgenabschätzung, sondern auch den Ausbau sowie die Verschärfung der rechtlichen Konsequenzen von DSG-Verletzungen eine gewisse Veränderung. Ob damit Datenschutzverstösse künftig effizienter sanktioniert werden wird sich weisen müssen.

310 Das Schweizer DSG definiert den *privaten Bereich* damit als *weitgehend resp. prinzipiell freien Bereich*. Es unterscheidet sich folglich grundlegend von einem Ansatz, wie ihn Art. 6 DSGVO auch für den privaten Bereich wählt: Die DSGVO sieht mit Blick auf den gewählten Ausgangspunkt für Personendatenverarbeitungen durch Behörden und Private keine Differenzierung vor (datenschutzrechtlicher Monismus) – ebenso gilt für den privaten Bereich das Prinzip der Spezialermächtigung, Art. 6 DSGVO.[473]

311 Mit beschriebenem *Dualismus adressiert und anerkennt die Schweiz die Einschlägigkeit*, datenschutzrechtlich *bereichsdifferenzierend zu normieren*. Insofern aufschlussreich ist nochmals die Botschaft, die auf die Bedeutung sowie Chancen der Datenverarbeitungen für Forschung, Wirtschaft und Verwaltung hinweist.[474] Die Ausdifferenzierung wird zudem zum einen im öffentlich-rechtlichen Bereich des Bundes qua Legalitätsprinzip mit der gesetzlichen Spezialregelung weiter ausgebaut. Zum anderen sind im privaten Bereich mehrere Spezialgesetze mit spezifischen Datenschutzbestimmungen zu beachten, so beispielsweise das Humanforschungsgesetz mit Art. 32 f. HFG.[475]

312 Eine *Schlussfolgerung*, wonach das *Datenschutzrecht die Integrität verschiedener Systeme resp. Bereiche* schützen soll, wurde in der Schweiz – soweit ersichtlich – bislang nicht gezogen. Immerhin wurde jüngst spezifisch im Zusammenhang mit dem Bankgeheimnis resp. den beruflichen Geheimhaltungspflichten und Cloud-Services zur Diskussion gestellt, ob der Datenschutz nicht nur Subjekte, sondern auch Systeme schütze.[476] In Frage gestellt wurden die Tauglichkeit eines Rechts

digen Konsumentinnen und Konsumenten; kritisch zur Gleichsetzung von öffentlicher und privater Datenverarbeitung gemäss BDSG und für eine Differenzierung plädierend Giesen, JZ 2007, 918 ff., 923.

473 Vgl. zu dieser Vereinheitlichung qua DSGVO von Lewinski, DuD 2012, 564 ff., 565, wobei der Autor weiter die Unitarisierung des Datenschutzrechts mit Blick auf den räumlichen Anwendungsbereich und die Vereinheitlichung der Datenschutzvorgaben bei Personendatenverarbeitungen mit EU-Bezug erwähnt, 569; entsprechend könnte nunmehr mit Blick auf die DSGVO von einem doppelten Unitarismus gesprochen werden.

474 BBl 1988 II 414 ff., 417; vgl. damit die Parallele zu Deutschland, wonach Datenschutz und Forschung seit Anbeginn der datenschutzrechtlichen Debatten relevant ist, Gerling, DuD 2008, 733 ff., 733.

475 Zu diesem vertiefend zweiter Teil, VI. Kapitel, B. 6.3.

476 Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.

auf informationelle Selbstbestimmung und damit auch der datenschutzrechtliche Subjektschutz.[477]

Ungeachtet der exakten Ausgestaltung des datenschutzrechtlichen Subjektschutzes bleibt festzuhalten: Die Einschlägigkeit systemischer Schutzerwägungen als datenschutzrechtliches Koordinatensystem ist namentlich im Dualismus des DSG für den privaten gegenüber dem öffentlichen Bereich anerkannt. Dem Subjektschutz bleibt das DSG auch nach Totalrevision verpflichtet, Art. 1 DSG resp. Art. 1 nDSG.[478] Mit der Totalrevision erfolgen zwar Anpassungen oder Ergänzungen der Perspektiven. Gleichwohl wird das DSG nicht von einer Fokussierung auf das einzelne Subjekt und den Individualrechtsschutz abgehen. Exemplarisch für die *Einführung neuer, ergänzender Komponenten* die Botschaft zum Entwurf zur Totalrevision des DSG: 313

> «Eine erste Leitlinie der Revision bildet der risikobasierte Ansatz. Der Revisionsentwurf orientiert sich konsequent an den potenziellen Risiken für die betroffenen Personen, denn die Gefahren für die Privatsphäre der betroffenen Personen hängen weitgehend von den Aktivitäten der verschiedenen Verantwortlichen und Auftragsbearbeiter ab.»[479]

3.2.2. Resümee und Einbettung

An dieser Stelle seien die vorangehenden Ausführungen wie folgt *zusammengefasst:* Das eidgenössische Datenschutzgesetz ist entgegen seiner formellen Erscheinung und Titulierung als *Einheitsgesetz* gerade auch aus materiellrechtlicher Sicht als *duales Gesetz* zu qualifizieren.[480] 314

Von zentraler Bedeutung ist der Entscheid für jeweils *entgegengesetzte Ausgangspunkte*. Indem der Grundsatz der Freiheit der Datenbearbeitung mit Schranken für den privaten Sektor versus den Grundsatz des Verbotes der Datenbearbeitung mit Erlaubnisvorbehalt für den öffentlichen Sektor umgesetzt wird, geht das DSG in pointierter Weise von einer *bereichsspezifischen Differenzierung* im Datenschutzgesetz resp. -recht aus.[481] Dieser Dualismus, welcher das datenschutzrechtliche Regime für den privaten und den öffentlichen Bereich des Bundes differenziert, ist ein *primäres Charakteristikum des Schweizer Datenschutzgesetzes*. 315

477 So Passadelis mit den Worten «Am überkommenen Primat der informationellen Selbstbestimmung festzuhalten, bedeutet, noch mehr kostbare Zeit zu verlieren», Gastkommentar, NZZ vom 17. Mai 2017, abrufbar unter: <https://www.nzz.ch/meinung/datenschutzrecht-komplexe-regulierung-ld.1293903?reduced=true> (zuletzt besucht am 30. April 2021).

478 Die Totalrevision hält an der entsprechenden Bestimmung mit Art. 1 nDSG fest.

479 Botschaft DSG 2017–1084, 17.059, 6941 ff., 6970.

480 Vgl. Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.10.

481 Zur weiteren Ausdifferenzierungsmöglichkeit, indem die jeweiligen Ausnahmetatbestände weit definiert werden, vgl. Buchner, 81; so liesse sich eine Abschwächung des «pointierten» Dualismus zu einem leichten Dualismus vollziehen, indem Erlaubnistatbestände beim Verbotsgrundsatz gleichermassen wie die Verbote beim Erlaubnistatbestand weit gefasst würden.

316 Das Regelungsregime für die Personendatenverarbeitung durch öffentliche Stellen des Bundes setzt insb. auch das Legalitätsprinzip um, in Entsprechung der grund- resp. verfassungsrechtlichen Konzeptionierung, vgl. Art. 36, insb. Abs. 1 BV. Das Regelungsregime bezüglich Personendatenverarbeitungen durch Private und den privaten Bereich setzt an der qualifizierten Personendatenverarbeitung an. Erst sie ist es, die zu einer Persönlichkeitsverletzung führt: Die Struktur von Art. 28 ff. ZGB wird in das Datenschutzgesetz importiert. Entsprechend knüpft das DSG am *Subjektschutz* an.

317 Mit ebendieser *dualistischen Ausgestaltung qua entgegengesetztem Ausgangspunkt* ist im DSG die Relevanz *systemischer Schutzerwägungen* in markanter Weise angelegt. Sie finden weiterführende Anerkennung, indem für den öffentlichen Bereich die jeweiligen Spezialerlasse die rechtliche Grundlage zwecks Erfüllung des Legalitätsprinzips liefern. Aber auch im privaten Bereich existieren für spezifische Kontexte, z. B. im Bankenrecht, im Humanforschungsgesetz oder im Arbeitsrecht, bereichsspezifisch motivierte datenschutzrechtliche Sondernormen.

318 Die vorangehenden Ausführungen haben weiter gezeigt, dass im Rahmen der erstmaligen Verabschiedung des DSG der Datenschutz hauptsächlich als Gegenspieler von ökonomischen Interessen wahrgenommen wurde. Der Blick auf den Gesetzgebungsprozess des DSG zeigte, wie sehr ökonomische Rationalitäten die Datenschutzgesetzgebung für den privaten Bereich beeinflussten. Der Widerstand von Wirtschaftsvertretern gab dazu Anlass, zwei verschiedene Bereiche in einem Gesetz zur Verabschiedung zu bringen.

319 Die systemische Schutzdimension des Datenschutzes wurde in der Schweiz bei Lichte betrachtet bislang nur beschränkt bewusst und sachbezogen verhandelt, obschon die bereichsspezifische Differenzierung eigentlicher Brennpunkt im Zuge der Verabschiedung des ersten DSG war. Im Ergebnis zeigt sich die bereichsspezifische Differenzierung in beschriebener Grobstruktur stärker von politischen Kräften als von sachlogischen Argumenten getragen.

320 Wer heute das DSG als Einheitsgesetz in der Hand hält, das den Schutz der Persönlichkeit und der Grundrechte bezweckt, erahnt wenig von der Spannkraft, welche die Auseinandersetzung um die Bedeutung von Kontexten für das Datenschutzrecht in der Schweiz in sich trug. Die aktuellen Entwicklungen in Europa weisen in eine Richtung, in der die systemische Relevanz des Datenschutzrechts weiter in den Hintergrund gedrängt wird. Auch im Bericht der Begleitgruppe Revision DSG wurde dafürgehalten, dass die Bestimmungen für den öffentlichen und den privaten Bereich so weit wie möglich vereinheitlicht werden sollten.[482] Gleichwohl stand die Aufhebung der differenzierenden Mechanik mit Blick auf

482 EJPD, Bericht Begleitgruppe, 8.

den Ausgangspunkt von Personendatenverarbeitungen im öffentlichen gegenüber dem privaten Bereich niemals ernsthaft zur Debatte.

321 In Bezug auf die Frage der Relevanz und Angemessenheit der bereichsspezifischen Differenzierung datenschutzrechtlicher Vorgaben, welche die Schweiz innerhalb des DSG primär durch den entgegengesetzten Ausgangspunkt für den öffentlichen gegenüber dem privaten Bereich implementiert, nimmt das Schweizer System – vergleicht man das Regime mit denjenigen von Europa und den USA – eine *Zwischenposition* ein. Die DSGVO sieht sowohl für den privaten als auch für den öffentlichen Bereich den Ausgangspunkt des Verarbeitungsverbotes mit Erlaubnisvorbehalt vor, wobei diese Entscheidung das Ausgangselement für das monistische System der DSGVO darstellt. Anders dagegen die USA, die den öffentlichen Bereich einer allgemeinen Datenschutzgesetzgebung zuführen, den privaten Bereich indes sektoriell datenschutzrechtlich regulieren. Ein Blick auf den *Fair Credit Reporting Act* brachte hierbei eine in Europa nur ungenügend zur Kenntnis genommene Schutzdimension zu Tage: Der Erlass dient nicht an erster Stelle dem Subjektschutz, wie es der europäischen Tradition entsprechen würde. Vielmehr soll mit dem Erlass die *Integrität des Kredit- und Bankensektors* gewährleistet werden, dessen Effizienz vom Vertrauen in akkurate und faire Personendatenverarbeitungen abhängt. Zugleich macht der Erlass deutlich, dass ökonomische Rationalitäten nicht zwingend gegen, sondern auch für eine Datenschutzregulierung sprechen können.

3.3. Weitere Elemente zur Implementierung des dualen Systems

322 Der infolge der entgegengesetzten Ausgangspunkte *pointierte Dualismus* wird konsequent durch *zusätzliche Instrumente und deren Ausgestaltung* fortgeschrieben, z. B. bezüglich Transparenzvorgaben oder Kompetenzen des EDÖB.[483] Die Totalrevision wird hier allerdings einige Anpassungen bringen, teilweise im Sinne von Vereinheitlichungen.

323 Um in Anknüpfung an den über die Ausgangspunkte definierten Dualismus die Weite und Breite des Feldes zu umreissen: Die allgemeinen Verarbeitungsgrundsätze gemäss Art. 4 DSG resp. Art. 6 nDSG, die als «gemeinsames Fundament» jeder Personendatenverarbeitung bezeichnet wurden und als «gemeinsame Bestimmungen» für den öffentlichen und den privaten Bereich gelten, finden durch die verschiedenen Ausgangspunkte auch eine eigenständige Einbettung und damit Bedeutung.[484] Im privaten Bereich markieren sie die Schranken der grundsätzlich freien Personendatenverarbeitung, während sie im öffentlichen Be-

483 Partikulär ist immerhin der Import eines privatrechtlichen Instrumentariums im Rahmen der Rechtsdurchsetzung in den öffentlichen Sektor gemäss Art. 25 DSG.

484 Vertiefend zweiter Teil, Kapitel IV.–VI.

reich aufgrund des prinzipiellen Verarbeitungsverbotes gewissermassen eine weitere, zweite Schranke liefern. Die generalklauselartigen Bearbeitungsgrundsätze werden im V. Kapitel dieses zweiten Teils zu vertiefen sein.

324 Generalklauselartige Verarbeitungsgrundsätze liefern, sofern sie die Hauptschranke der Personendatenverarbeitung im privaten Bereich darstellen, nur einen *grosszügigen sowie vagen Rahmen*. Zwei Beispiele zur Veranschaulichung: Die Zweckgrundsätze gemäss Art. 4 Abs. 3 resp. Art. 6 Abs. 3 nDSG werden, *erstens*, für den privaten Sektor vom Gesetzgeber nur am Rande näher umrissen. Das DSG selbst verzichtet im privaten Bereich weitgehend darauf, konkretisierte Wertungen und Hierarchisierungen in Bezug auf verschiedene Zweckrelationen vorzusehen.[485] Dagegen werden die Verarbeitungszusammenhänge im öffentlichen Bereich aufgrund des Legalitätsprinzips die Verarbeitungszusammenhänge konkretisiert. *Zweitens* finden sich auch mit Blick auf die Rechtfertigungsgründe für persönlichkeitsverletzende Datenumgänge vom Gesetzgeber keine hinreichend konkretisierten Hinweise.[486]

325 Spezifisch beleuchtet werden in Bezug auf die dualistische Strukturierung die Transparenzvorgaben, denen im privaten Sektor von Gesetzes wegen aufgrund der persönlichkeitsrechtlichen Anknüpfung eine Hauptverantwortung für die Durchsetzung des DSG zugewiesen wird. Zudem werden die Funktion und namentlich die Kompetenzen des EDÖB beleuchtet, die ihrerseits für den öffentlichen und privaten Bereich differenziert werden. Die Totalrevision wird hier Anpassungen bringen, die aber nur angedeutet werden können. Mit ihnen geht eine vereinheitlichende Tendenz einher. Die Darstellung der weiter differenzierenden resp. mit Totalrevision angeglichenen Instrumente ist nicht abschliessend.

3.3.1. Unterschiedliche Transparenzvorgaben und jüngste Angleichungen

326 Ein tragendes Element datenschutzrechtlicher Regulierung ist die Gewährleistung von *Transparenz*.[487] In diesem Zusammenhang sind Auskunftsrechte, Registrierungs- und Informationspflichten sowie der Erkennbarkeitsgrundsatz relevant, vgl. unter noch geltendem DSG die Art. 4 Abs. 3 und Abs. 4 DSG.[488] Auch durch

485 Die wichtigsten Konkretisierungen finden sich für diesen Aspekt in einem gesetzgeberisch konkretisierten überwiegenden Interesse, vgl. Art. 13 Abs. 2 DSG resp. Art. 32 Abs. 2 nDSG.

486 Immerhin hat die Praxis hierbei wichtige Impulse gegeben, indem sie Rechtfertigungsgründe für die Verletzung der allgemeinen Verarbeitungsgrundsätze nur mit Zurückhaltung zulassen will, BGE 136 II 508, «Regeste» und E 5.; entsprechend auch EDÖB, Schlussbericht PostFinance, 6, 23; eine Forderung, wonach der Gesetzgeber vorstrukturierende konkrete Interessenabwägungen vorzunehmen habe, formulierte früh schon Bull, in: Hohmann (Hrsg.), 173 ff., 181.

487 Zur Stärkung der Transparenz mit der Totalrevision: Botschaft DSG 2017–1084, 17.059, 6941 ff., 6972 ff.; EJPD, Bericht Begleitgruppe DSG, 3.

488 Zu den Informationspflichten und dem Auskunftsrecht nach neuem DSG Bühlmann/Lagler, SZW 2021, 16 ff.

die gesetzgeberischen Entwicklungen hinsichtlich der Instrumente, die datenschutzrechtliche Transparenz gewährleisten, zieht sich erneut wie ein roter Faden die Frage nach der Differenzierung resp. Angleichung zwischen dem öffentlichen und dem privaten Bereich.[489] Die nachfolgenden Ausführungen zeichnen die gesetzlichen Entwicklungen aus der *Perspektive des Bereichsbezugs* nach. Hierbei wird sich zeigen, dass im Rahmen der Verabschiedung des ersten DSG über diese Instrumente eine weitere Ausdifferenzierung zwischen öffentlichem und privatem Bereich erfolgte; diese soll mit der Totalrevision indes beseitigt werden.[490]

327 Gemäss Art. 8 Abs. 1 DSG kann jede Person von Inhabern einer Datensammlung grundsätzlich Auskunft über sie betreffende personenbezogene Angaben erhalten. Das *Auskunftsrecht* ist entsprechend vorab an das Vorliegen einer Datensammlung i. S. v. Art. 3 lit. g DSG, nicht aber an deren Registrierung gemäss Art. 11a DSG geknüpft. Es erstreckt sich punktuell auch auf eine *Information über die Herkunft der Daten,* vgl. Art. 8 Abs. 2 lit. a in fine DSG. Im Gesetzgebungsverfahren wurde ein entsprechender Antrag von der Ständerätin Weber gestellt.[491] Vom Berichterstatter Danioth wurde dieses Anliegen, wenig sachlich, als «in der heutigen Zeit sympathisch»[492] bezeichnet. Er erklärte sich zwar mit der Zielsetzung einverstanden, wollte allerdings keine voraussetzungslose Informationspflicht zur Datenherkunft. Im Ergebnis wurde ein Auskunftsrecht verankert, das sich auf die «verfügbaren Angaben» zur Datenherkunft bezieht, vgl. Art. 8 Abs. 2 lit. a in fine DSG. Weiter erstreckt sich das Auskunftsrecht auf den *Zweck der Datenbearbeitung und eine allfällige gesetzliche Grundlage,* Art. 8 Abs. 2 lit. b DSG. Die Einschränkungen des Auskunftsrechts sind unter dem noch geltenden Recht beträchtlich, namentlich auch im privaten Bereich.[493] Gemäss Art. 9 Abs. 4 DSG kann spezifisch und weiterreichend als für den öffentlichen Sektor die Auskunft verweigert werden, sofern ein eigenes überwiegendes Interesse geltend gemacht werden kann und die Daten nicht an Dritte weitergegeben werden.

328 Das Auskunftsrecht verfolgt verschiedene *Stossrichtungen:* Zunächst wird dem betroffenen Datensubjekt ein Anspruch eingeräumt, welcher diesem zumindest formell eine aktive Rolle im Personendatenverarbeitungsprozess zuweisen und es so zumindest ansatzweise dem Status des Informationsobjektes entheben will. Zugleich soll dem Datensubjekt ein *Überprüfungsmechanismus* über die

489 BBl 1988 II 414 ff., 439, 484; EJPD, Erläuternder Bericht, 20 ff. und 56 ff.
490 Vertiefend zu den Entwicklungen mit Blick auf die Transparenzvorgaben Baeriswyl, digma 2020, 6 ff.
491 Weber, AB 88.032, 13. März 1990, 141.
492 Danioth, AB 88.032, 13. März 1990, 141.
493 Belser, in: Schweizer (Hrsg.), 55 ff., 61 ff. bemerkt hierzu, dass es kein Zufall sei, dass die Ausnahmen von der Regel mehr Platz einnähmen als die Regel selbst; zur Regelung nach neuem Recht Bühlmann/Lagler, SZW 2021, 16 ff.

Regelkonformität der Datenbearbeitungshandlungen zur Hand gegeben werden. Dagegen wurden weitere Kontrollinstrumente, beispielsweise eine Bewilligungspflicht für die Einrichtung von Datensammlungen und Informationssystemen durch Private, wie es gewisse ausländische Rechtsordnungen kannten, durch die wirtschaftlichen Interessenvertreter zu Fall gebracht.[494] Entsprechende Entscheidungen sind im Lichte eines Konzeptes zu lesen, das zum einen von einer klaren Differenzierung zwischen öffentlichem und privatem Bereich, zum anderen von einer Anknüpfung des Datenschutzes für den privaten Bereich an den zivilrechtlichen Persönlichkeitsschutz ausgeht. In einem solchen Konzept ist es das Individuum, das betroffene Datensubjekt, dem es an erster Stelle obliegt, die Einhaltung des Datenschutzes durchzusetzen. Das Auskunftsrecht, so wird behauptet, solle dem Subjekt die entsprechende Position einräumen:

> «Über das Auskunftsrecht soll eine betroffene Person […] feststellen können, *ob* und *welche* Personendaten über sie *in welcher Weise* bearbeitet werden. Diese Informationen sollen der betroffenen Person helfen, ihre gemäss DSG bestehenden weiteren Rechte auszuüben. Insofern wird insbesondere auf Art. 4 DSG verwiesen.»[495] [Hervorhebung durch die Autorin]

329 Allerdings hat sich gezeigt, dass Auskunftsrechte und eine daran anschliessende individualrechtliche Überprüfung von Personendatenverarbeitungen auf ihre Gesetzmässigkeit hin faktisch nur marginale Bedeutung erlangt haben.[496] Gleichwohl ist zu attestieren, dass im Zuge der Stärkung datenschutzrechtlicher Anliegen mit den Revisionswellen auch die Geltendmachung der Auskunftsbegehren in der Praxis an Bedeutung gewinnt. Die Implementierung eines Standardprozesses, welcher das Auskunftsrecht regelkonform abwickelt, ist mittlerweile zum Standard geworden.

330 Im Bestreben, das Auskunftsrecht in der Praxis wirksam werden zu lassen, auferlegt Art. 11a DSG Inhabern von Datensammlungen die Pflicht, diese beim EDÖB *registrieren* zu lassen. Es war Koller, der darauf hinwies, dass für ein Auskunftsrecht ein Register der Datensammlungen vorgesehen werden müsse. Zugleich müsse man sicherstellen, dass es nicht zu einer übertriebenen Datenschutzbürokratie komme.[497] Privaten gegenüber wurde die Registrierungspflicht entsprechend beschränkt: Registrierungspflichtig ist nicht jeder Inhaber einer Datensammlung. Vielmehr arbeitet das DSG auch an dieser Stelle mit qualifizierenden Elementen: Registrierungspflichtig ist die Inhaberin einer Datensammlung entweder, wenn sie nach Art. 11a Abs. 3 lit. a i. V. m. Art. 3 lit. c und lit. d DSG regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bear-

494 Vgl. BBl 1988 II 414 ff., 429; Danioth, AB 80.032, 13. März 1990, 142.
495 Rosenthal, HK-DSG, Art. 8 N 1; vgl. zur Auffassung, wonach das Auskunftsrecht der Schlüssel zum Datenschutz sei, auch Belser, in: Schweizer (Hrsg.), *55* ff., *55*.
496 Vertiefend zu einem Vollzugsdefizit dritter Teil, VII. Kapitel.
497 Koller, AB 88.032, 13. März 1990, 134.

beitet, oder wenn nach Art. 11a Abs. 3 lit. n DSG regelmässig Personendaten an Dritte bekannt gegeben werden. Zudem finden sich in Art. 11a Abs. 5 DSG mehrere Ausnahmetatbestände («Escape»-Tatbestände), aufgrund derer die Registrierungspflicht entfallen kann. Dazu gehören die Einsetzung eines internen Datenschutzbeauftragten oder das erfolgreiche Durchlaufen eines Zertifizierungsverfahrens. Indem allerdings die Registersammlung Hilfsfunktionen wahrnimmt und die Ausübung des Auskunftsrechts erleichtern soll,[498] schwächt jede Lockerung der Registrierungspflicht die Durchsetzung des Auskunftsrechts. Dies hat Konsequenzen gerade für den privaten Bereich, für den die Einwilligung in die Personendatenerhebung keine grundsätzliche Voraussetzung für eine Verarbeitungshandlung ist. Die Registrierungspflicht von Datensammlungen wird mit der Totalrevision dahinfallen.

331 Ebenfalls das Ziel der Transparenz verfolgt das in der Schweiz unter den allgemeinen Verarbeitungsgrundsätzen formulierte *Erkennbarkeitsgebot*, vgl. Art. 4 Abs. 3 und 4 DSG resp. Art. 6 Abs. 3 nDSG. Das Erkennbarkeitsgebot wird im Zuge der generalklauselartigen Verarbeitungsgrundsätze genauer analysiert. An dieser Stelle genügt die Anmerkung, dass die im DSG gewählte Vorgabe der Erkennbarkeit ein tiefes Transparenzniveau umsetzt. Hier interessieren die Entwicklungen im Hinblick auf die Diskussionen rund um eine Informationspflicht durch die Datenverarbeitenden. Das DSG, wie es 1992 verabschiedet wurde, kannte keine allgemeine Informationspflicht. Dagegen wurde eine solche Informationspflicht im Rahmen der Teilrevision 2006, in Kraft ab 2008, als Antwort auf die «Motion erhöhter Transparenz» eingefügt.[499]

332 Die mit besagter Teilrevision vorgenommenen Änderungen erfolgten u. a. mit dem Ziel, dem Zusatzprotokoll vom 8. November 2001 zum Europarat-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitender Datenübermittlung beitreten zu können.[500] Zudem wurde mit Art. 7a DSG eine Informationspflicht beim Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen eingefügt, die für Bundesbehörden wie Private einschlägig war.[501] Art. 7a DSG vollzog entsprechend einen Vereinheitlichungsschritt, der indes bald wieder rückgängig gemacht wurde: Nur zwei Jahre später und im Jahr 2010 wurde die Bestimmung aufgehoben, ihr Inhalt zweigeteilt sowie mit jeweils eigenständigem, differenziertem Gehalt mit entsprechend divergierendem Schutzniveau implementiert: eine Informationspflicht, die sich auf die

498 Rosenthal, HK-DSG, Art. 11a N 1.
499 Vgl. Botschaft DSG 2003, 2101 ff., 2106 ff.; eine Übersicht über die am 1. Januar 2008 in Kraft getretene Revision des DSG verschaffen die Beiträge in Epiney/Hobi (Hrsg.), 1 ff.
500 Vgl. Botschaft DSG 2003, 2101 ff.
501 Die Durchsetzung eines Verstosses durch Private wurde als Antragsdelikt ausgestaltet, wobei eine Busse von bis zu CHF 10'000.00 ausgesprochen werden konnte.

Beschaffung von besonders schützenswerten Daten sowie diejenige von Persönlichkeitsprofilen im privaten Sektor beschränkt, vgl. Art. 14 DSG, gegenüber einer allgemeinen, nicht auf qualifizierte Daten oder Datenprofile gerichteten Informationspflicht für Bundesorgane, vgl. Art. 18a DSG. Der Mehraufwand hält sich damit für die personendatenverarbeitenden Privaten in Grenzen.

333 Folglich lässt sich festhalten, dass das noch geltende Schweizer Datenschutzgesetz auch im Rahmen der prozeduralen und organisatorischen Instrumente im Zusammenhang mit dem *Auskunftsrecht sowie der Informierungs- und Registrierungspflicht* den Dualismus fortsetzt.

334 Mit der Totalrevision hingegen werden diese Differenzierungen aufgegeben, indem Informationspflichten gemäss Art. 19 ff. nDSG für Datenverarbeitende sowohl des öffentlichen Bereichs des Bundes als auch des privaten Bereichs regeln. Zugleich wird das Instrument des vom EDÖB geführten Registers von Datensammlungen fallengelassen resp. ersetzt durch eine Pflicht der Verantwortlichen, ein Verzeichnis ihrer Verarbeitungstätigkeiten zu führen, Art. 12 nDSG.[502]

335 Folglich lässt sich nach Totalrevision eine Vereinheitlichungstendenz verzeichnen hinsichtlich der Instrumente und Vorgaben an die Transparenz, die bislang zur Akzentuierung des Dualismus eingesetzt wurden. Neben der Erhöhung der Transparenz ist ein zusätzliches Ziel der Totalrevision, den Datenschutz früher greifen zu lassen.[503] Insofern sind verschiedene neue Instrumente zu nennen, die gleichzeitig die Transparenz von Verarbeitungshandlungen wie auch die Eigenverantwortung der Verarbeitenden stärken. Sie werden einheitlich für Verarbeitende des öffentlichen wie des privaten Bereiches verankert. Zu diesen Instrumenten inspirierten die europäischen Entwicklungen: Neben dem Verzeichnis der Bearbeitungstätigkeiten, welches das Basisinstrument der Verantwortlichen zur Erfüllung ihrer datenschutzrechtlichen Pflichten und damit auch der Transparenzvorgaben darstellt, ist die Datenschutz-Folgenabschätzung zu nennen.[504] Sodann sind als Vorgaben, welche die Transparenz der Personendatenverarbeitungsprozesse stärken, die Meldepflichten bei Datensicherheitsvorfällen sowie die Informationspflichten bei automatisierten Einzelfallentscheidungen zu nennen.[505]

336 *Zusammenfassend* lässt sich festhalten, dass die Transparenzvorgaben unter geltendem Datenschutzgesetz für den öffentlichen Bereich dezidiert unterschiedlich

502 Insofern auch Art. 30 DSGVO.

503 Vgl. EJPD, Bericht Begleitgruppe, 3; Baeriswyl, digma 2020, 6 ff.; gefordert wurde dies bereits 2011 durch Brunner, Jusletter vom 4. April 2011, N 66, Zusammenfassung; dass allerdings auch die Transparenz keine Zauberformel ist, bemerkt bereits Bull, NVwZ 2011, 257 ff., 259.

504 Vgl. Art. 12 und Art. 22 nDSG; Art. 30 und Art. 35 DSGVO.

505 Vgl. Art. 24 nDSG und Art. 34 DSGVO; Art. 21 nDSG; zu den umfassenden Informationspflichten gemäss DSGVO Art. 13 f. DSGVO.

gegenüber dem privaten Bereich gestaltet werden. Die Totalrevision bringt sowohl den Ausbau als auch eine Vereinheitlichung der Transparenzvorgaben. Die Erweiterung des gemeinsamen Regelungskorpus bezieht sich damit *weniger auf die harmonisierende Gestaltung des materiellen Datenschutzrechts* für die beiden Bereiche als vielmehr auf die Schaffung gleichermassen zu beachtender Umsetzungsinstrumente sowie auf die Vereinheitlichung prozeduraler und organisatorischer Vorgaben. Damit ist auf den EDÖB und seine Kompetenzen sowie deren Ausbau durch die Totalrevision einzugehen.

3.3.2. Die behördlichen Kompetenzen, insbesondere diejenigen des EDÖB

337 Im Zusammenhang mit der Durchsetzung datenschutzrechtlicher Bestimmungen sind diverse Behörden aktiv: Neben den Zivilgerichten, dem Bundesverwaltungsgericht und dem Bundesgericht sind sodann die Strafbehörden (insb. im Zusammenhang mit der strafrechtlich sanktionierten Verletzung von Berufsgeheimnissen, aber auch nach Totalrevision gemäss Art. 60 ff. nDSG), sodann insb. der EDÖB und auf kantonaler Eben im öffentlichen Bereich die jeweiligen kantonalen Datenschutzbeauftragten.[506] Die Wirksamkeit des Datenschutzrechts hängt von der Ausgestaltung des Rechtsdurchsetzungsinstrumentariums ab.

338 In der Schweiz wurde von Beginn an vertreten, dass die Verwirklichung des Datenschutzrechts auf die Installation *spezieller Organe* angewiesen sei: Danioth äusserte in der Differenzbereinigung im Ständerat seine feste Überzeugung, wonach es sich beim Datenschutzbeauftragten um den «eigentlichen Dreh- und Angelpunkt eines effizienten Datenschutzes» handle.[507] Mit Art. 18 BGÖ wurde die Position des EDB zu derjenigen des EDÖB erweitert.[508] Zuvor war die Funktion auf den Datenschutz beschränkt. Das vom DSG geschaffene Amt ist im fünften Abschnitt des DSG und Art. 26 ff. resp. nach Totalrevision im 7. Kapitel und Art. 43 ff. nDSG geregelt. Die Totalrevision stärkt die Kompetenzen des EDÖB.

339 Die Position des EDÖB nach DSG ist resp. war *ein wirksames Steuerungsinstrument hinsichtlich der Differenzierung des Datenschutzrechts für den öffentlichen gegenüber dem privaten Bereich*.[509] Zudem artikuliert sich mit dieser Funktion, dass der Datenschutz in der Schweiz – anders als es sich aufgrund der Konsultation des Zweckartikels des DSG oder der zivilrechtlichen Rechtsinstrumente für den privaten Bereich, vgl. Art. 15 DSG und Art. 32 nDSG, vermuten liesse – *keineswegs ausschliesslich dem Individualgüterrechtsschutz* dient. Vielmehr wird

506 Zu Aufgaben und Bedeutung der öffentlichen Datenschutzbeauftragten Jöhri, in: Passadelis/Rosenthal/Thür (Hrsg.), § 8.
507 Danioth, AB 88.032, 12. Dezember 1991, 1063.
508 Öffentlichkeitsgesetz vom 17. Dezember 2004, SR 152.3.
509 Vertiefend zur Sanktionierung von Datenschutzverstössen vgl. Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7.

eine spezifische Funktion geschaffen, um der Einhaltung und Durchsetzung des Datenschutzrechts Nachachtung zu schaffen.[510] Anders gewendet: Es greift in der Konzeptionierung des Gesetzgebers zu kurz, die Rechtsdurchsetzung einzig und allein dem Individuum aufzubürden. Der Einhaltung des Datenschutzes wird über die Funktion des EDÖB als eine Aufgabe anerkannt, die durchaus auch von gesellschaftlicher, nicht nur individueller Relevanz ist.

340 Die Einsetzung eines Datenschutzbeauftragten wurde in der Schweiz mit der Hürdenhaftigkeit individueller Rechtsdurchsetzung begründet.[511] Den Gesetzgebungsmaterialien ist zugleich zu entnehmen, dass man schon früh der *Durchschlagskraft der materiellrechtlichen Normen* des DSG skeptisch gegenüberstand; allem voran wurde das Defizit der ungenügende Strukturierungskraft der generalklauselartigen Regeln antizipiert – chiffriert in den Worten von Bundesrat Koller:

> «Die Aufsichtskompetenzen in diesem Gesetz sind nämlich deshalb besonders wichtig, weil das Gesetz ja wirklich nur grundsätzliche Regeln des Datenschutzes aufstellt und daher ihre Konkretisierung auch aufgrund der voraussehbaren technischen Entwicklungen durch die Aufsichtsorgane zu realisieren ist.»[512]

341 Die Einführung der Funktion eines Datenschutzbeauftragten zielte damit auch darauf ab, die Schwächen eines Regelungssystems, das vorrangig mit *Generalklauseln* arbeitet, abzufedern. Die Relevanz des Amtes wird für den privaten wie den öffentlichen Bereich gar als so hoch eingeschätzt, dass erst seine Kontrollen sicherstellen würden, dass die datenschutzrechtlichen «Vorschriften nicht toter Buchstabe blieben.»[513]

342 In den Kompetenzen des EDÖB werden die bereichsspezifische Differenzierung resp. der duale Ansatz des DSG konsequent fortgesetzt. Die grössten Differenzen zwischen den Räten richteten sich auf den Umfang der Kompetenzen – namentlich im privaten Sektor.[514] Nochmals sei der Prozess im Rahmen der Verabschiedung des DSG eingeblendet: Der Entwurf des Bundesrates schlug einen Datenschutzbeauftragten vor, der auch im privaten Sektor Verfügungsgewalt haben sollte.[515] Die ständerätliche Kommission lehnte diesen Vorschlag ab; sie habe sich den «berechtigten Anliegen nach einer Liberalisierung im Bereich der Wirtschaft nicht verschlossen».[516] Im Ständerat wurde später viel daran gesetzt, dem Datenschutzbeauftragten nur restriktive Kompetenzen zuzubilligen – und

510 Vertiefend zu Aufgabe und Bedeutung des öffentlichen Datenschutzbeauftragten Jöhri, in: Passadelis/Rosenthal/Thür (Hrsg.), § 8.
511 Danioth, AB 88.032, 13. März 1990, 127.
512 Koller, AB 88.032, 12. Dezember 1991, 1064.
513 Vgl. Huber, BK-DSG, Art. 27 N 26a; Peter, 276.
514 Vgl. zum Ganzen namentlich Koller, AB 88.032, 12. Dezember 1991, 1064.
515 Vgl. Koller, AB 88.032, 13. März 1990, 146.
516 Danioth, AB 88.032, 13. März 1990, 127.

ein zunächst angedachtes Verbandsklagerecht zu verhindern. Der Datenschutzbeauftragte sollte im privaten Bereich grundsätzlich lediglich eine Ombudsstellung mit beratender Funktion einnehmen und bloss im Falle von Systemfehlern über weiterreichende Kompetenzen verfügen. Verbindliche Verfügungen sollte er, weil man keinen «Datenschutzpolizisten» wolle, im privaten Bereich (vorbehältlich Verfügungen im Zusammenhang mit der Registrier- und Meldepflicht) nicht erlassen können. Im Übrigen sollten «Kontrahenten» an den Zivilrichter verwiesen werden.[517] Entsprechend wurde im Rahmen der Verabschiedung des ersten DSG in der kleinen Kammer die Funktion des Eidgenössischen Datenschutzbeauftragten für den privaten Bereich konsequent auf diejenige eines reinen Ombudsmanns reduziert.[518]

343 Die nationalrätliche Kommission nahm sowohl die Verfügungs- als auch die Klagelegitimation des Datenschutzbeauftragten wieder in den Entwurf auf. Zugleich sollte nach ihr ein eingeschränktes Verbandsklagerecht vorgesehen werden.[519]

344 Im Ergebnis wurde nicht nur die Verfügungskompetenz für den privaten Bereich, sondern auch die Klagelegitimation gestrichen. Und auch das als Kompensation für besagte Streichungen in den privatrechtlichen Verhältnissen diskutierte *Verbandsklagerecht* setzte sich nicht durch.[520] Eine Verbandsklage hatte bereits der Vernehmlassungsentwurf vorgesehen, wobei eine Datenschutzkommission als Rechtsmittelinstanz vorgeschlagen worden war.[521] Zwei Argumente wurden für einen solchen Vorschlag angeführt: Erstens würde sie als prozedurales Instrument eine Kompensationsfunktion für die zurückgestutzten materiellrechtlichen Normen aufweisen. Zweitens habe sie eine andere Stossrichtung, welche die individualrechtliche Konzeption aufweiche:

> «[…] [D]as Verbandsklagerecht im privatrechtlichen Bereich [ist] eine Norm […], die dazu beigetragen hat, auch Enttäuschte versöhnlich zu stimmen und einen gewissen Ausgleich herzustellen. […] Das bedeutet gleichzeitig auch eine Abkehr von der individualistischen Konzeption, wie sie ursprünglich vorgesehen war, die dem einzelnen die ganze Last aufbürdet, den Rechtsweg zu gehen, sein Recht zu suchen mit allen Schwierigkeiten, die damit verbunden sind, mit allen Auflagen, mit allen Kosten […].»[522]

345 Doch auch die Verbandsklage konnte sich im Zuge der Differenzbereinigung nicht durchzusetzen. Sie – die Verbandsklage – stelle

> «im Privatrecht einen Fremdkörper dar […]. Wir haben heute zur Genüge gehört, dass dem Datenschutzgesetz der Persönlichkeitsschutz zugrunde läge. Es geht also um die

517 Danioth, a. a. O.
518 Vgl. Nabholz, AB 88.032, 10. März 1992, 389.
519 Vgl. Koller, AB 88.032, 5. Juni 1991, 874.
520 Rhinow, AB 88.032, 13. März 1990, 146.
521 Danioth, AB 88.032, 13. März 1990, 127.
522 Onken, AB 88.032, 13. März 1990, 146.

> Rechte der Persönlichkeit, es geht nicht um Kollektivinteressen. Und diese Persönlichkeitsrechte kann jeder ohne weiteres selbst vertreten. Er ist nicht darauf angewiesen, dass irgendein Verband für ihn Klage erhebt.»[523]

346 Der Ständerat setzte sich somit weitgehend durch. Das einzige Entgegenkommen bestand darin, dass der Eidgenössische Datenschutzbeauftragte bei sog. Systemfehlern an die Kommission gelangen können sollte.[524]

347 Im Ergebnis wurde eine Regulierung verabschiedet, die einen Datenschutzbeauftragten mit Kompetenzen sowohl für den öffentlichen als auch den privaten Bereich vorsah. Die Gesetzgebungsmaterialien offenbarten, dass dessen hoheitliche Kompetenzen für den privaten Bereich weitreichend *beschnitten wurden*. Er wurde weder mit Verfügungs- noch mit Klagekompetenz ausgestattet. Für deren Fehlen findet sich alsdann keine Verbandsklage als Kompensation. Wenn auch der Datenschutzbeauftragte, wie in den parlamentarischen Beratungen immer wieder betont, keine Entscheidungs- und Verfügungskompetenz haben solle, so sei doch seine «Funktion als Vermittler und Berater Dreh- und Angelpunkt des Datenschutzrechts».[525]

348 Die Ausführungen zum Gesetzgebungsprozess bezüglich der Ausgestaltung der *prozeduralen Instrumente* dokumentieren erneut, dass das *Verhältnis von Subjektschutz einerseits sowie einer systemischen Schutzdimension resp. kollektiven Schutzinteressen andererseit*s – wenn auch nicht explizit unter diesen Titeln verhandelt – von massgeblicher Bedeutung war. Erneut setzte sich der Entscheid für ein duales Regime, welches den privaten gegenüber dem öffentlichen Bereich differenzierend behandelt, in konsequenter Weise in der Ausgestaltung der prozeduralen Instrumente durch. Der grundsätzlich freie private Bereich sollte ebenso wenig durch eine «starke behördliche Hand» zurückdividiert werden. Für den Privatsektor wurde folglich in Bezug auf den Rechtsschutz der individualrechtliche Ansatz recht konsequent implementiert.

349 Die Hauptaufgaben des Eidgenössischen Datenschutzbeauftragten im Privatbereich nach noch geltendem DSG lassen sich anhand *dreier Kompetenzbereiche* strukturieren: *Beratung* gemäss Art. 28 DSG, *Aufsicht resp. Kontrolle* gemäss

523 Schönenberger, AB 88.032, 13. März 1990, 147; in Bezug auf die Verbandsklage im privaten Bereich lässt sich indes im Zuge der ZPO sowie der geplanten Revision ein Wandel der Ansichten nachzeichnen; vgl. zum kollektiven Rechtsschutz Art. 89 ZPO und zur geplanten Änderung Domanig, Jusletter vom 17. Juni 2019, N 8; zur datenschutzrechtlichen Einschlägigkeit von Art. 89 ZPO Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.14; zur Notwendigkeit, kollektive Rechtsdurchsetzungsinstrumente im Feld des «Bioinformationsrechts» anzuerkennen Gruber, 185 ff.

524 Vgl. Danioth, AB 88.032, 12. Dezember 1991, 1064.

525 Huber, BSK-DSG, Art. 28 N 2; zu den Aufgaben des Datenschutzbeauftragten im Privatbereich vgl. Schweizer, in: Schweizer (Hrsg.), 91 ff., 94 ff.

Art. 29 DSG sowie *Information* gemäss Art. 30 DSG.[526] Entsprechend hilfreiche Informationen finden sich themenspezifisch in den Leitfäden des EDÖB.[527]

Das erste Feld «Beratungsaufgaben und -aufwand» des EDÖB gegenüber Privaten wird auf rund 20 Prozent seines Gesamtaufwandes geschätzt.[528] Gleichwohl wird angenommen, dass das Beratungsangebot des EDÖB von vielen Unternehmen und weiteren privaten Datenbearbeitenden gemieden wird, da bei Mängeln stets mit weiteren Kontrollen im Rahmen der Aufsichtskompetenz des EDÖB gerechnet werden müsse.[529] Dass es sich beim Verhältnis privater personendatenverarbeitender Stellen und dem EDÖB folglich eher um ein Verhältnis des Misstrauens als eines der Kooperation handelt, spiegelt sich in einer Aussage eines privaten Datenbearbeiters, wonach er auf die Beratungsdienste des EDÖB verzichte und es stattdessen vorziehe, sich auf einen wirtschaftsfreundlicheren privaten Berater zu stützen.[530] Die Doppelrolle von Beratung und Aufsicht wird dementsprechend als Grund dafür genannt, weshalb Private Beratungen beim EDÖB vermeiden. Sie fürchten dessen Aufsichtsfunktion. Diese doppelte Funktion wird damit als «Schwachpunkt» bezeichnet; dies ungeachtet der Tatsache, dass die Kompetenzen des EDÖB ohnehin schwach sind.[531] 350

Das zweite Kompetenzfeld, die *Aufsichtsfunktion* mit Abklärungs- und Empfehlungsbefugnissen, basiert auf Art. 29 DSG.[532] Die Aufsichtsbefugnis im Privatbereich nach Art. 29 DSG greift indes – anders als diejenige im öffentlichen Bereich nach Art. 27 DSG – *nur in Konstellationen erhöhter oder grundlegender Relevanz*, was das Gesetz unter dem Begriff des Systemfehlers erfasst.[533] Unter noch geltendem Recht stehen damit im Privatsektor nicht alle Datenbearbeitungen unter der Aufsichtshoheit des Datenschutzbeauftragten. Vielmehr wird die *Aufsicht auf drei bestimmte Sachverhalte beschränkt*: Erfasst werden sog. Systemfehler, Art. 29 Abs. 1 lit. a DSG, Aufsichtsaufgaben im Rahmen der Registrierung von Datensammlungen, Art. 29 Abs. 1 lit. b i. V. m. Art. 11a DSG, sowie Informationspflichten nach Art. 29 Abs. 1 lit. c i. V. m. Art. 6 Abs. 3 DSG. 351

Von *besonderem Interesse* für diese Studie sind die «Bearbeitungsmethoden, die geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler)». Der Ausdruck *Systemfehler* wurde vorab mit möglichen Konfigurationsfehlern der Grossrechner in den 1980er Jahren assoziiert. Heute 352

526 Zu den (auch weiteren) Aufgaben, dargelegt für die beiden Bereiche, Jöhri, in: Passadelis/Rosenthal/Thür (Hrsg.), § 8 N 8.29 ff.
527 Abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden.html> (zuletzt besucht am 3. September 2021).
528 Bolliger/Féraud/Epiney/Hänni, 163; Huber, BSK-DSG, Art. 28 N 12a.
529 Huber, BSK-DSG, Art. 28 N 7.
530 Bolliger/Féraud/Epiney/Hänni, 169.
531 Dies., 191 f.
532 Dazu Jöhri, HK-DSG, Art. 27 N 2 f.; BBl 1988 II 414 ff., 414.
533 Art. 29 Abs. 1 lit. a DSG; Rosenthal, HK-DSG, Art. 29 N 1.

werden indes unter den Begriff «Systemfehler» keineswegs bloss technische Defizite i. S. v. Konfigurations- oder Programmierungsfehlern subsumiert. Vielmehr wird damit auch einfach die Art und Weise von Personendatenverarbeitungen adressiert.[534] Würden durch Personendatenverarbeitungen eine Vielzahl von Personen in ihrer Persönlichkeit verletzt, mache es wenig Sinn, jede einzelne Person den Weg über das Zivilgericht beschreiten zu lassen.[535]

353 Das Tatbestandselement will umgekehrt Datenbearbeitungen, die nur wenige Personen in ihrer Persönlichkeit verletzen, von der Aufsicht des EDÖB ausklammern. Die Bestimmung macht eine Vielzahl von Betroffenen, mithin ein *quantitatives Kriterium*, zur Voraussetzung einer Intervention des EDÖB mittels einer Empfehlung. Damit anerkennt das Gesetz, dass die individualrechtliche Durchsetzung, die eine logische Folge der persönlichkeitsrechtlichen Anknüpfung bildet, nicht per se das angemessene Instrumentarium zur Durchsetzung des Datenschutzrechts ist.[536]

354 Ob die *Quantität* der betroffenen Personen das (isoliert) einschlägige Kriterium sein soll, um das Beurteilungselement für den Systemfehler zu liefern und damit die Untersuchungsbefugnis auszulösen resp. um die individualrechtliche Konzeption zu durchbrechen, wird im Laufe dieser Arbeit an verschiedenen Stellen vertieft werden.[537]

355 Jedenfalls ist in den letzten Jahren eine erhöhte Behördenaktivität gestützt auf Art. 29 Abs. 1 lit. a DSG zu verzeichnen.[538] Ein Blick auf die Praxis des EDÖB belegt, dass dieser den Begriff des Systemfehlers nach Art. 29 Abs. 1 lit. a DSG weit auslegt.[539] Der EDÖB hat wiederholt Empfehlungen gegenüber personendatenverarbeitenden Privaten erlassen und diese bei Nichteinhaltung konsequent zur Beurteilung dem Bundesverwaltungsgericht vorgelegt.

356 Neuer der *Entscheid des Bundesverwaltungsgerichts A-3548/2018 i. S. Helsana+ vom 19. März 2019*, in welchem sich das Gericht nicht nur mit der Aktiv- und Passivlegitimation von Kläger und Beklagter befasste, sondern auch mit dem Tatbestand des Systemfehlers, Art. 29 Abs. 1 lit. a DSG.[540] Hierzu führte es aus, dass

534 Meier, N 1903.
535 Huber, BSK-DSG, Art. 29 N 7.
536 Vgl. Brunner, Jusletter vom 4. April 2011, der die individuelle Kontrolle im Datenschutzrecht für den Privatbereich als zu stark ausgeprägt beurteilt.
537 Die Totalrevision gestaltet die Untersuchungskompetenz des EDÖB für den privaten und öffentlichen Bereich deckungsgleich, wobei das Tatbestandselement des Systemfehlers aufgegeben wird, vgl. Art. 49 ff. nDSG; vertiefend zu den Neuerungen dritter Teil, VIII. Kapitel, A.2.; kritisch beurteilt wird das individualistische Privatheitsparadigma auch von Schwartz, Wis. L. Rev. 2000, 743 ff., 759 ff.
538 Bolliger/Féraud/Epiney/Hänni, 161; die Empfehlungen gestützt auf Art. 29 DSG sind abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April 2021).
539 Huber, BSK-DSG, Art. 29 N 12.
540 BVGer A-3548/2018, Urteil vom 19. März 2019, E 1 und E 1.6.2.

ein Systemfehler vorliege, wenn «Verarbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen».[541] Eine Empfehlung sei basierend auf Abklärungen möglich, Art. 29 Abs. 3 DSG; wird dieser nicht Folge geleistet, steht dem EDÖB die Klage an das Bundesverwaltungsgericht offen, Art. 29 Abs. 4 i. V. m. Art. 35 lit. b VGG. Passivlegitimiert sei der Empfehlungsadressat. Hinsichtlich der Aktivlegitimation des Klägers und dessen Rechtsbegehren führte das Bundesverwaltungsgericht aus, dass die Beschaffung der Postleitzahl, Geburtsdatum und Versichertennummer eine Verarbeitung von Personendaten i. S. v. Art. 2 Abs. 1 DSG sei. Beim 2. Rechtsbegehren handle es sich nicht um eine Bearbeitungsmethode i. S. v. Art. 29 Abs. 1 DSG; es gehe nur um die Rechtmässigkeit des Endzweckes, über die der EDÖB keine Klagelegitimation habe. Zum Systemfehler führt das Bundesverwaltungsgericht in E 1.6.3. aus, dass hierunter alle Datenbearbeitungen fallen, die sich nicht auf einzelne Fälle beziehen, sondern methodisch, mithin wiederkehrend sind und die potentiell eine grössere Zahl von Personen betreffen können, wobei der EDÖB bei der Beurteilung des Vorliegens des Tatbestandselementes einen weiten Ermessensspielraum habe. Ob die Verarbeitungshandlungen gegen das Rechtmässigkeitsprinzip verstossen, sei dagegen eine Frage des Rechts. Unbestritten sei i. c., dass eine grosse Zahl von Personen von Verarbeitungshandlungen betroffen ist. Folglich wurde die Aktivlegitimation des EDÖB und die Passivlegitimation der Beklagten bejaht.[542] Gemäss Art. 44 Abs. 2 VGG gälte der Grundsatz der Sachverhaltsabklärung von Amtes wegen.[543]

Mit entsprechenden behördlichen Aktivitäten des EDÖB hat das Datenschutzrecht für den privaten Bereich wichtige Impulse erfahren und seiner Einhaltung ist ein gewisser Nachdruck verliehen worden.[544] Damit werden die gesetzlich markant unterschiedlich stark ausgestalteten Aufsichtsniveaus des privaten und des öffentlichen Sektors einander durch die Praxis etwas angenähert. Von Gesetzes wegen bleibt das Schutzniveau im privaten Sektor dennoch geringer, so dass bei Privaten nicht abschliessend feststeht, welche Handlungen der Kontrolle durch den EDÖB zugänglich sind. Es ist nicht jede Verarbeitungshandlung und jedweder Einzelfall, bei der der EDÖB in seiner Aufsichtsfunktion aktiv werden kann. Zudem hat eine Empfehlung vonseiten des EDÖB keinen Verfügungscharakter. Gleichwohl beurteilt der EDÖB die Empfehlung als seine härteste «Sanktionsmöglichkeit».[545] 357

541 BVGer A-3548/2018, Urteil vom 19. März 2019, E 1.6.3.
542 BVGer A-3548/2018, Urteil vom 19. März 2019, E 1.7. und E 1.8.
543 BVGer A-3548/2018, Urteil vom 19. März 2019, E 2.
544 Vgl. dritter Teil, VII. Kapitel, A., wo eine *Tour d'Horizon* über die entsprechende Behördenpraxis gegeben wird; vgl. sodann die Übersicht über die Empfehlungen: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April 2021).
545 Bolliger/Féraud/Epiney/Hänni, 181.

358 Wird gemeinhin von der Kompetenz zu Empfehlungen gesprochen, drängt sich umgekehrt die Frage nach einer *Pflicht zum Erlass einer Empfehlung* auf. In der ständerätlichen Differenzbereinigung wurde zwar eine graduelle Verstärkung angedacht, die Kann-Vorschrift durch eine Muss-Vorschrift zu ersetzen.[546] Letztere konnte sich jedoch nicht durchsetzen. Gemäss Art. 29 Abs. 3 DSG *kann* der EDÖB eine Empfehlung abgeben, er *muss* aber *nicht*.

359 Immerhin wird in der Lehre eine Pflicht zum Erlass einer Empfehlung angenommen, allerdings unter restriktiven Voraussetzungen. So soll gemäss Huber das formelle Verfahren nach Art. 29 DSG mit einer Empfehlung abgeschlossen werden, wenn ein «sehr problematisches Vorgehen, das zentrale Rechte massiv einschränkt», vorliege.[547] Anders gilt im öffentlichen Sektor der Erlass einer Empfehlung von Gesetzes wegen grundsätzlich als zwingend.[548]

360 Der EDÖB hat darüber hinaus nach noch geltendem Recht gegenüber Privaten keine eigentlichen Sanktionsmöglichkeiten; das Verhängen von Bussen resp. Strafen oder die rechtswirksame Anordnung von Massnahmen ist ihm nach DSG nicht erlaubt. Dies gilt auch im Rahmen der Untersuchungskompetenzen gemäss Art. 29 Abs. 2 DSG. Wird ihm die Mitwirkung verweigert, stehen ihm selbst keine Zwangsmassnahmen offen. Anders als beispielsweise die Wettbewerbskommission, kann er auch keine Hausdurchsuchung anordnen.[549] Immerhin hat der EDÖB die Möglichkeit, bei einer verweigerten Mitwirkung Strafanzeige zu erstatten, vgl. Art. 34 DSG.[550]

361 Wird eine Empfehlung des EDÖB gemäss Art. 29 Abs. 3 DSG durch den Adressaten des privaten Sektors missachtet, kann der EDÖB den Fall dem Bundesverwaltungsgericht vorlegen, Art. 29 Abs. 3 i. V. m. Art. 33 DSG. Stützt dieses die Empfehlung des Beauftragten durch einen Entscheid, erlangt die Angelegenheit Rechtsverbindlichkeit. Für den Fall, dass die Empfehlung gerichtlich nicht bestätigt wird, vgl. 29 Abs. 4 a. E. DSG, ist der EDÖB zur Verwaltungsgerichtsbeschwerde an das Bundesgericht legitimiert: Eine Empfehlung des EDÖB im Privatrechtsbereich nach Art. 29 DSG gilt als öffentlich-rechtliche Angelegenheit gemäss Art. 82 ff. BGG. Damit wird eine ursprünglich aus dem Privatbereich hervorgehende und auf dem DSG für den privaten Sektor basierende Empfehlung des EDÖB im Instanzenzug als öffentlich-rechtliche Angelegenheit gehandhabt.[551]

546 Danioth, AB 88.032, 12. Dezember 1991, 1064.
547 Huber, BSK-DSG, Art. 29 N 26.
548 Ders., a. a. O., Art. 27 N 13 f. und zu Art. 29 N 26.
549 Zur Wettbewerbskommission mit ihren umfangreichen Kompetenzen vgl. Art. 18 ff. KG, insb. auch Art. 42 KG.
550 BBl 1988 II 414 ff., 485.
551 Huber, BSK-DSG, Art. 29 N 35b.

Ergänzend ist auf die Möglichkeit des EDÖB hinzuweisen, eine *vorsorgliche Massnahme* (ggf. selbst im Superprovisorium) beim Präsidium der ersten Abteilung des Bundesverwaltungsgerichts zu beantragen, Art. 33 Abs. 2 DSG. Zudem kann der EDÖB innerhalb gewisser Schranken die Öffentlichkeit über seine Empfehlungen informieren, Art. 30 Abs. 2 DSG (vgl. zum Informationsauftrag sogleich). 362

Kaum Anlass zur Diskussion gab im Lichte des gewählten Ausgangspunktes für den privaten Sektor und der persönlichkeitsrechtlichen Anknüpfung die *dritte Aufgabe und Kompetenz* des EDÖB, dessen *Informationstätigkeit*. Der EDÖB erstattet jährlichen Bericht an die Bundesversammlung, mit zeitgleicher Aushändigung an den Bundesrat. Diese periodischen Berichte werden publiziert, vgl. Art. 30 Abs. 1 DSG.[552] Ausserdem kann der EDÖB in Fällen des Allgemeininteresses die Öffentlichkeit in geeigneter Weise informieren, vgl. Art. 30 Abs. 2 DSG. Dieses Instrument ist in seiner Wirkungsmacht für die Einhaltung des Datenschutzrechts gerade auch im Zuge des Bedeutungswandels, der dem Datenschutz zugemessen wird, nicht zu unterschätzen, zumal datenschutzrechtliche Verfehlungen heute als Risiko für die Reputation eines Unternehmens gelten. Die Informierung der Öffentlichkeit durch den EDÖB kann folglich durchaus ein wirksames Instrument sein, um datenschutzrechtlichen Belangen Nachdruck zu verleihen. 363

Nach dieser *Tour d'Horizon* über die Kompetenzen des EDÖB, namentlich im privaten Bereich, vor Totalrevision ist festzustellen, dass diese im internationalen Vergleich – bereits vor den mit der DSGVO einhergehenden Neuerungen – als schwach zu bewerten sind.[553] Auf Kritik stiess in der Schweiz insb. die niedrige Aufsichts- sowie die fehlende Verfügungskompetenz des EDÖB für den privaten Sektor.[554] Allerdings ist das gewählte Regime vor dem Hintergrund des für den privaten Bereich gewählten Ausgangspunktes *systemkongruent*. 364

In einer Rückblende lässt sich in der Auseinandersetzung um die Kompetenzen des EDÖB und die Ausgestaltung der prozeduralen Durchsetzungsinstrumente im Zuge der Verabschiedung des ersten DSG eine hohe Ambivalenz hinsichtlich des Entscheides für einen weitgehend freien, privaten Verarbeitungsbereich mit seiner persönlichkeitsrechtlichen Anknüpfung ausmachen. Die Frage nach der Bedeutung systembedingter Trennungen resp. Durchbrechungen zeigt sich ebenso im Themenfeld rund um die Kompetenzen des EDÖB in eindrücklicher Weise. Aufgrund der dualen Struktur mit der Entscheidung für einen prinzipiell freien Bereich im privaten Sektor (nicht jede Personendatenverarbeitung ist verboten, sondern erst die qualifizierte – vertiefend hierzu die nachfolgenden Teile) sowie der persönlichkeitsrechtlichen Anknüpfung des DSG erschiene es inkonsequent, 365

552 Vgl. <https://www.edoeb.admin.ch/edoeb/de/home.html> (zuletzt besucht am 30. April 2021).
553 Huber, BSK-DSG, Art. 29 N 1a; Bolliger/Féraud/Epiney/Hänni, 199, 213.
554 Meier, N 1878.

dem Datenschutzbeauftragten Verfügungs- und Klagekompetenzen zuzuweisen. Anders präsentiert sich das Bild dagegen beispielsweise im Bereich des Wettbewerbsrechts, wo der Markt tiefgreifend reguliert ist und dementsprechend auch behördliche Verfügungskompetenzen vorgesehen sind.

366 Zudem ist es mit Blick auf den «rasanten technischen Fortschritt» fraglich, ob die (bessere) Einhaltung des Datenschutzrechts *in erster Linie* durch die starke Hand eines interventionsmächtigen Staates sichergestellt werden kann. Eine Strategie der DSGVO liegt in einem weit angelegten behördlichen Massnahmen- und Sanktionskatalog, vgl. Art. 83 f. DSGVO. In der Schweiz wurden in diesem Kontext allem voran die drakonischen Bussen zur Kenntnis genommen, die sich der Höhe von Bussen bei Kartellrechtsverstössen annähern.[555]

367 *Zweierlei* gilt es anzufügen: *Zum einen* beschränkt sich die DSGVO keineswegs auf die besagten Bussen, um der Einhaltung der datenschutzrechtlichen Vorgaben Nachachtung zu verschaffen. Vielmehr kommt den Behörden ein weit- und tiefgreifendes Arsenal an hoheitlichen Befugnissen und möglichen Massnahmen zur Verwirklichung des europäischen Datenschutzrechts zu.[556] Die DSGVO wählt somit den Ansatz, die datenschutzrechtlichen Vorgaben mittels starker obrigkeitlicher Massnahmen zu sichern. Der entsprechende behördliche Massnahmenkatalog gemäss DSGVO steht im Einklang mit einem Regime, das von einem grundsätzlichen und einheitlichen Verarbeitungsverbot für den privaten wie den öffentlichen Bereich ausgeht, und ist insofern systemisch kongruent. *Zum anderen* allerdings ist nicht zu übersehen, dass die DSGVO die «Verantwortlichen» (und Auftragsverarbeiter), die personendatenverarbeitenden Stellen selbst, an erster Stelle nachdrücklich in die Pflicht nimmt, für die Einhaltung der datenschutzrechtlichen Vorgaben zu sorgen. Insoweit bringt die DSGVO zugleich eine Stärkung der *Eigenverantwortung* mit sich.

368 Damit ist auf die Neuerungen gemäss Totalrevision einzugehen. Im Rahmen der Verabschiedung des Gesetzes stiessen gerade die Neuordnung der Befugnisse sowohl durch den EDÖB, Art. 49 ff. nDSG, als auch durch die kantonalen Strafbehörden, Art. 60 nDSG ff., auf Widerstand.[557] Die Totalrevision stärkt die Position des EDÖB für den privaten Bereich.[558] Insofern ist eine Annäherung der Normierung des Sanktionssystems für den privaten Bereich gegenüber dem öffentlichen

555 Vgl. Passadelis/Roth, Jusletter vom 4. April 2016, N 23; eine Übersicht über die Bussgeldentscheidungen unter DSGVO geben Kehr/Zapp, CB 2020, 100 ff.; Schweighofer, Jusletter IT vom 9. Februar 2016, N 9.

556 Hierzu auch Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.

557 Vgl. Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zum Vorentwurf, 44 ff., abrufbar unter: <https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ve-berd.pdf> (zuletzt besucht am 30. April 2021).

558 Vertiefend vgl. Rosenthal, Jusletter vom 16. November 2020, N 181 ff.; vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 7168 ff.

Bereich festzustellen. Die über die Gestaltung der Sanktionen bislang erfolgte Fortsetzung und Ausprägung des dualistischen Konzeptes wird nunmehr überwunden. Neu beschränkt sich das «schärfste Instrument» des EDÖB im privaten Bereich nicht mehr auf die «Empfehlung». Vielmehr agiert er nach Totalrevision über das ordentliche Verwaltungsverfahren und kann Verfügungen erlassen, vgl. Art. 51 nDSG. Im Rahmen der durchzuführenden Untersuchungen, die nicht nur beim Vorliegen eines Systemfehlers angezeigt sind, werden ihm mehrere Befugnisse zugesprochen, Art. 50 nDSG. Ein Verstoss gegen datenschutzrechtliche Vorgaben ist von Amtes wegen zu *untersuchen*, vgl. Art. 49 Abs. 1 nDSG, wobei nach Abs. 2 ein Opportunitätsprinzip für Verletzungen von geringfügiger Bedeutung greifen kann. An dieser Stelle kann das nach bisherigem Recht etablierte Kriterium des Systemfehlers als Auslegungshilfe dienen: Beim Vorliegen eines Systemfehlers dürfte das Opportunitätsprinzip nicht greifen.

Der EDÖB selbst kann auch nach totalrevidiertem DSG keine Verwaltungsbussen erlassen. Immerhin ist festzustellen, dass in der Unternehmenspraxis die Verfügung, eine bestimmte Verarbeitungshandlung zu unterlassen, einschneidender als eine Bussgeldzahlung sein kann. Strafbestimmungen und einen Bussenkatalog führen die Art. 60 ff. nDSG ein. Zuständig für die Aussprache entsprechender Bussen bei Vorliegen der Tatbestände gemäss Art. 60 ff. nDSG sind die kantonalen Strafbehörden. Bemerkenswerterweise nicht von einer Bussenandrohung erfasst ist die Verletzung der allgemeinen Verarbeitungsgrundsätze, das Herzstück des materiellrechtlichen Datenschutzrechts. Nach Art. 60 nDSG ist insb. eine Verletzung der im Rahmen der Untersuchung durch den EDÖB statuierten Mitwirkungspflichten strafbewehrt. Mit den Bussen belegt sind nicht die Unternehmen, stattdessen die verantwortlichen Personen. Wer dies allerdings im Unternehmen ist (der Datenschutzbeauftragte, die Mitglieder der Geschäftsleitung oder des Verwaltungsrates oder auch Mitarbeitende niedrigerer Hierarchiestufen), ist aktuell nicht geklärt. 369

Mit dem Fokus auf den Ausbau und die Verschärfung der behördlichen Massnahmen vermag man indes eine Stossrichtung, welche die Neuerungen sowohl nach DSGVO als auch nach totalrevidiertem DSG verfolgen, nicht in den Blick zu nehmen: Betont und gestärkt wird die *primäre Verantwortung der jeweils personendatenverarbeitenden Stellen für die Einhaltung der datenschutzrechtlichen Vorgaben*. Symbolhaft ausgedrückt wird dies auch in der neuen Bezeichnung der Verarbeitenden als «Verantwortliche».[559] Diese «präventive» Funktionsmechanik 370

559 Der Bericht der Begleitgruppe Revision DSG, Normkonzept zur Revision des DSG vom 29. Oktober 2014, spricht von dem Ziel, dass das Datenschutzrecht früher greifen solle, vgl. EJPD, Bericht Begleitgruppe, 3; vgl. Art. 5 lit. j nDSG, wobei die Rolle des Verantwortlichen namentlich auch im Zusammenspiel mit der Rolle des Auftragsverarbeitenden relevant ist, vgl. Art. 5 lit. k nDSG; vgl. Art. 24 ff. DSGVO. Zudem wird das Konzept der gemeinsam Verantwortlichen anerkannt; die Rol-

wird über (teilweise neue) Instrumente wie das Verzeichnis der Verarbeitungstätigkeiten und umfassende Dokumentations- und Rechenschaftspflichten, aber auch die Datenschutz-Folgenabschätzung, die Strategien von «privacy by design» und «privacy by default» sowie die allfällige Funktion eines betrieblichen Datenschutzbeauftragten (beachte die unterschiedliche Forderung qua DSGVO und totalrevidiertem DSG) verwirklicht. Eine richtungsweisende Stossrichtung der Neuerungswellen ist darin zu sehen, dass die personendatenverarbeitenden Stellen selbst in die Pflicht und Verantwortung genommen werden. Das führt im Ergebnis zur Forderung einer umfassenden Daten-Governance und Datenschutz-Compliance.[560] Folglich greift es zu kurz, die «Verbesserung» des Datenschutzes allein im Ausbau der behördlichen Kompetenzen oder der Betroffenenrechte zu verorten. Eine wirksame Rechtseinhaltung im Feld des Datenschutzes im privaten Bereich kann weder isoliert über das (persönlichkeitsrechtlich verletzte) Datensubjekt noch durch einen «starken» Staat – beides «retrospektive» Ansätze – gewährleistet werden. Vielmehr bedarf es an erster Stelle der Verantwortung der Verarbeitenden. Die Einhaltung des Datenschutzrechts fusst offensichtlich auf mehreren Säulen. Welche Bedeutung die bei Datenschutzverletzungen zuständigen Behörden in der Schweiz den neu eingeräumten und verschärften Rechtsdurchsetzungsinstrumenten einräumt, wird sich erst weisen müssen. Unter der DSGVO kann festgestellt werden, dass die zuständigen Behörden der verschiedenen Länder sehr unterschiedlich scharf vorgehen.[561]

C. Ergebnisse und zusammenfassende Kontextualisierung

371 Das *primäre Charakteristikum* des DSG ist sein *Dualismus* mit divergierendem Schutzniveau für den öffentlichen Bereich des Bundes gegenüber dem privaten Bereich. Er wird über einen materiellrechtlichen Grundsatzentscheid vollzogen. Der Dualismus wird in markanter Weise durch einen *entgegengesetzten Ausgangspunkt* für die beiden Sektoren implementiert: Das Datenschutzgesetz sieht für den öffentlichen Bereich der Bundesbehörden ein grundsätzliches Verbot der Personendatenverarbeitungen mit Erlaubnistatbeständen vor. Für den privaten Bereich hingegen gilt die Maxime der Bearbeitungsfreiheit, die durch Schranken begrenzt wird. Die wichtigsten Schranken sind die generalklauselartigen Bearbeitungsgrundsätze, denen sich nachfolgend das Kapitel V. widmet. Der besagte

lendefinierung ist eine zu klärende Vorfrage, an die sich die jeweils zu beachtenden Datenschutzpflichten anschliessen.

560 Vgl. zum Begriff der Compliance und spezifisch zur Datenschutz-Compliance einige Jahre vor dem Inkrafttreten der DSGVO Petri, Jusletter IT vom 1. September 2010, N 3 ff. und N 13 ff.; m. E. zu eng die Beschreibung unter dem Titel der Governance Räther, ZHR 2019, 94 ff., 97; vertiefend hierzu dritter Teil, VIII. Kapitel, A.2.6.

561 Vgl. <https://datenrecht.ch/behoerden/page/2/> (zuletzt besucht am 30. April 2021).

Dualismus, der über einen entgegengesetzten Ausgangspunkt umgesetzt wird, gilt nach geltendem Recht und wird auch mit der Totalrevision nicht aufgegeben, vgl. Art. 12 i. V. m. Art. 4 ff. DSG und Art. 17 ff. i. V. m. Art. 4 DSG resp. Art. 30 ff. i. V. m. Art. 6 ff. nDSG und Art. 33 ff. i. V. m. Art. 6 ff. nDSG.

372 Den Dualismus aufzugeben und einen monistischen Ansatz zu implementieren, stand in der Schweiz weder im Zuge der beiden Teilrevisionen noch im Zuge der Totalrevision zur Debatte.[562] Das DSG setzt damit nach geltendem Recht wie nach Totalrevision – in Abbildung der Mechanik von Art. 28 ZGB – *für den privaten Bereich an der qualifizierten Personendatenverarbeitung* an. Nicht jede Personendatenverarbeitungshandlung begründet eine Persönlichkeitsverletzung. Vielmehr sind es nur qualifizierte Verarbeitungshandlungen, die eine Persönlichkeitsverletzung markieren, die indes gerechtfertigt werden können. Dagegen gilt das Legalitätsprinzip resp. Prinzip des Verarbeitungsverbotes mit der Notwendigkeit eines Erlaubnistatbestandes, der i. d. R. in einem Spezialgesetz definiert wird, für den öffentlichen Bereich des Bundes. Das Datenschutzrecht der Schweiz ist somit ein bereichsspezifisch stark ausdifferenziertes Rechtsgebiet.

373 Materiellrechtlich anders definiert die DSGVO heute sowohl für die Personendatenverarbeitung durch Behörden als auch für diejenige durch Private ein Verarbeitungsverbot mit Erlaubnisvorbehalt, vgl. Art. 6 DSGVO – ein Monismus, umgesetzt durch den datenschutzrechtlich strikteren Ausgangspunkt.

374 In der Schweiz wird der mit den entgegengesetzten Ausgangspunkten dezidiert bereichsspezifisch differenzierende, dualistische Ansatz *im noch geltenden DSG konsequent weiter umgesetzt*. Zwei Instrumente, die eher umsetzungsrechtlicher Natur sind, wurden genauer beleuchtet: zum einen die Transparenzvorgaben, zum anderen die Kompetenzen des EDÖB. Nach noch geltendem DSG setzte sich der Dualismus entsprechend konsequent fort, namentlich über *unterschiedliche Transparenzvorgaben* für die beiden Bereiche, aber auch über die *unterschiedliche Gestaltung der Kompetenzen des EDÖB*. Seine Kompetenzen waren für den privaten Bereich schwach gestaltet. Die Rechtsdurchsetzung wird im noch geltenden Recht in konsequenter Umsetzung des Dualismus und der persönlichkeitsrechtlichen Anknüpfung in erster Linie den Individuen zugewiesen.[563]

375 In Bezug auf besagte Instrumente bringt die *Totalrevision* bedeutsame Neuerungen, die zu einer Annäherung resp. Vereinheitlichung und damit zu einer Abmilderung der bereichsbezogenen Ausdifferenzierung der beiden Bereiche führen. Zum einen werden die Transparenzvorgaben für die beiden Bereiche vereinheitlicht,

562 Brunner, Jusletter vom 4. April 2011, N 1; kritisch zum Festhalten am bisherigen System Wermelinger/Schweri, Jusletter vom 3. März 2008, N 64 ff.; die Frage, ob sich die ursprüngliche Unterscheidung zwischen den beiden Bereichen weiterhin durchführen lasse, wirft explizit auf Baeriswyl, in: Baeriswyl/Rudin (Hrsg.), 47 ff., 59.

563 Vertiefend zweiter Teil, VI. Kapitel.

zum anderen werden die Kompetenzen des EDÖB für den privaten Bereich sowie für die strafrechtliche Verantwortung ausgebaut. Selbst wenn der Massnahmenkatalog in der Schweiz gestärkt wird, bleibt der behördliche Massnahmen- und Sanktionskatalog hinter demjenigen der DSGVO zurück. Die Schweiz wählt hinsichtlich der bereichsspezifischen Ausdifferenzierungsentscheidung also einen Mittelweg: Annäherungen *ja* (insb. durch die Umsetzungsinstrumente), durchgängige Vereinheitlichung *nein* (insb. durch Beibehaltung des materiellrechtlichen Dualismus, basierend auf dem entgegengesetzten Ausgangspunkt).

376 Wenn sich gerade in der DSGVO eine Überzeugung niederschlägt, wonach die Einhaltung des Datenschutzes einer starken behördlichen resp. staatlichen Hand bedarf, setzt sie, wie auch die Totalrevision des DSG, auf eine weitere Strategie: Die personendatenverarbeitenden Stellen werden durch zusätzliche Instrumente – z. B. das Verarbeitungsverzeichnis – als *primär Verantwortliche* in die Pflicht genommen, proaktiv die Vorgaben des Datenschutzrechts zu implementieren. Die DSGVO wie das totalrevidierte DSG zielen darauf ab, eine bessere faktische Einhaltung des Datenschutzrechts zu erreichen. Dies geschieht keineswegs bloss durch eine Stärkung der Position des Individuums sowie der behördlichen Massnahmen und Sanktionen, sondern in erster Linie dadurch, dass die *Verarbeitenden früher und nachdrücklicher in die Pflicht und Eigenverantwortung* genommen werden, datenschutzkonform zu handeln und sich entsprechend organisatorisch sowie prozedural aufzustellen. Insofern folgt die Totalrevision einem von der DSGVO vorgezeichneten Entwicklungstrend in Richtung einer umfassenden Datenschutz-Compliance.

377 Diesen Vereinheitlichungs- und Weiterentwicklungslinien zum Trotz hat die Betrachtung der Entstehungsgeschichte des DSG vor Augen geführt, von welch zentraler Bedeutung die Frage nach der Ausdifferenzierung des Datenschutzrechts zwischen Bereichen war: Die *Auseinandersetzung um die Bereichsdifferenzierung der datenschutzgesetzlichen Regulierung* für den öffentlichen und privaten Bereich war die eigentliche Ursache für die lange Dauer des Gesetzgebungsprozesses zur Verabschiedung des DSG. Sowohl der gescheiterte Versuch, ein Datenschutzgesetz für den privaten Bereich gänzlich zu verhindern, als auch die Abschwächung der Vorgaben für den privaten Bereich gingen massgeblich von der Privatwirtschaft aus. Nach langem Ringen konnte ein Gesetz in Kraft gesetzt werden, dessen Basiskonstruktion im Zweikammersystem zu verorten ist.

378 Dass die datenschutzrechtlichen Herausforderungen gleichwohl facettenreicher sind und spezifische Erwägungen weiterer Verarbeitungskontexte nicht ausgeblendet werden, zeigt sich anhand mehrerer Elemente: im öffentlichen Bereich anhand des Verarbeitungsverbotes mit Erlaubnistatbestand und der damit verbundenen hohen Bedeutung des Legalitätsprinzips, wonach jede Personendatenverarbeitung, um rechtens zu sein, einer rechtlichen Grundlage ausserhalb

des DSG bedarf. Hier liegt die Bruchstelle, an welcher plurale Verarbeitungszusammenhänge – Steuerbereich, Migrationskontext, Strafverfolgung usf. – datenschutzrechtlich angekoppelt werden.[564] Aber auch der private Bereich zeigt sich nicht als einheitlicher Bereich. Vielmehr ist insofern auf spezialrechtliche Gesetze und Bestimmungen zu verweisen, so beispielsweise auf das Humanforschungsgesetz oder den arbeitsrechtlichen Kontext. Zudem ist die Funktion des EDÖB indikativ für den Gedanken, dass es im Datenschutzrecht keineswegs bloss isoliert um den Individualrechtsschutz geht, sondern dass das Rechtsgebiet allgemeiner gesellschaftliche Anliegen schützt.

379 Kernstrukturelement des schweizerischen Datenschutzgesetzes bleibt allerdings – zumindest materiellrechtlich – der Dualismus zwischen öffentlichem und privatem Bereich. Die Beschreibung des Dualismus im DSG, des insofern einschlägigen Gesetzgebungsprozesses im Rahmen seiner Verabschiedung sowie der jüngsten Entwicklungslinien hat die Relevanz rund um die *Fragen systemdifferenzierender Normierungen für den Datenschutz* explizit gemacht. Dieser Dimension allerdings wurde – gerade auch von wissenschaftlicher Seite – nicht zuletzt aufgrund der Anknüpfung von datenschutzrechtlichen Regelungen am Subjektschutz bislang nicht die gebührende Aufmerksamkeit geschenkt.[565]

380 Die Varianzen der gesetzgeberischen Ansätze sind aktuell beträchtlich: Während die DSGVO einen Monismus vorsieht und die Dualität datenschutzrechtlicher Vorgaben zwischen öffentlichen und privaten Personendatenverarbeitenden aufgibt, die Schweiz hingegen am Dualismus zwischen öffentlich und privat festhält, implementiert man in den USA einen anderen Ansatz. Der öffentliche Bereich wird datenschutzgesetzlich reguliert: auf Bundesebene durch den *Privacy Act* 1974. Dagegen kennt das US-amerikanische System kein datenschutzrechtliches Querschnittsgesetz für den privaten Bereich. Im privaten Bereich wird datenschutzrechtlich -nicht zuletzt infolge des tiefliegenden Misstrauens gegenüber staatlichen Eingriffen – mit sektorspezifischen Erlassen legiferiert.[566] Exempla-

564 Für die Schweiz wurde die Bekanntgabe von Personendaten resp. die informationelle Trennung zwischen verschiedenen Bundesbehörden mit jeweils unterschiedlichen Aufgaben von Baumann, SJZ 2006, 1 ff., 3 ff. thematisiert; anwendbar seien teilweise spezialgesetzliche Regelungen, teilweise das DSG und hierbei insb. auch der Zweckbindungsgrundsatz, wobei die öffentliche Verwaltung keine Informationseinheit sei.

565 Druey attestiert im Jahr 1990 sinngemäss, dass trotz der Verabschiedung des DSG das Bewusstsein aufseiten der Juristen für informationsrechtliche Fragen eher peripher sei, vgl. Druey, «Daten-Schmutz», 379 – eine solche Einschätzung wird noch einige Jahre zutreffend bleiben – trotz der Verabschiedung des DSG; vgl. immerhin die Frage nach einer systemischen Schutzdimension des Bankkundengeheimnisses Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.

566 Hierzu Buchner, 15 ff.; mit dem hier vorgeschlagenen Recht auf informationellen Systemschutz wird in die Richtung sektorspezifischer Regulierung gewiesen. Eine solche darf sich indes nicht auf die innersektorielle Gestaltung beschränken; vielmehr sind insb. die Datenflüsse zwischen verschiedenen Sektoren resp. Gesellschaftsbereichen zu gestalten; eine sektorspezifische Lösung erwähnt Cichocki, Jusletter IT vom 21. Mai 2015, N 51; zur Tendenz der Gesetzgebungen in den 1970er Jahren ausserhalb von Deutschland in Richtung bereichsspezifischer Regelungen zu gehen, vgl. Mallmann, 11.

risch wurde auf den *Fair Credit Reporting Act* hingewiesen, dessen einleitender § 602 festhält, dass die akkurate und faire, transparente Personendatenverarbeitung im Kontext des Credit Reporting der Effizienz des Kreditwesens und Banksystems dient, wohingegen unfaire Methoden das Vertrauen in den Sektor erodieren und sich damit der Bereich selbst unterminiert.[567] Bemerkenswerterweise wurde in der Schweiz genau in diesem Kontext und in Bezug auf das Bankkundengeheimnis die Frage nach einer Systemschutzdimension aufgeworfen.[568]

381 Eine solche *systemische Schutzdimension* wird in einem Modell, wie es die Schweiz vorsieht, gerade auch aufgrund der Anknüpfung an die Individualrechte des Datenschutzrechts nur beschränkt sichtbar. Noch weiter in den Hintergrund gedrängt wird sie in einem monistischen System, wie es die DSGVO implementiert, die bereits auf die Basiskategorisierung von öffentlichem und privatem Sektor verzichtet. Immerhin ist in Bezug auf eine systembezogene Differenzierung auf Folgendes hinzuweisen: Indem die DSGVO ebenso Instrumente der «Selbstregulierung» vorsieht, namentlich den betrieblichen Datenschutzbeauftragten, die Integration bereichs- und branchenspezifischer Verhaltensregeln sowie die Zertifizierung, anerkennt sie trotz ihres Monismus die Relevanz bereichsspezifischer Differenzierungen.[569] Mit dem betrieblichen Datenschutzbeauftragten, aber auch mit Zertifizierungen oder der Berücksichtigung branchenspezifischer «Codes of Conduct» wird gewissermassen die «Re-Strukturierung» der Bereiche, in der Grobstruktur auch des privaten Bereiches, vollzogen. Umgangssprachlich ausgedrückt: Der Datenschutz und dessen Einhaltung wird über solche Instrumente der Selbstregulierung in die «Hände» der jeweiligen (privaten) Akteure zurückgespielt. Diese sind es, in primärer Selbstverantwortung, die durch die Erfüllung der zahlreichen Pflichten sicherzustellen haben, konform («compliant») mit dem Datenschutzrecht zu sein. Das Konzept setzt damit früher an und ergänzt so ein Konzept, das Personendatenverarbeitung primär in ihrer Relevanz als Persönlichkeitsverletzung liest.

382 Gänzlich aus dem Blick gerät bei einem Fokus auf das (statisch-räumlich gedachte) Zweikammersystem (Dualismus öffentlich versus privat) und die Person sowie Personendaten als Quasi-Objekte (Dualismus Subjekt versus Objekt) die *dynamische Dimension* der Thematik, wie sie im ersten Teil dieser Arbeit herausgearbeitet wurde. Der historische Teil hat u. a. anhand der Geheimworte und Geheimhaltungspflichten eine Sichtweise herausgearbeitet, welche Datenflüsse innerhalb, namentlich aber ebenso zwischen verschiedenen Kontexten und Berei-

567 Zum Rechtstext vgl. <https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf> (zuletzt besucht am 4. Juli 2021).
568 Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.
569 Vgl. Art. 37 ff. DSGVO; zur Zertifizierung gemäss DSGVO für Cloud-Dienste als effizientes Überwachungsinstrument vgl. Borges, Jusletter IT vom 23. Februar 2017, N 3 f.

chen in das Blickfeld rücken lässt. Die Frage nach einer Systemschutzdimension wird denn auch jüngst im Zusammenhang mit dem Bankgeheimnis aufgeworfen.[570]

383 Zwei zeitgenössische Beispiele sollen die *datenschutzrechtliche Herausforderung und Brisanz von Personendatenflüssen zwischen verschiedenen Kontexten und Bereichen* veranschaulichen: Hierzu an erster Stelle ein Zeitungsbericht mit dem Titel «Das Geschäft mit den Daten. Schweizer Gemeinden verdienen an Adressen».[571] Der Beitrag legt in der Rubrik «Wirtschaft» den Finger auf den Knotenpunkt. Mehrere Gemeinden hatten auch an Private Adressen verkauft und damit ökonomische Interessen verfolgt. Diese Adressen hatten die Gemeinden infolge erfüllter staatlicher Meldepflichten gegenüber der Einwohnerkontrolle bei einer Niederlassung auf dem Gemeindeterritorium erlangt. Für die Gemeinden wurde damit der Adresshandel zu einem Geschäft, das die Staatskasse alimentierte. Die Transferproblematik bei bereichsspezifisch differenzierenden Regulierungen beschrieb für Deutschland grundlegend Buchner, der die Zugriffsbegehrlichkeiten des einem strengeren Datenschutzregime unterliegenden öffentlichen Sektors auf die Datenbestände des niederschwelliger geregelten privaten Bereichs thematisiert.[572] Illustrativ ist in diesem Zusammenhang zweitens der jüngste Facebook-Skandal, wo Personendaten aus persönlichen Kommunikationsbeziehungen, ausgetauscht über Facebook, zu Cambridge Analytica flossen (mutmasslich gegen Entgelt), wobei in der Folge Auswertungen stattfanden und gezielt auf das Wahlverhalten der Facebook-Nutzenden eingewirkt wurde.[573]

384 Nachdem in diesem IV. Kapitel gezeigt wurde, inwiefern die bereichsspezifische Differenzierung für und im Datenschutzrecht eine Kernfrage ist, wendet sich das V. Kapitel den *generalklauselartigen Verarbeitungsgrundsätzen* zu. Diese wurden als das «gemeinsame Fundament» des DSG für den öffentlichen und privaten Bereich beschrieben.[574] Allerdings sind die Grundsätze, wegen des gerade beschriebenen Dualismus, in *je unterschiedliche Funktionsmechanismen* eingebettet – je nachdem, ob sie für den öffentlichen oder den privaten Bereich zur Anwendung kommen. Ihre Bedeutung gilt es in diesen unterschiedlichen Anknüpfungen zu untersuchen.

570 Walder Wyss AG (Isler/Kunz/Müller/Schneider/Vasella), N 14 ff.
571 Vetsch, Weltwoche vom 24. Oktober 1979, 9.
572 Vgl. Buchner, 72 ff.; zum kommerziellen Adresshandel zwischen dem deutschen öffentlich-rechtlichen Rundfunk und privaten Adresshändlern aus datenschutzrechtlicher Perspektive Hermerschmidt, MMR 2005, 155 ff., 156 ff.
573 Vgl. insofern exemplarisch den Bericht: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html> (zuletzt besucht am 30. April 2021); Söbbing, InTeR 2018, 182 ff.
574 So Danioth, AB 88.032, 13. März 1990, 127.

V. Kapitel: Zweites Strukturmerkmal – Generalklauseln

A. Die gemeinsamen Verarbeitungsgrundsätze

1. Vorbemerkungen

385 Wie sieht die materielle Datenschutzregulierung aus, welche die Schweiz an ihr duales System anknüpft? Im Zentrum stehen die *generalklauselartigen Bearbeitungsgrundsätze,* wie sie sich als Kernelemente datenschutzrechtlicher Normierung etabliert haben. Sie sind heute namentlich in Art. 4 DSG sowie in Art. 5 DSGVO niedergelegt. Mit der Totalrevision finden sich diese in Art. 6 nDSG. Im Zuge der Verabschiedung des ersten eidgenössischen Datenschutzgesetzes warb Bundesrat Koller, im Bewusstsein um den Widerstand von privatwirtschaftlicher Seite, für die Implementierung eines «gemeinsamen Minimal-Standards» mit den Worten:

> «Ein wesentliches Merkmal des schweizerischen Entwurfs besteht darin, dass dieser sowohl den Datenschutz in der Bundesverwaltung wie auch jenen im privaten Bereich im gleichen Gesetz regelt. Für eine solche Konzeption spricht, dass die allgemeingültigen Datenschutzgrundsätze auf beiden Gebieten die gleichen sind. Der Betroffene kann durch die Informationsbeschaffung und -weitergabe Privater ebenso stark wie durch Datenbearbeitungen von Privaten verletzt werden. Aber auch das Anliegen einer ökonomischen Gesetzgebung legt eine solche Lösung nahe, denn so lassen sich Überschneidungen und Wiederholungen vermeiden, letztlich also Normen sparen.»[575]

386 Allerdings wurden auch in der Schweiz die *Defizite generalklauselartiger Regelungen* anerkannt. Das Datenschutzrecht blieb nicht von der Kritik verschont, die wiederholt und allgemein an Regulierungen per Generalklauseln geübt worden war.[576] Für Deutschland war es namentlich Simitis, der den Preis eines solchen Normierungskonzeptes als hoch bezeichnete. Allem voran das «Allgemeininteresse» würde mit seiner «kaum zu übertreffenden Elastizität» als «Über-Generalklausel» alles in den Schatten stellen.[577] In der Schweiz wurden die Schwächen des generalklauselartigen Regimes im Gesetzgebungsprozess wie folgt adressiert:

---

575 Koller, AB 88.032, 5. Juni 1991, 949.

576 Kritisch zu den exzessiven Generalklauseln im Datenschutzrecht Simitis, NJW 1997, 281 ff.; Wächter, Falsifikation; Rosenthal, in: Datenschutz-Forum Schweiz (Hrsg.), 69 ff., 70 ff.; grundlegend zu Generalklauseln u. a. Auer, Materialisierung, 1 ff., 130; Röthel, in: Riesenhuber (Hrsg.), 225 ff.; Teubner, *passim*; zur Einschätzung, wonach die ungenügende Steuerungswirkung der Generalklauseln einen bedeutsamen Grund für das sog. Vollzugsdefizit des DSG liefern, dritter Teil, VII. Kapitel.

577 Simitis, NomosKomm-BDSG., Einleitung: Geschichte – Ziele – Prinzipien, N 44 f.

> «M. Danioth s'est félicité tout à l'heure de la densité réglementaire réduite de ce projet de loi, par conséquent de la marge d'appréciation et d'interprétation laissée pour son application. Il n'est pas question d'instruire ici un procès d'intention, Mais il nous reste qu'à espérer que notre confiance est en l'occurrence bien placée. Au fond, toute cette affaire de protection des données est bel et bien basée sur la confiance. Durant des années, les maîtres de fichiers, qu'il s'agisse de fichiers publics ou privés, ont abusé de l'incroyable crédulité des citoyens, des consommateurs, des patients, des assurés, des locataires, des bénéficiaires de prestations sociales, bref, de tous ces très ou trop braves gens. Presque tous avaient un sentiment de confiance et de crédulité qui confinait à la naïveté la plus totale.»[578]

Ähnlich skeptisch äusserte sich im Gesetzgebungsprozess Onken im Zusammenhang mit der bereits dargelegten Änderung betreffend die Verweigerung des Auskunftsrechts.[579] Sollte eine Auskunft im ursprünglichen Vorschlag nur sofern unbedingt notwendig verweigert werden dürfen, könnte nunmehr ein Auskunftsbegehren abschlägig behandelt werden, sofern ein «diffuses» überwiegendes Interesse dazu bestünde.[580] Gleichwohl setzte sich in der Schweiz die Überzeugung durch, wonach die Vorteile einer generalklauselartigen Regulierung überwiegen würden:[581] 387

> «Im Rahmen der Regulierungsfolgenabschätzungen wurde angetönt, unbestimmte Rechtsbegriffe seien nach Möglichkeit zu vermeiden. Beim Datenschutzgesetz handelt es sich indes um eine technologieneutrale Rahmengesetzgebung, welche auf eine Vielzahl unterschiedlich gelagerter Fälle anwendbar bleiben und sich dynamisch weiterentwickeln können muss. Dem Bedürfnis nach exakteren, bereichsspezifischen Ausführungsbestimmungen dienen jedoch die Empfehlungen der guten Praxis.»[582]

Damit ist das *zweite Strukturelement* des DSG eingeführt: *die Regelung mittels Generalklauseln resp. unbestimmten Rechtsbegriffen*. Der letzte Passus bezeichnet nicht nur ein Charakteristikum des eidgenössischen Datenschutzgesetzes, sondern problematisiert und rechtfertigt es zugleich. 388

Wenn auch mit der Totalrevision die Systematisierung, Redaktion sowie Gewichtung der allgemeinen Bearbeitungsgrundsätze punktuell neugestaltet wird, bleiben insb. die Grundsätze der Rechtmässigkeit, von Treu und Glauben, der Verhältnismässigkeit, Zweckbindung und Erkennbarkeit sowohl für den privaten als 389

578 Jaggi, AB 88.032, 13. März 1990, 132.
579 Hierzu zweiter Teil, IV. Kapitel, B.3.3.1.
580 Onken, AB 88.032, 13. März 1990, 129.
581 Mit der Totalrevision werden generalklauselartige Vorgaben auch in Zukunft im Regelungs- und Gesetzeskonzept eine zentrale Bedeutung einnehmen. Die gesetzliche Leitidee, gleichermassen wie diejenige des Dualismus (vgl. insofern zweiter Teil, IV. Kapitel) sowie diejenige der persönlichkeitsrechtlichen Anknüpfung für den privaten Bereich (vgl. insofern zweiter Teil, V. Kapitel), wird auch in Zukunft die Struktur des DSG prägen. Die Totalrevision weicht folglich von den in dieser Schrift herausgearbeiteten drei Strukturmerkmalen nicht ab. Gleichwohl werden ergänzende und flankierende neue Akzente und Aspekte vorgesehen. Dargestellt werden diese Entwicklungen im dritten Teil, insb. im XIII. Kapitel, A.
582 EJPD, Erläuternder Bericht, 36; zur Regelung des Datenschutzes in einem Rahmengesetz auch Danioth, in: Schweizer (Hrsg.), 9 ff., 10.

auch den öffentlichen Sektor zentrale Verarbeitungsvorgaben, vgl. Art. 6 nDSG. Im privaten Bereich greift darüber hinaus die «Persönlichkeit» resp. der Persönlichkeitsschutz als generalklauselartiges Regime, vgl. Art. 12 f. DSG resp. Art. 30 f. nDSG, insb. mit der Generalklausel im Zusammenhang mit den Rechtfertigungsgründen.

390 Die *generalklauselartigen Verarbeitungsgrundsätze* sind *Kernelemente des materiellen Datenschutzrechts*. Sie werden nachfolgend analysiert, mit dem Ziel, Wirkungsweisen, Stärken und Schwächen für ein effektives Datenschutzkonzept herauszuschälen. An den Verarbeitungsgrundsätzen ändert die Totalrevision nichts Wesentliches; die bislang entwickelte Lehre und Rechtsprechung dürfte künftig ebenso einschlägig sein. Da beim Abschluss dieser Studie Totalrevision des DSG gerade erst verabschiedet worden war, bleibt es bei punktuellen Hinweisen auf deren Neuerungen. Immerhin ist dies materiellrechtlich nicht sonderlich problematisch, da die generalklauselartigen allgemeinen Verarbeitungsgrundsätze keine namhaften Veränderungen erfahren. Ins Zentrum gerückt wird somit die datenschutzrechtliche Normierung des noch in Kraft stehenden DSG anhand der gemeinsamen, weitgehend generalklauselartigen Verarbeitungsgrundätze, an die sich private wie öffentliche Stellen des Bundes zu halten haben. Auf die DSGVO wird ebenso bloss am Rande eingegangen. Immerhin ist in Erinnerung zu rufen, dass diese wegen ihres extraterritorialen Anwendungsbereiches auch für personendatenverarbeitende Stellen in der Schweiz einschlägig sein kann, vgl. Art. 3 Abs. 2 lit. a und lit. b DSGVO. Sie ist indes nicht nur aus diesem Grund richtungsweisend für das zeitgenössische Datenschutzrecht.

2. Einbettung

391 Es ist Art. 4 DSG resp. Art. 6 nDSG, der die wichtigsten Vorgaben – «les grands principes», wie Meier sie nennt – für Verarbeitungen von personenbezogenen Angaben durch Bundesbehörden wie Private formuliert.[583] Die Verarbeitungsgrundsätze werden, obschon sehr allgemein gehalten, als «harter Kern» des Datenschutzgesetzes bezeichnet.[584] Sie sind stets dann zu beachten, wenn keine spezifischen anderen Vorgaben greifen. Damit bilden sie zugleich eine Art Auffangregime. Einige der Generalklauseln haben ausserhalb des Datenschutzrechts als eher junge Rechtsmaterie eine lange Rechtstradition, andere gelten als spezifischer mit datenschutzrechtlicher Intention aus der Wiege gehoben, obschon sie

583 Meier, N 621 ff.
584 Ders., N 621; zu den datenschutzrechtlichen Grundsätzen vgl. auch Epiney, in: Epiney/Theuerkauf (Hrsg.), 1 ff., 23 ff.

sich durchaus aus bereits bekannten Grundsätzen ableiten lassen.[585] Der vertieften Analyse sind *fünf Bemerkungen* vorauszuschicken:

392 *Erstens* eröffnet jede Normierung mittels unbestimmter Rechtsbegriffe Räume der Flexibilisierung, Konkretisierung und Rechtsfortbildung.[586] Seit jeher versuchte die juristische Methodenlehre mittels einer trennscharfen Klassifizierung und Kategorisierung der verschiedenen offenen Rechtsbegriffe – unbestimmte Rechtsbegriffe, Generalklauseln, Blankett-Normen, Ermessensbegriffe usf. – eindeutige Vorgaben und damit klare methodische Anweisungen für die Rechtsanwendung zu präsentieren.[587] Im Privatrecht werden bis heute leidenschaftliche Debatten rund um die Lückentheorie und das Verhältnis von Art. 1 und Art. 2 ZGB sowie über das Verhältnis ihrer Absätze geführt. Ebenso intensiv verhandelt werden Fragen nach der Abgrenzung von Konstruktionen, die ein Vorgehen nach Art. 1 ZGB und damit die sog. Auslegung ansprechen, gegenüber den Ermessensentscheidungen nach Art. 4 ZGB.[588] Zu Recht wird festgehalten, dass einige Abgrenzungen und Begrifflichkeiten keineswegs eindeutig und strukturierend ausfallen.[589] Entsprechende Spannungsfelder finden sich selbstredend ebenso in einem Datenschutzrecht wieder, das seine allgemeinen Verarbeitungsgrundsätze in Gestalt unbestimmter Rechtsbegriffe zu einem tragenden Fundament seiner Normierung macht. Die Konkretisierung und deren Methode zeigt sich in einem jungen Rechtsgebiet, das im Schatten der «undurchschaubaren Technologien» operiert und das bislang gerade in der Schweiz – zumindest bis es zum Entwicklungsanstoss qua DSGVO und zur Verabschiedung der Totalrevision des DSG kam – wenig wissenschaftliche wie behördliche Aufmerksamkeit fand, als gleichermassen akut wie herausfordernd. Denn die Wirksamkeit des Datenschutzrechts hängt auch davon ab, wie erfolgreich konkretisierte und damit strukturierende Vorgaben an Datenverarbeitungen formuliert werden.[590]

393 *Zweitens* sind die entgegengesetzten Ausgangspunkte, wie sie im Rahmen des *Dualismus* des DSG im IV. Kapitel dieses zweiten Teils beschrieben wurden,

585 Meier, N 629.
586 Vgl. hierzu z. B. Auer, Materialisierung, *passim*.
587 Dazu Pfaffinger, ZSR 2011, 417 ff., 426.
588 Vgl. Meier-Hayoz, BK-1962-ZGB, Art. 4 N 19 ff.; Hrubesch-Millauer, ZBJV 2013, 469 ff.; BGE 141 III 43, E 2.5.1., Analogie nur bei Lücke; BGE 140 III 636, E 2.1.; 140 III 206, E 3.5.; 138 V 346, E 5; vgl. Dürr, ZK-ZGB, Art. 1 N 230 ff., 525 ff.; zur Analogie als Art. 1 Abs. 1 ZGB zugehöriges Auslegungselement vgl. Hausheer/Jaun, Art. 1 ZGB N 202 f.; zum Analogieschluss als Instrument der Lückenfüllung und Art. 1 Abs. 2 ZGB zugehörend s. Kramer, 191 ff., 211; Honsell, BSK-ZGB I, Art. 1 N 12; vertiefend zur Analogie Emmenegger/Tschentscher, BK-ZGB, Art. 1 N 376 ff. mit Zuweisung zur Lückenfüllung, N 380 und N 164 mit Präsentation eines Vierphasenmodells; kritisch zur etablierten Methodenlehre mit Blick auf Art. 1 ZGB und das Verhältnis von Gesetzestext und Auslegung Amstutz, ZSR 2007, 233 ff., wobei er spezifisch auf die Relevanz der Polykontextualität der modernen Gesellschaft eingeht, 242 ff.
589 Vgl. Kramer, 183 ff. und 199 ff.
590 Eindrücklich insofern Bull, NVwZ 2011, 257 ff., 258, wonach ein Ausweichen in höchstrangige Grossformeln vom Problem ablenke.

ebenso in Bezug auf die allgemeinen Verarbeitungsvorgaben einschlägig. Die allgemeinen Bearbeitungsgrundsätze werden in den beiden Bereichen auf *unterschiedlichen Stufen wirksam*: Im öffentlichen Bereich ist gesetzlich eine *doppelte Schranke* vorgesehen, wohingegen im privaten Sektor nur eine *einfache Schrankenlösung* greift: Im öffentlichen Sektor definiert das prinzipielle Verarbeitungsverbot eine *erste Schranke* für Personendatenverarbeitungen durch Bundesbehörden, vgl. Art. 17 DSG resp. Art. 34 nDSG; eine *zweite Schranke* setzen daran anschliessend, gewissermassen auf einer zweiten Stufe, die allgemeinen Verarbeitungsgrundsätze, vgl. Art. 4 DSG resp. Art. 6 nDSG. Einer solchen doppelten Schrankenordnung entspricht auch das in der DSGVO gewählte Konzept, vgl. Art. 5 f. DSGVO, wenn auch für beide Sektoren. Anders definiert das DSG vor und nach Totalrevision im privaten Bereich die allgemeinen Verarbeitungsgrundsätze als die entscheidenden Schranken der prinzipiell zulässigen Personendatenverarbeitung, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 nDSG. Weil die generalklauselartigen Bearbeitungsgrundsätze insb. gemäss Art. 4 DSG resp. Art. 6 nDSG das Kernstück des materiellen Datenschutzrechts im privaten Sektor darstellen – ihnen kommt die entscheidende Schrankenfunktion zu –, räumt diese Arbeit ihnen einen zentralen Platz ein.

394 *Drittens* ist festzustellen, dass infolge des Dualismus als erstem Charakteristikum des DSG auch der *Interpretationsspielraum* für die beiden Sektoren *nicht identisch* ist. Eine entsprechende Differenzierungsnotwendigkeit wird ungenügend reflektiert, sowohl was die Anwendung als auch was die Auslegung der generalklauselartigen Bearbeitungsgrundsätze betrifft. Wenn oftmals davon gesprochen wird, dass der öffentliche und der private Sektor im DSG ein *gemeinsames Fundament* aufweisen, namentlich mit den allgemeinen Bearbeitungsgrundsätzen gemäss Art. 4 DSG resp. Art. 6 nDSG, dann ist diese Aussage unter Anerkennung des *entgegengesetzten Ausgangspunktes für den privaten gegenüber dem öffentlichen Bereich* zu lesen.

395 *Viertens* ist im Rahmen einer Konkretisierung der generalklauselartigen Verarbeitungsgrundsätze nicht nur ihre Verortung *innerhalb des DSG* relevant, sondern auch ihre *allgemeine Einbettung in die Schweizer Rechtsordnung*, allem voran in das *Verfassungsrecht*. Allerdings finden sich für Art. 13 Abs. 2 BV und dessen Schutzgehalt divergierende Interpretationen – sie reichen von einem behaupteten Recht auf informationelle Selbstbestimmung über die Verbürgung eines Privatsphärenschutzes bis zu einer wortgetreuen «Interpretation» als Missbrauchsgarantie.[591] Solche verfassungsrechtlichen Interpretationsdivergenzen schlagen sich

591 Beispielhaft zu einem Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV mit analogem Gehalt gemäss Rechtsprechung des Volkszählungsurteils des Bundesverfassungsgerichts Baumann, SJZ 2006, 1 ff., 2; Schweizer, SG-Komm.-BV, Art. 13 Abs. 2 N 72; Graham-Siegenthaler, 155; Aebi-Müller, N 541 ff.; Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), 19 ff., 34 ff.; von der

in der Nomenklatur von Lehre und Rechtsprechung zum eidgenössischen Datenschutzgesetz nieder.[592]

Zur Behauptung, wonach in der Schweiz ein Recht auf informationelle Selbstbestimmung garantiert werde – entgegen dem Wortlaut von Art. 13 Abs. 2 BV und der Beschreibung des Systems des DSG für den privaten Bereich als eines der Bearbeitungsfreiheit mit Schranken –, mag die verfehlte Einordnung der *Gültigkeitsvoraussetzungen* der datenschutzrechtlichen Einwilligung bei den allgemeinen Verarbeitungsgrundsätzen, Art. 4 Abs. 5 DSG, verleiten. Die Totalrevision hält an dieser Systematik fest, vgl. Art. 6 Abs. 6 und Abs. 7 nDSG. Der Einwilligung kommt im Schweizer DSG für den privaten Sektor indes *nicht* dieselbe Funktion zu wie in einem System des Verarbeitungsverbotes mit Erlaubnisvorbehalt, wie es Art. 6 DSGVO vorsieht. Ebenda ist die Einwilligung, mangels anderweitigem Erlaubnistatbestand, Voraussetzung für eine rechtmässige Datenverarbeitung. Bei Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG handelt es sich weniger um einen allgemeinen Bearbeitungsgrundsatz als vielmehr um die grundsätzlichen Voraussetzungen für eine rechtsgültige Einwilligung für den Fall, dass eine solche verlangt wird. 396

Fünftens: Die *allgemeinen Bearbeitungsgrundsätze* können in der Schweiz aus *zwei Perspektiven* gelesen werden: Auf der einen Seite formulieren sie gegenüber den Verantwortlichen Vorgaben an die Verarbeitung von Personenangaben, indem sie für den privaten Bereich die Schranken der im Ausgangspunkt grundsätzlich freien Bearbeitung festlegen. Auf der anderen Seite wird anhand der Verarbeitungsgrundsätze und namentlich des Verstosses gegen dieselben die datenschutzrechtliche Persönlichkeitsverletzung – der privatrechtliche Datenschutz gilt als Emanation von Art. 28 ZGB – markiert.[593] Ein Verstoss gegen die allgemeinen Datenverarbeitungsgrundsätze wird vom Gesetzgeber als Persönlichkeitsverletzung definiert. In der Lehre besteht insofern Konsens, als ein Verstoss gegen die Grundsätze von Art. 4 Abs. 1–4 DSG *per se eine Persönlichkeitsverletzung* begründet.[594] Diese Regelmechanik gilt auch nach der Totalrevision. *E contrario* heisst dies, dass Datenbearbeitungen im privaten Sektor, welche die anhand der allgemeinen Bearbeitungsgrundsätze definierten Mindestvorgaben *einhalten*, *keine* Persönlichkeitsverletzung darstellen. Das ist in doppelter Hinsicht konsequent: Zum einen spiegelt es das System von Art. 28 ZGB wider. Demnach be- 397

Gewährleistung eines privatrechtlichen Rechts auf informationelle Selbstbestimmung spricht Probst, in: Epiney/Sangsue (Hrsg.), 41 ff., 52 f.; zum verfassungsrechtlichen Schutz der informationellen Privatheit Rudin, in: Sutter-Somm/Hafner/Schmid/Seelmann (Hrsg.), 416 ff. und 425.

592 Zum Ganzen Rosenthal, HK-DSG, Art. 4 N 1 f.

593 Vgl. vertiefend zweiter Teil, VI. Kapitel.

594 Rosenthal, HK-DSG, Art. 4 N 2; damit eröffnet sich die Frage, ob Rechtfertigungsgründe die Widerrechtlichkeit entfallen lassen, wobei die persönlichkeitsrechtliche Methode der Abwägung von Interessen vorgesehen wird; vgl. hierzu Art. 12 f. DSG und Art. 30 f. nDSG, vertiefend zweiter Teil, VI. Kapitel, B.

gründen nur «qualifizierte» Handlungen resp. Eingriffe eine Persönlichkeitsverletzung. Nicht hinreichend schwere Eingriffe sind persönlichkeitsrechtlich irrelevant – sie tangieren unter Umständen die Persönlichkeit, verletzen diese aber nicht.[595] Zum anderen implementiert das Regelungskonzept konsequent den Entscheid für den Ausgangspunkt der grundsätzlichen Datenverarbeitungsfreiheit mit Schranken im privaten Bereich.

398 Die Grundsätze gemäss Art. 4 Abs. 1–4 DSG resp. Art. 6 Abs. 1–5 nDSG sind die *bedeutsamsten materiellen Vorgaben der Datenschutzgesetzgebung*.[596] Weitere Leitprinzipien, Pflichten und Rechte werden aus ihnen abgeleitet. Sie lassen sich als allgemeinste Vorgaben im Sinne eines Mindeststandards zur *Gewährleistung der fairen oder integren Datenverarbeitung* beschreiben.

B. Die generalklauselartigen Verarbeitungsgrundsätze im Einzelnen

1. Das Rechtmässigkeitsprinzip

1.1. Grundlagen

399 Das Prinzip der Rechtmässigkeit erscheint selbsterklärend, ist es doch Fundament der *gesamten Rechtsordnung und des Rechts an sich*: Jedes individuelle wie behördliche Handeln hat im Einklang mit den Forderungen des Rechts zu stehen – in diesem Sinne artikuliert das Rechtmässigkeitsprinzip seinen eigenen Geltungsanspruch. Folglich ist der Grundsatz der Rechtmässigkeit nicht auf bestimmte Rechtsfelder beschränkt. Vorrangige Bedeutung hat er im öffentlichen Recht als *Verfassungsgebot in Gestalt des Legalitätsprinzips resp. Gesetzmässigkeitsgebotes* erlangt, vgl. Art. 5 Abs. 1 BV, zunächst für die *Grundrechtsdogmatik* und das *Verwaltungsrecht*.[597] Verankert wird der Rechtmässigkeitsgrundsatz sodann im *Strafrecht*, Art. 1 StGB. Im *Privatrecht* hingegen dominiert ein Gegenbegriff – die Widerrechtlichkeit, vgl. Art. 28 ZGB oder Art. 41 OR.

400 In der allgemeinen Datenschutzgesetzgebung figuriert die *Rechtmässigkeit meist an erster Stelle der allgemeinen Verarbeitungsgrundsätze*. An vorderster Stelle des materiellen Datenschutzrechts und der allgemeinen Verarbeitungsvorgaben steht der Grundsatz der Rechtmässigkeit mit Art. 5 Abs. 1 lit. a DSGVO im Datenschutzrecht der EU. Die Schweiz verankert den Verarbeitungsgrundsatz in Art. 4

595 Meili, BSK-ZGB I, Art. 28 ZGB N 38.
596 Mit der Totalrevision wird das Richtigkeitsgebot in den Artikel zu den allgemeinen Verarbeitungsgrundsätzen integriert.
597 Vgl. BGE 142 II 182; spezifisch zur Rechtmässigkeit und Zweckmässigkeit als rechtliche Entscheidungsräume der Verwaltung und damit zum Ermessen im Verwaltungsrecht vgl. Neupert, 3 ff.

Abs. 1 DSG in seiner geltenden Fassung wie folgt: «Personendaten dürfen nur rechtmässig bearbeitet werden.» Art. 6 Abs. 1 nDSG lautet neu «Personendaten müssen rechtmässig bearbeitet werden.» Die Totalrevision des DSG verwendet damit eine imperative Formulierung. Es war nicht immer so, dass sämtliche Verarbeitungen von Personendaten allgemein unter das Rechtmässigkeitsgebot gestellt wurden. Vielmehr fand anfänglich eine Beschränkung auf die Beschaffung von Personendaten mit rechtmässigen Mitteln statt. Damit wurde der Anwendungsbereich und Gehalt des Grundsatzes deutlich enger gesetzt.[598]

401 Welche konkrete Bedeutung und Rolle wird dem Rechtmässigkeitsgrundsatz als Verarbeitungsgrundsatz in der Schweizer Datenschutzlehre und -rechtsprechung zugewiesen? Gehalt und Umfang gelten als umstritten.[599] Vorhandene Konkretisierungsversuche weisen beträchtliche Divergenzen auf.

402 Nachfolgend wird ein Befund vertieft, der sich bereits in den bisherigen Erörterungen andeutete und der den datenschutzrechtlichen Rechtmässigkeitsgrundsatz als *facettenreich sowie multifunktional* benennt. Denn der Grundsatz ermöglicht es, die *komplette Landschaft datenschutzrechtlicher Regulierung* innerhalb, aber auch ausserhalb des Datenschutzgesetzes in den Blick zu nehmen. In diesem Sinne hat das Rechtmässigkeitsprinzip eine *Brückenfunktion*. Parallel dazu lassen sich anhand des Grundsatzes systemische Ansätze des Datenschutzrechts freilegen. Der Rechtmässigkeitsgrundsatz ist somit weit mehr als eine rhetorische Selbstbeschwörung des Datenschutzgesetzes bezüglich seines eigenen Geltungsanspruches.[600]

403 Die folgende Analyse wird von einer Überzeugung angestossen, wonach sich eine konzeptionelle Schwachstelle des Datenschutzrechts dort auftut, wo man sich mit dem Rechtmässigkeitsprinzip auf eine Selbstbestätigung des rechtlichen Geltungsanspruches zurückzieht. Wenn einem prioritär angesiedelten Verarbeitungsgrundsatz keine oder kaum darüber hinausreichende Wirkung verliehen wird, gebietet sich ein kritisches Hinterfragen. An dieser Stelle soll geprüft werden, ob dem Rechtmässigkeitsprinzip weiterreichende Gestaltungsmacht im und für das Datenschutzrecht innewohnt. Ziel der Reflexion ist, den Verarbeitungsgrundsatz dergestalt produktiv zu machen, wie es einem auf dem ersten Platz des materiel-

598 BBl 1988 II 414 ff., 460 und 517.

599 M. w. H. BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4., insb. 5.4.1.; zu den gerichtlichen Ausführungen in Bezug auf die datenschutzrechtlichen Vorgaben vgl. Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; Vasella/Ziegler, digma 2019, 80 ff.; Pärli, SZS 2018, 107 ff.; vertiefte Analysen stehen gleichwohl aus.

600 Vgl. zum Vollzugsdefizit des Datenschutzes dritter Teil, VII. Kapitel; veranschaulichend der Beitrag von Baeriswyl, digma 2010, 140 ff. unter dem Haupttitel «Geschichten aus dem Wilden Westen», wobei er beschreibt, dass der Datenschutz im Zeitalter der Digitalisierung aufgrund des Regelungsregimes des DSG für den Privatbereich auf der Strecke bleibt.

len Datenschutzgesetzes angesiedelten «allgemeinen Verarbeitungsgrundsatz» gebührt.

1.2. Facettenreiche Konkretisierungen – Systematisierung

404 Ein Blick auf die Erwägungen von Lehre und Rechtsprechung zum Rechtmässigkeitsprinzip im Datenschutz für den privaten Sektor dokumentiert, dass sein Gehalt von einer Konsolidierung weit entfernt ist.[601] Als unbestritten gilt einzig, dass eine

> «Datenbearbeitung immer dann unrechtmässig im Sinne von Art. 4 Abs. 1 DSG ist, wenn der Datenbearbeiter dabei gegen eine Rechtsnorm verstösst, die den Schutz der Persönlichkeit bezweckt, dies unabhängig davon, ob sich die Rechtsnorm im Datenschutzgesetz oder in einem anderen Erlass befindet. Nicht geklärt ist jedoch, ob auch der Verstoss gegen eine Rechtsnorm, die nicht (zumindest auch) dem Schutz der Persönlichkeit dient, die Bearbeitung von Personen-daten unrechtmässig macht. Das Bundesgericht hat sich zu dieser Frage bisher nicht geäussert.»[602]

405 Mit diesem Passus hat das Bundesverwaltungsgericht das Rechtmässigkeitsprinzip strikt und m. E. nicht überzeugend resp. unnötig zurückgebunden: Lediglich die Verletzung von Rechtsnormen, welche dem persönlichkeitsrechtlichen Subjektschutz dienen, sollen in eine datenschutzrechtliche Unrechtmässigkeit münden.[603]

406 Unklar ist sodann spezifisch die Relation zwischen Rechtmässigkeit, Unrechtmässigkeit resp. Widerrechtlichkeit. Die Passagen zum Rechtmässigkeitsprinzip und dessen Konkretisierung zeichnen im Verbund gelesen ein diffuses Bild:

> «Eine rechtswidrige Datenbeschaffung durch Private oder Bundesorgane ist immer dann gegeben, wenn ein Verstoss gegen Normen des StGB vorliegt […].»[604]

407 Anders dagegen:

> «Ein rechtswidriges Verhalten liegt dabei immer schon dann vor, wenn die Bearbeitung der Daten gegen eine in der Schweiz geltende rechtlich verbindliche Norm verstösst.»[605]

408 Und eine weitere inhaltliche Variante verleiht der EDÖB dem datenschutzrechtlichen Rechtmässigkeitsprinzip mit den teilweise missverständlichen Worten:

> «Die Bearbeitung von Personendaten darf nur rechtmässig erfolgen. Das heisst, es wird ein Rechtfertigungsgrund benötigt, entweder in Form einer Einwilligung der betroffenen Person, eines überwiegenden öffentlichen oder privaten Interesses oder eines Gesetzes.

601 «Gehalt und Umfang des Rechtmässigkeitsprinzips gemäss Art. 4 Abs. 1 DSG sind umstritten», vgl. BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.1.
602 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.2.
603 Die entsprechende Auslegung ist dem subjektivrechtlich verhafteten Datenschutzkonzept geschuldet. Sie exkludiert das Konzept eines datenschutzrechtlichen Systemschutzes.
604 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
605 So Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.62.

> So ist die Bearbeitung von Daten, die ein Fernmeldedienstanbieter für den Verbindungsaufbau und die Rechnungsstellung benötigt, gesetzlich abgedeckt. Falls dieser jedoch weitere Datenbearbeitungen vornehmen möchte, z. B. zum Aufbau eines Kundentreueprogramms, so braucht er dazu die vorgängige Einwilligung des Kunden.»[606]

409 Regelmässig wird eine persönlichkeitsverletzende Datenverarbeitung angenommen, wenn mit ihr *gegen eine Norm der Schweizer Rechtsordnung verstossen wird*.[607] Dass eine solche rechtfertigbar ist, scheinen die zitierten Passagen m. E. fälschlicherweise auszuschliessen.

410 Umstritten ist, ob eine Datenbearbeitung lediglich dann eine «Persönlichkeitsverletzung gemäss Art. 4 Abs. 1 DSG begründet» (will meinen: i. V. m. Art. 12 DSG), sofern sie auf einem diese erst ermöglichenden oder umsetzenden Verhalten beruht, das unabhängig vom DSG widerrechtlich ist,[608] oder ob auch Verstösse gegen die Vorgaben des *Datenschutzgesetzes selbst verpönt sind* und entsprechend unter Art. 4 Abs. 1 DSG zu subsumieren sind.[609]

411 Dass sich die Verletzung des Rechtmässigkeitsgrundsatzes auf Verstösse gegen Normen *ausserhalb* des Datenschutzgesetzes beschränke, versuchen einige Autoren mit einer Probe aufs Exempel zu erhärten: Wäre beispielsweise die Nichtbeachtung der Registerpflicht gem. Art. 11a DSG ein Fall von Art. 4 Abs. 1 DSG, würde die Nichtanmeldung automatisch eine Persönlichkeitsverletzung aller Personen, die in der Datensammlung aufgeführt werden, begründen. Ebendies, so Rosenthal, könne «niemand ernsthaft behaupten wollen».[610] Im Rahmen des Rechtmässigkeitsprinzips wird somit primär die Konformität von *Datenverarbeitungen mit Normen ausserhalb des DSG* eingefordert.[611]

412 Als Rechtsnormen, deren Nichteinhaltung eine Verletzung des Rechtmässigkeitsgrundsatzes begründet, kommen nicht nur zahlreiche Normen aus dem *Strafgesetz* in Betracht, beispielsweise die Berufsgeheimnisse, sondern auch – im Zusammenhang mit der kommerziellen Datenbearbeitung – Art. 27 ff. ZGB und Art. 3 UWG.[612] Als *unrechtmässig* im Sinne von Art. 4 Abs. 1 DSG gilt indes eine Datenbearbeitung bloss, wenn der Verstoss gegen eine Norm der Schweizer Rechtsordnung *ausserhalb des DSG* liegt und dieser nicht aufgrund einer vorrangigen Gegennorm erlaubt sei.[613]

606 Vgl. hierzu den EDÖB, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/telekommunikation/telefonie/allgemeine-grundsaetze.html> (zuletzt besucht am 30. April 2021).
607 Rosenthal, HK-DSG, Art. 4 N 6 f.; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 5 f.; Rampini, BSK-DSG, Art. 12 N 9.
608 So Ders., a. a. O., Art. 4 N 9 f.
609 In diesem Sinne Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
610 Rosenthal, HK-DSG, Art. 4 N 11 f.
611 Vgl. Meier, N 640.
612 Vgl. Ders., N 641; vgl. auch Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
613 Rosenthal, HK-DSG, Art. 4 N 11 f.

413 Wenn Personendatenverarbeitungen im Einklang mit der gesamten Rechtsordnung zu stehen haben, sind sodann für das Privatrecht ZGB und OR zu beachten. Für das OR hat der Datenschutz im Arbeitsverhältnis besondere Bedeutung erlangt, vgl. Art. 328b OR.[614] Für das ZGB ist das Familienrecht spezifisch erwähnenswert, das für den Kontext der Familie mehrere Normierungen zum Umgang mit personenbezogenen Angaben vorsieht, namentlich im Zusammenhang mit Rechten auf Kenntnis der genetischen Elternschaft resp. Vaterschaft.[615] Eine besondere Auseinandersetzung fand die Frage nach Informationsansprüchen im Adoptionskontext.[616]

414 Die Landschaft einschlägiger Datenschutznormen wird sodann vervollständigt durch zahlreiche *bereichsspezifische Spezialgesetze*, die als Kernthema oder als Teilthema den Datenschutz normieren. Zu nennen sind das Humanforschungsgesetz, vgl. Art. 3 lit. f, lit. h und lit. i sowie Art. 17, Art. 18 Abs. 3 und Art. 32 f. HFG, das Fernmeldegesetz, das Bankengesetz mit Art. 47 BankG. Vor diesem Hintergrund vermag das jüngste Diktum des Bundesverwaltungsgerichts, wonach es unter dem Rechtmässigkeitsprinzip um die Verletzung von Rechtsnormen geht, die dem Schutz der Persönlichkeit dienen würden, nicht zu überzeugen.

415 Trotz Interpretationsdivergenzen lässt sich folgern, dass dem Rechtmässigkeitsprinzip nach DSG eine *Brücken-, Integrations- oder Koppelungsfunktion* zukommt. Es könnte auch als *Drehkreuz* beschrieben werden. In Bezug auf diese Brücken- oder Koppelungsfunktion lassen sich *drei Richtungen* beschreiben. Mit diesen wird deutlich, dass über den Grundsatz datenschutzrechtliche *Präzisierungen und Ausdifferenzierungen* vorgenommen werden.

416 Erstens verbindet das Rechtmässigkeitsprinzip gemäss DSG das *Datenschutzgesetz mit der weiteren Rechtsordnung*. Es geht um die Einbettung des DSG in die gesamte Rechtsordnung resp. die Integration von Normen ausserhalb des DSG in dieses (Koppelungsfunktion nach «aussen»). Eine ähnliche Mechanik ist aufgrund von Art. 7 ZGB bekannt, nach welchem bestimmte Normen des OR ebenso für die zivilrechtlichen Verhältnisse als anwendbar gelten. Dieses zunächst unauffällige Element *vervollständigt das Bild der datenschutzrechtlichen Landschaft*. Es zeigt sich, dass die datenschutzrechtliche Regulierung der Schweiz, trotz des DSG als «Querschnittsgesetz», hoch ausdifferenziert ist. Zwar hat sich die Schweiz mit ihrem DSG – wie die EU mit der DSGVO – für einen «Omnibus»-Ansatz entschieden, wohingegen die USA im privaten Bereich einen sektori-

614 Vgl. insofern die einschlägige Kommentarliteratur. Spezifisch und grundlegend zum Verhältnis und zur Problematik des Datenaustausches zwischen Arbeitgeber und Versicherung Pärli, 1 ff.; Wildhaber, Jusletter vom 6. Dezember 2010.

615 Zum Recht des Ehemannes auf Kenntnis seiner genetischen Vaterschaft ausserhalb des Anfechtungsprozesses Entscheid der 3. Abteilung des Obergerichts des Kantons Luzern (Oger LU) vom 18. September 2012, FamPra.ch 2013, 220; hierzu Pfaffinger, FamPra.ch 2014, 604 ff.

616 Vgl. Art. 286b f. ZGB; vertiefend Dies., *passim*.

ellen Ansatz vorsehen.[617] Das DSG als «Querschnittsgesetz» unterstellt Verarbeitungen von Personendaten durch die Bundesbehörden wie durch Private einer allgemeinen Datenschutznormierung. Allerdings differenziert die Schweiz, wie im IV. Kapitel dieses zweiten Teils herausgearbeitet wurde, innerhalb dieses Querschnittsgesetzes pointiert zwischen dem öffentlichen und privaten Bereich. Spezialgesetzgebungen bringen eine zusätzliche Ausdifferenzierung des datenschutzrechtlichen Regimes mit sich. Damit wird offensichtlich anerkannt, dass *diverse gesellschaftliche Bereiche resp. Kontexte*, wie beispielsweise der Humanforschungsbereich, der Telekommunikationssektor, der Bankensektor, der Arbeitsbereich oder der Bereich der Familie, (zumindest punktuell) datenschutzrechtlich differenziert zu behandeln sind. Entsprechend ist die *Kontextrelevanz* für die datenschutzrechtliche Regulierung selbst in Ländern, die sich für einen «Omnibus»-Ansatz entschieden haben, erstellt.[618] Aus dem Befund, wonach über das datenschutzgesetzliche Rechtmässigkeitsgebot Normen in Spezialerlassen für besondere Verarbeitungskontexte adressiert werden, ergibt sich, dass die Schweiz, trotz der Entscheidung für ein «Querschnittsgesetz», *einen kontextuellen Ansatz* kennt. Ein kontextueller Ansatz, der über den Dualismus von öffentlich und privat gemäss DSG hinausgeht. Diese Charakterisierung des Rechtmässigkeitsprinzips in seiner Koppelungsfunktion wird jüngst eindrücklich bestätigt im Helsana+-Urteil des Bundesverwaltungsgerichts, selbst wenn seine Argumentation stark im Persönlichkeitsparadigma verhaftet bleibt.[619]

In den Erwägungen zum Rechtmässigkeitsprinzip gemäss DSG stehen indes *weni-* 417
ger Integrations- als vielmehr Abgrenzungsthemen im Vordergrund, die im Lichte der Gesetzeshistorie nachvollziehbar werden. So bereitet insb. die Abgrenzung zum Zweckbindungsgrundsatz Schwierigkeiten. Zudem münden Konkretisierungsversuche nicht selten in eine Vermengung mit dem Verarbeitungsgrundsatz von Treu und Glauben oder in die Aussage, dass den beiden Grundsätzen kein materieller Unterschied eigen sei.[620] Die Abgrenzungsthematik ist nicht neu, wurde doch in den 1980er Jahren eine vereinte Regelung geplant:[621] So lautete ein ursprünglicher Vorschlag für einen Art. 4 Abs. 1: «Personendaten dürfen nur *mit rechtmässigen Mitteln und nicht wider Treu und Glauben* [Hervorhebung durch die Autorin] beschafft werden».[622] In Kraft trat 1992 ein Art. 4 Abs. 1 DSG mit

617 Nissenbaum, 235.
618 wegweisend zu diesem zentralen Konzept für Privacy-Belange Nissenbaum, *passim*; in Europa weniger offensichtlich als in den USA mit seinem sektorspezifischen Ansatz für den privaten Bereich.
619 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018; zum Urteil s. auch Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; Vasella/Ziegler, digma 2019, 80 ff.; kritisch zur verordneten Selbstverantwortung Pärli, SZS 2018, 107 ff.
620 Vgl. Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 5; Pedrazzini, Grundlagen, 26; Meier, N 641 sieht in der Beschaffung von Daten zu Marketingzwecken unter der falschen Angabe, dass die Erhebung zu Forschungs- oder Statistikzwecken erfolgt, einen Verstoss gegen Art. 4 Abs. 1 DSG.
621 Vgl. Steinauer, in: Schweizer (Hrsg.), 43 ff., 45.
622 Vgl. BBl 1988 II 414 ff., 460 und 517.

dem Wortlaut: «Personendaten dürfen nur rechtmässig beschafft werden». Man separierte in einem *ersten Schritt* den Bearbeitungsgrundsatz der Rechtmässigkeit von Treu und Glauben; letzterer wurde in einen Abs. 2 ausgelagert. Der so verselbstständigte Rechtmässigkeitsgrundsatz fokussierte eingrenzend auf die Personendaten*beschaffung*. Es folgte *in einem zweiten Schritt* mit der Teilrevision von 2003 eine Ausdehnung des Rechtmässigkeitsgebotes, wobei die bis heute in Kraft stehende Version von Art. 4 Abs. 1 DSG lautet: «Personendaten dürfen nur rechtmässig bearbeitet werden.»

418 Gesetzlich wird folglich die Einschlägigkeit des Rechtmässigkeitsprinzips *für den gesamten Verarbeitungszyklus* von Personendaten verbürgt.[623] In der Lehre gilt gleichwohl die unrechtmässige Beschaffung und hierbei namentlich diejenige *durch unrechtmässige Mittel wie Drohung, Diebstahl, Arglist und Täuschung, Zwang* als paradigmatisch für eine Verletzung des Rechtmässigkeitsgebotes gemäss Art. 4 Abs. 1 DSG.[624]

419 Art. 4 Abs. 1 DSG resp. nach Totalrevision Art. 6 Abs. 1 nDSG sieht ein *umfassendes Rechtmässigkeitsgebot für die Bearbeitung von Daten auf jeder Prozessstufe vor*, was internationalen Vorgaben entspricht. Dennoch steht die Rechtmässigkeit hinsichtlich der Beschaffung von Personendaten im Vordergrund. Der Grundsatz richtet sich, wenn auch nicht ausschliesslich, auf die «*Eintrittskontrolle*». Dass der rechtmässigen Erhebung besondere Relevanz zugemessen wird, ist in Anbetracht der Tatsache angemessen, wonach einmal erhobene Personendaten kaum mehr aus dem «Informationskreislauf» eliminiert werden können. Speichermöglichkeiten und Weiterverarbeitungen sind technisch nahezu unbeschränkt möglich und Löschungen stellen heute in der Realität eine grosse Herausforderung dar. Wird also dem «initialen» Eintritt von Personendaten in Bearbeitungsprozesse – der Erhebung – auch in der Schweiz über das Rechtmässigkeitsgebot erhöhte Aufmerksamkeit geschenkt, bleibt man damit dennoch – zumindest formell betrachtet – weit von Systemen entfernt, die einen Grundsatz der *Direkterhebung* anerkennen.[625]

420 Mit der Akzentuierung der Rechtmässigkeit auf den Zeitpunkt der Personendaten*erhebung* wird man auf den Grundsatzentscheid für einen Ausgangspunkt der Datenschutzgesetzgebung zurückgeführt und sieht sich mit dieser Korrelation

623 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 5.
624 Vgl. Meier, N 369 f.
625 So Deutschland in § 4 Abs. 2 BDSG vor den Anpassungen des Gesetzes an die Vorgaben der DSGVO. Die DSGVO verankert kein Direkterhebungsgebot, womit die Entwicklungen in diesem Bereich in den Mitgliedstaaten der EU, welche aufgrund der Öffnungsklauseln Regelungsräume haben und diese durch Ausführungsgesetzgebungen nutzen, offen sind; vgl. auch <https://www.cr-online.de/blog/2016/05/04/dsgvo-was-wird-aus-dem-grundsatz-der-direkterhebung/> (zuletzt besucht am 30. April 2021).

konfrontiert. Auch in diesem Zusammenhang findet das Rechtmässigkeitsprinzip verschiedene Bedeutungsgehalte.

421 Somit ist auf eine *zweite*, etwas anders gelagerte *Koppelungs- und Koordinationsmechanik* des Rechtmässigkeitsprinzips einzugehen: diejenige «nach innen» im Sinne der Referenz auf den datenschutzgesetzlichen Ausgangspunkt der Personendatenverarbeitung. In Systemen mit prinzipiellem Verarbeitungsverbot sind Personendatenverarbeitungen erst und nur dann rechtmässig, wenn sie von einem Erlaubnistatbestand gedeckt werden, vgl. Art. 6 i. V. m. Art. 5 Abs. 1 lit. a DSGVO.[626] Die Unrechtmässigkeit jeglichen Umgangs mit Personendaten ist die gesetzlich angenommene Regel, es sei denn, es liegt ein Erlaubnistatbestand vor. Das Vorliegen eines Erlaubnistatbestandes ist folglich vorrangige Bedingung für eine rechtmässige Personendatenverarbeitung. Gründet der Privatsektor der Schweiz datenschutzrechtlich in der Basisannahme der «Rechtmässigkeit» der Verarbeitung, wird die Ausnahme – die *Unrechtmässigkeit* – zum eigentlichen Bezugspunkt. Eine Hauptherausforderung im Umgang mit dem Rechtmässigkeitsprinzip im privaten Bereich liegt in der Koordinierung des Begriffs der «Rechtmässigkeit» der Datenbearbeitung i. S. v. Art. 4 Abs. 1 DSG mit der persönlichkeitsverletzenden Datenbearbeitung, Art. 12 f. DSG, neu vgl. Art. 30 f. und Art. 6 Abs. 1 nDSG. Die unrechtmässige Datenverarbeitung ist grundsätzlich widerrechtlich, es sei denn, es liegen Rechtfertigungsgründe vor.[627] Es fragt sich: Bedeutet ein Verstoss gegen das Rechtmässigkeitsgebot i. S. v. Art. 4 Abs. 1 DSG per se eine widerrechtliche Persönlichkeitsverletzung, womit also die Rechtfertigung ausgeschlossen würde? Ist der Begriff «unrechtmässig» i. S. v. Art. 4 Abs. 1 DSG gleichzusetzen mit demjenigen der Widerrechtlichkeit i. S. v. Art. 12 f. DSG? Wie lassen sich «Rechtmässigkeit», «Unrechtmässigkeit» resp. «Widerrechtlichkeit» verstehen und koordinieren? Offenkundig lässt sich das Rechtmässigkeitsprinzip harmonischer in das System des öffentlichen Bereiches als in dasjenige des privaten Bereichs einfügen.

422 In Bezug auf den *Dualismus* zeigt sich das Rechtmässigkeitsprinzip als *Drehkreuz*, das unterschiedliche Ausrichtungen erhält, je nachdem, für welchen Bereich – den öffentlichen oder den privaten – man an dieses herantritt. Die Rechtmässigkeit einer Datenbearbeitung im *öffentlichen Bereich* setzt entsprechend dem Legalitätsprinzip eine rechtliche Grundlage ausserhalb des DSG voraus, Art. 4 Abs. 1 i. V. m. Art. 17 DSG, nach Totalrevision Art. 34 i. V. m. Art. 6 Abs. 1 nDSG. Die fehlende gesetzliche Grundlage gemäss Art. 17 DSG gilt als

626 Vgl. § 4 Abs. 1 BDSG; Art. 6 Abs. 1 DSGVO; zur humoristischen «Verarbeitung» der DSGVO/GDPR mit den GDPRTOONS und den Cartoon von Dreyer, abrufbar unter: <http://www.gdprtoons.com> (zuletzt besucht am 30. April 2021).

627 Illustrativ hierfür Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6 f.

klassisches Beispiel für einen Verstoss gegen Art. 4 Abs. 1 DSG.[628] Hingegen ist die rechtmässige Datenbearbeitung im *privaten Bereich* eine, die nicht widerrechtlich das Persönlichkeitsrecht verletzt, Art. 4 Abs. 1 i. V. m. Art. 12 f. DSG resp. Art. 6 Abs. 1 i. V. m. Art. 30 f. nDSG. Die Aussage in der Botschaft zur Verabschiedung eines ersten Datenschutzgesetzes, wonach die allgemeinen Bearbeitungsgrundsätze als «gemeinsames datenschutzrechtliches Fundament» für den öffentlichen und den privaten Bereich gelten, bedarf damit der *Präzisierung: Der Rechtmässigkeitsgrundsatz entfaltet sich unterschiedlich für den privatrechtlichen und den öffentlich-rechtlichen Datenschutz der Schweiz, weil er divergierend eingebettet ist.* Seine prominenteste Anknüpfung hat das Rechtmässigkeitsprinzip seit jeher im öffentlich-rechtlichen Legalitätsprinzip mit der Funktion, staatliches Handeln zu legitimieren. Hier verlangt das Legalitätsprinzip, staatliches Handeln an das Recht zu binden («Verboten ist, was nicht erlaubt ist»). Für den privaten Bereich ist die Rechtmässigkeit die implizite Basisannahme. Es sind die Schranken, deren Durchbrechung Datenverarbeitungen zu unrechtmässigen Datenverarbeitungen machen und damit zu einer Persönlichkeitsverletzung führen, die mangels Rechtfertigungsgrund auch widerrechtlich ist.

423 An dieser Stelle kann im Sinne eines *Zwischenergebnisses* festgehalten werden, dass dem Rechtmässigkeitsprinzip eine *Koppelungsfunktion* in *zweierlei Richtungen* zukommt: Zum einen erfolgt über dieses die *Inklusion von Normen ausserhalb des DSG* in das allgemeine Datenschutzregime, zum anderen dient es der Anknüpfung an die innerhalb des DSG gewählten, entgegengesetzten Ausgangspunkte für den öffentlichen und privaten Sektor. Über das Rechtmässigkeitsprinzip wird der jeweils in einem Datenschutzsystem gewählte *Ausgangspunkt* – Verarbeitungsverbot mit Erlaubnistatbeständen oder Grundsatz der Freiheit der Datenverarbeitung mit Schranken – *angekoppelt*. Mit Blick auf den Dualismus zeigt sich das Rechtmässigkeitsprinzip als *Drehkreuz*, das unterschiedliche Ausrichtungen erhält, je nachdem, für welchen Bereich – den öffentlichen oder den privaten – man es liest. Der Rechtmässigkeitsgrundsatz entfaltet sich unterschiedlich für den privatrechtlichen und den öffentlich-rechtlichen Datenschutz der Schweiz, weil er divergierend eingebettet ist.

424 Es verbleibt, *drittens*, eine «Koordinierungsaufgabe», die Koordinierung des *Rechtmässigkeitsprinzips im privaten Bereich* mit dem *privatrechtlichen Persönlichkeitsschutz* und dessen Dogmatik. Die nachfolgenden Erwägungen gehen der Frage nach, wie die Koordinierung des Rechtmässigkeitsprinzips mit dem System des Persönlichkeitsschutzes gemäss Art. 28 ZGB und dem dort verwendeten Begriff der *Widerrechtlichkeit* bewerkstelligt werden kann.[629] Bezüglich der Harmo-

628 So Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 6.
629 Hierzu sogleich mehr zweiter Teil, VI. Kapitel, B., insb. 2.–4.

nisierung der Figuren der «Rechtmässigkeit» resp. «Unrechtmässigkeit» sowie der «Widerrechtlichkeit» werden verschiedene Meinungen präsentiert.

425 Vertreten wird, dass vorab ein Verstoss gegen eine Rechtsnorm (ausserhalb des DSG) die Verletzung des Rechtmässigkeitsgebots i. S. v. Art. 4 Abs. 1 DSG begründet. Eine so erstellte Unrechtmässigkeit gemäss Art. 4 Abs. 1 DSG begründet eine Persönlichkeitsverletzung, vgl. Art. 12 Abs. 2 lit. a DSG, womit das Vorliegen eines Rechtfertigungsgrundes zu prüfen ist.[630]

426 Anders die Argumentation des EDÖB im Fall Logistep, der zum Bundesgerichtsentscheid BGE 136 II 508 führte. Die Frage der Rechtmässigkeit wird auf die Frage der Widerrechtlichkeit einer Persönlichkeitsverletzung ausgerichtet. Der EDÖB monierte einen Verstoss gegen das Rechtmässigkeitsprinzip und hielt dem Bundesverwaltungsgericht vor, «Art. 12 Abs. 2 lit. a DSG falsch ausgelegt zu haben».[631] Die aktuelle Bestimmung schliesse seiner Meinung nach Rechtfertigungsgründe aus. Stattdessen müsse geprüft werden, ob ein Grundsatz der Datenbearbeitung verletzt worden sei. Dies erfordere eine Verhältnismässigkeitsprüfung, welche die bestehenden Rechtfertigungsgründe mitberücksichtige. Das Bundesverwaltungsgericht habe die dabei notwendige Interessenabwägung fehlerhaft vorgenommen, denn es bestünden keine überwiegenden privaten oder öffentlichen Interessen. Die Persönlichkeit der betroffenen Personen sei somit widerrechtlich verletzt worden. Indem die Vorinstanz dies verkannt habe, habe sie auch gegen das in Art. 4 Abs. 1 DSG verankerte *Legalitätsprinzip* verstossen.[632] Das Bundesgericht dagegen hielt dafür, dass eine Rechtfertigung ebenso im Rahmen von Art. 12 Abs. 2 lit. a DSG denkbar sei.

427 Die heute wohl herrschende Lehre und Rechtsprechung vertritt die Ansicht, dass auch ein Verstoss gegen die allgemeinen Verarbeitungsgrundsätze, wie sie in Art. 4 DSG und in Art. 12 Abs. 2 lit. a DSG formuliert werden, einer Rechtfertigung zugänglich sind. Allerdings dürfe dies nur mit Zurückhaltung angenommen werden.[633] Die Frage nach dem Rechtmässigkeitsprinzip und der Widerrechtlichkeit im privaten Bereich ist damit indes noch nicht spezifisch beantwortet. Im Zentrum steht die Frage, welche Verstösse gegen Vorgaben innerhalb des DSG als «Verstoss gegen das Rechtmässigkeitsprinzip» zu qualifizieren sind. Sie stellt sich nicht nur aufgrund der Tatsache, dass das Rechtmässigkeitsprinzip dem Grundsatz nach selbst unbeschränkt auf das Normgefüge eines Regelungsregimes verweist. Hieraus würde für das Datenschutzrecht im privaten Sektor folgen,

630 So Rosenthal, HK-DSG, Art. 4 N 7 ff.; vgl. insofern neu Art. 6 Abs. 1 i. V. m. Art. 30 Abs. 2 lit. a nDSG.
631 BGE 136 II 508, E 2.1.
632 BGE 136 II 508, E 2.1.
633 Mit Hinweis auf BGE 136 II 508, E 5.2.4.; Hussein, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.126; Rosenthal, HK-DSG, Art. 12 N 16 ff.; mit Hinweis des Auslegungshinweises des BJ Rampini, BSK-DSG, Art. 12 N 9b.

dass Verstösse gegen bestimmte Datenschutzvorgaben, die nicht explizit von Art. 12 DSG als persönlichkeitsverletzend taxiert werden, über das Rechtmässigkeitsprinzip und damit Art. 12 Abs. 2 lit. a DSG in den persönlichkeitsverletzenden Bereich fallen. Eine weite Auslegung wird mit dem Ingress von Art. 12 Abs. 2 DSG eröffnet, indem er die durch Datenverarbeitungen erfolgenden persönlichkeitsverletzenden Tatbestände *enumerativ* aufführt. Zwar liesse sich mit Fug und Recht anführen, dass ein Umweg über das Rechtmässigkeitsgebot überflüssig ist. Je grosszügiger man Verstösse gegen Vorgaben des Datenschutzgesetzes direkt oder über das Rechtmässigkeitsprinzip in die Persönlichkeitsverletzung inkludiert, desto höher wird das Datenschutzniveau.

428 Was aber ist von der engen Auslegung zu halten, wonach einzig Verstösse gegen Normen ausserhalb des DSG zur Verletzung des Rechtmässigkeitsprinzips führen, namentlich wenn diese den Individualrechtsschutz garantieren?[634] Rosenthal ist durchaus beizupflichten, wenn er eine Interpretation, die nicht nur Verstösse gegen bestimmte Vorgaben *ausserhalb* des DSG, sondern auch eine Interpretation, die *Verstösse gegen Vorgaben innerhalb des DSG* in den Rechtmässigkeitsgrundsatz inkludiert, im Lichte des Konzeptes des DSG problematisiert.[635]

429 Die unterschiedlichen Auslegungen – Inklusion oder Exklusion von Verstössen gegen weitere Vorgaben des Datenschutzgesetzes in das Rechtmässigkeitsgebot – beeinflussen das Datenschutzniveau im privaten Sektor: Werden Verstösse gegen datenschutzgesetzlich «interne» Regeln unter den Tatbestand von Art. 4 Abs. 1 DSG subsumiert, führt dies zum Ausbau der individualrechtlichen Position gemäss Art. 12 i. V. m. Art. 4 Abs. 1 DSG. Das Datensubjekt könnte konsequent Verstösse gegen datenschutzgesetzliche Vorgaben als Persönlichkeitsverletzung rügen, weil diese als Verstoss gegen das Rechtmässigkeitsprinzip über Art. 12 Abs. 2 lit. a DSG in die Annahme einer Persönlichkeitsverletzung münden würden. Auf Art. 11a DSG exemplarisch angewendet hiesse dies, dass die Nichtanmeldung einer Datensammlung als Verstoss gegen das Datenschutzgesetz vom Betroffenen über Art. 12 Abs. 1 i. V. m. Art. 4 Abs. 1 DSG gerügt werden könnte, dem Individuum mithin ein zivilrechtlicher Anspruch zukäme. Den Verstoss gegen die Registrierung über das Rechtmässigkeitsprinzip in den zivilrechtlichen Persönlichkeitsschutz einfliessen zu lassen, erscheint gut begründbar, zumal Betroffene von Gesetzes wegen ein Recht auf Auskunft gegenüber dem Betreiber einer Datensammlung haben, ob sie in dieser aufgeführt werden. Die Registrierung ist nahezu *conditio sine qua non* zur Realisierung der Betroffenenrechte. Verstösst der Betreiber einer Datensammlung gegen die Anmeldungspflicht, erschwert er zugleich das Recht der Betroffenen, eine entsprechende Auskunft zu

634 Rosenthal, HK-DSG, Art. 12 N 7; jüngst BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.

635 Ders., a. a. O., Art. 12 N 7 und N 11.

erhalten. So wird in doppelter Hinsicht gegen den Anspruch auf Transparenz verstossen, der eine tragende Säule datenschutzrechtlicher Normierungen ist: Weder die Kenntnis um die Existenz der Sammlung an sich noch die Kenntnis um die Erfassung des Individuums in der Sammlung wird gewährleistet. Folglich liesse sich vertreten, dass eine Verletzung der Anmeldepflicht gemäss Art. 11a DSG über Art. 12 Abs. 2 lit. a i. V. m. Art. 4 Abs. 1 DSG zu erfassen ist, womit ein zivilrechtlicher Anspruch des Individuums begründbar wird. Eine solche Interpretation des noch geltenden Rechts stünde in Einklang mit den jüngsten Rechtsentwicklungen. Zwar entfällt mit Totalrevision die Registrierungspflicht. Allerdings greift eine allgemeine Informationspflicht sowie eine Pflicht zur Erstellung eines Verarbeitungsverzeichnisses. Diese Pflichten bilden die Grundlage für die sowohl mit der DSGVO als auch mit der Totalrevision einhergehende Stärkung der Individualrechte, namentlich auch des Auskunftsrechts. Um Auskunftsrechte wirksam gewährleisten zu können, ist eine systematische Organisation der Informationen erforderlich.

Die hier vertretene Auslegung stärkt die *Transparenz*, was dem *Trend der jüngsten datenschutzrechtlichen Entwicklungen* entspricht.[636] In Anbetracht der Tatsache, dass die Registrierung von Datensammlungen ein Schlüsselelement für die Ausübung der Betroffenenrechte darstellt, scheint eine andere Auslegung, als dass deren Verletzung über den Rechtmässigkeitsgrundsatz oder direkt als Persönlichkeitsverletzung zu qualifizieren ist, nicht überzeugend.[637] Die Diskussion verliert mit der Totalrevision allerdings ihre Bedeutung. 430

Anzufügen bleibt, dass Verstösse gegen datenschutzgesetzliche Vorgaben, die nicht explizit in Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG aufgeführt werden, bereits aufgrund des nicht abschliessend formulierten Tatbestandes als persönlichkeitsverletzende Verarbeitungen qualifiziert werden können. Welche dies sind, bedarf der wertenden Auslegung. Der Umweg über das Rechtmässigkeitsprinzip wäre folglich überflüssig. Damit bestätigt sich, dass die *Kernbedeutung des Rechtmässigkeitsprinzips für den privaten Bereich* – anders als im öffentlichen Bereich – in der Vorgabe besteht, wonach auch *einschlägige Normen ausserhalb des DSG einzuhalten* sind. 431

636 Vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 6943 und 6972.

637 Man mag nun einwenden, dass ein Umweg über das Rechtmässigkeitsgebot und dessen Verletzung überflüssig wäre, könnte man doch den Verstoss gegen weitere datenschutzrechtliche Verstösse direkt über das «insbesondere» in Art. 12 Abs. 2 DSG einfliessen lassen; die Abstützung über Art. 4 Abs. 1 DSG wäre hierfür nicht erforderlich. Die Diskussion mag somit als überflüssig resp. sinnfrei erscheinen. Dennoch verdeutlicht die Inklusion von Verletzung weiterer datenschutzrechtlicher Pflichten und Vorgaben in das Rechtmässigkeitsprinzip die Geltungskraft datenschutzrechtlicher Regelung. Namentlich die datenschutzrechtlichen Vorgaben, die im Kontext mit der Absicherung des Transparenzgebotes verankert werden und dieses quasi flankieren, fliessen damit sichtbar in ihrer Gewichtung in die allgemeinen Bearbeitungsvorgaben ein.

432 In Erinnerung zu rufen bleibt, dass der Helsana+-Entscheid des Bundesverwaltungsgerichts eine *enge Auslegung zum Rechtmässigkeitsgebot* vertrat:[638] Das Gericht prüfte, ob die Datenbearbeitung der Beklagten im Rahmen des Programmes Helsana+, soweit es Personen betreffe, die nur eine Grundversicherung bei einer Versicherungsgesellschaft der Helsana-Gruppe haben, grundsätzlich unrechtmässig i. S. v. Art. 4 Abs. 1 DSG sei, da sie zu einem rechtswidrigen Zweck erfolge, nämlich eine indirekte Rückerstattung von Versicherungsprämien für die obligatorische Krankenversicherung ermögliche. Hierzu führte das Bundesverwaltungsgericht aus, dass Inhalt und Umfang des Rechtmässigkeitsgebotes nach Art. 4 Abs. 1 DSG umstritten seien. Unbestritten sei, dass Datenbearbeitungen immer dann unrechtmässig seien, wenn gegen eine Rechtsnorm verstossen werde, die den Schutz der Persönlichkeit bezwecke, unabhängig davon, ob sich die Rechtsnorm im DSG oder anderen Erlassen finde.[639] Ein Teil der Lehre beurteile eine Datenbearbeitung immer dann als unrechtmässig, wenn ein Verstoss gegen irgendeine Rechtsnorm vorliege.[640] Ein anderer Teil der Lehre will nur Verstösse gegen solche Verhaltensnormen, die direkt oder indirekt auch den Schutz vor einem Eingriff in die Persönlichkeit bezwecken, unter den Tatbestand subsumieren.[641] Niemand vertrete explizit, dass ein rechtswidriger Zweck der Datenbearbeitung in jedem Fall zur Unrechtmässigkeit der fraglichen Datenbearbeitung führe; alle Lehrmeinungen stellten vielmehr darauf ab, dass die Datenbearbeitung an sich gegen keine Rechtsnorm verstossen dürfe. Art. 4 Abs. 1 DSG beziehe sich, so führt das Bundesverwaltungsgericht fort, im Wortlaut auf die Rechtmässigkeit der Bearbeitung.[642]

433 Nach Ansicht der Autorin wird mit dieser Rechtsprechung der Aspekt der *Akzessorietät datenschutzrechtlicher Vorgaben, ein Terminus, wie er im historischen Teil entwickelt wurde,* übersehen.[643] Das DSG, so fährt das Gericht fort, äussere sich nicht dazu, zu welchen Zwecken Personendaten erhoben werden dürfen.[644] Es verlange nur, dass der Verarbeitungszweck bei der Beschaffung nach den Umständen erkennbar sei, dabei auch auf die Zweckbindung verwiesen werde. Alsdann findet eine Rechtsvergleichung statt, wobei die Differenz des DSG gegenüber der DSGVO herausgestellt wird: Art. 5 Abs. 1 DSGVO sage, anders als das DSG, dass Personendatenverarbeitungen nur für legitime Zwecke verfolgt wer-

638 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.4.
639 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.2.
640 Die Autorin schliesst sich dieser Auffassung an.
641 Die Auslegung vermag im Lichte der Erkenntnisse dieser Schrift nicht zu überzeugen, muss doch als ratio und Ziel und Zweck des Datenschutzrechts auch der Schutz von bereichsspezifisch definierten Schutzzwecken und Zielen sein.
642 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3.
643 Erster Teil, I. Kapitel.
644 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3., was kritisch beurteilt wurde. Zudem ist im Versicherungskontext auf die Spezialgesetze hinzuweisen, welche die systemische Schutzdimension des Datenschutzrechts dokumentieren und erfüllen.

den dürfen.[645] Mit der Totalrevision des DSG plane man indes keine Anpassung. Zudem führe eine teleologische Betrachtung von Art. 4 Abs. 1 DSG zu dem Schluss, dass das DSG dem Schutz der Persönlichkeit diene. Die allgemeine Zweckrichtung aller Datenschutzvorschriften lege nahe, dass sich das Rechtmässigkeitsprinzip nur darauf beziehe, dass Personendatenverarbeitung gegen Normen verstosse, die dem Schutz der Persönlichkeit dienen. Im Ergebnis hält das Bundesverwaltungsgericht fest, dass der Grundsatz der Rechtmässigkeit gemäss Art. 4 Abs. 1 DSG so zu verstehen sei, dass eine Datenbearbeitung zu einem rechtswidrigen Zweck erst dann unrechtmässig sei, wenn dabei gegen eine Norm verstossen wird, die zumindest auch, direkt oder indirekt, dem Schutz der Persönlichkeit dient.[646]

Eine solche Auslegung greift nach hier vertretener Ansicht zu kurz. Sie bindet das 434
Datenschutzrecht auf den Subjekt- und Persönlichkeitsschutz zurück. Die Vorgabe, dass eine unrechtmässige Datenverarbeitung nur dann vorliege, wenn gegen eine Norm verstossen werde, die dem Persönlichkeitsschutz diene, übersieht die Relevanz des Systemschutzes im Datenschutzrecht.[647]

Zusammenfassend präsentiert sich das Rechtmässigkeitsprinzip im Datenschutz 435
nach der hier vertretenen Ansicht als weit mehr denn ein Instrument der Selbstbeschwörung und -bestätigung des Rechts. Die Analyse des Rechtmässigkeitsprinzips macht es möglich, die Gesamtlandschaft des (Datenschutz-)Rechts wie auch den hohen Ausdifferenzierungsgrad des Schweizer Datenschutzrechts in den Blick zu nehmen. Aus funktionaler Sicht zeigt es namentlich eine *Anknüpfungs- resp. Ankoppelungsfunktion*, die mit einer *Differenzierungsfunktion* einhergeht. Die Qualifizierung des DSG als Querschnittsgesetz ist zwar nicht falsch, sie vermag indes nicht abzubilden, dass sich über das Rechtmässigkeitsprinzip eine *differenzierte und komplexe datenschutzrechtliche Landschaft* erschliesst. Drei Richtungen wurden insofern systematisiert: *Erstens* diejenige «nach aussen», also die Einbettung des DSG in die gesamte Rechtsordnung resp. Integration von Normen ausserhalb des DSG in dieses, *zweitens* jene «nach innen», also die Referenz auf den datenschutzgesetzlichen Ausgangspunkt der Personendatenverarbeitung (Grundsatz des prinzipiellen Verarbeitungsverbots) und insb. das Legalitätsprinzip resp. die prinzipielle Verarbeitungsfreiheit für den privaten Be-

645 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3.; m. E. hätte man hier in einer systematischen Interpretation und einer europarechtskompatiblen Auslegung auch in der Schweiz die systemische Datenschutzdimension inkludieren können – vertiefend zu diesem Ansatz dritter Teil, IX. Kapitel.

646 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3.

647 Eine systemtheoretische Analyse des Datenschutzrechts mit einer präzisierten Darstellung der modernen Systemtheorie und ihrer Kritiker findet sich bei Donos, 21 ff.; die vorliegende Arbeit beschreibt das Recht auf informationellen Systemschutz in erster Linie als Paradigma, welches das Recht auf informationellen Subjektschutz als individualistisches Privatheitsparadigma wenn auch nicht ersetzt, so doch ergänzt.

reich, und *drittens* geht es innerhalb des Datenschutzgesetzes für den privaten Sektor um dessen Koordinierung mit dem persönlichkeitsrechtlichen System und den Kategorien der Persönlichkeitsverletzung, der Widerrechtlichkeit sowie der Rechtfertigungsgründe. Folglich greift es zu kurz, den Ansatz des Schweizer Datenschutzrechts isoliert anhand des DSG als «Omnibus»-Ansatz zu qualifizieren. Mit und über das Rechtmässigkeitsprinzip wird in der Schweiz ein *differenziertes und abgestuftes Datenschutzregime abgebildet und implementiert, das sich harmonisch in die gesamte Rechtsordnung mit ihren für die jeweiligen Bereiche etablierten Leitprinzipien einfügt*.

2. Treu und Glauben

2.1. Grundlagen

436 Getreu der Redewendung «Nützt es nicht, so schadet es auch nicht» liess sich der bei der Schweizer Datenschutzgesetzgebung federführende Pedrazzini mit den Worten vernehmen: «Treu und Glauben sei immer recht am Platze».[648] Etwas anders gestaltet sich die Einschätzung von Druey, demzufolge Treu und Glauben für das Informationsrecht eine ungleich höhere Bedeutung zukomme als für andere Gebiete.[649] Die Zitate zweier Schweizer Experten für den Bereich des Informationsrechts liefern im Verbund ein ambivalentes Bild zur Bedeutung des Prinzips im Datenschutzrecht: Für den einen Verlegenheitslösung weist der andere dem Grundsatz dagegen besonderes Gewicht im Informationskontext zu. Die nachfolgenden Ausführungen gehen der Bedeutung von Treu und Glauben für das Datenschutzrecht auf den Grund.[650] Dabei wird eine Erkenntnis, die aus den Erörterungen zum Rechtmässigkeitsprinzip gewonnen wurde, nutzbar gemacht. Demnach vermag namentlich eine systematische und eingebettete Betrachtungsweise produktive Erkenntnisse zu generieren.

437 Treu und Glauben ist fester Bestandteil der allgemeinen datenschutzrechtlichen Verarbeitungsgrundsätze, vgl. Art. 4 Abs. 2 1. Satzteil DSG, vgl. auch Art. 6 Abs. 2 erster Teil nDSG und Art. 5 Abs. 1 lit. a DSGVO. Gerade *weil* die generalklauselartigen Bearbeitungsgrundsätze und damit Treu und Glauben im privaten Sektor gemäss DSG *die wichtigsten Schranken der grundsätzlich freien Bearbeitung definieren*, kommt der Aufgabe, diesen konkretisierte Handlungsanleitungen zu verleihen, besondere Relevanz zu.

---

648 Pedrazzini, in: Schweizer (Hrsg.), 19 ff., 26.
649 Druey, 315.
650 Zu Vertrauen und Glaubwürdigkeit im Zeitalter des Internets Müller, NZZ am Sonntag vom 4. Februar 2018, 20 f.; zu Vertrauen (und Risiko) als zentralen Elementen modernen Zusammenlebens Hotter, 74 ff.; zum Vertrauen durch das Recht Druey, Rechtswissenschaftliche Abteilung der Universität St. Gallen (Hrsg.), 525 ff.

Für das Datenschutzrecht prägt die *Abgrenzung* von Treu und Glauben gegenüber anderen Verarbeitungsgrundsätzen die Debatte zum Verarbeitungsgrundsatz: Wie gezeigt, wurde gesetzgeberisch eine vorab geplante gemeinschaftliche Normierung des Gebotes der Rechtmässigkeit mit demjenigen von Treu und Glauben in einem Absatz aufgegeben und Letzteres in eine vereinte Regelung mit dem Verhältnismässigkeitsgrundsatz in einen Absatz transferiert. Diese Systematik wird mit der Totalrevision und Art. 5 Abs. 2 nDSG beibehalten. Die folgenden Reflexionen werden indes den *eigenständigen Gehalt sowie spezifische Funktionen von Treu und Glauben, aber auch Schwächen für das Informations- und namentlich das Datenschutzrecht* vor Augen führen. Hierzu beginnt die Untersuchung mit allgemeineren methodischen Erwägungen zu den Generalklauseln und dem traditionsreichen Grundsatz. Nach dieser Betrachtung von Treu und Glauben auf abstraktester Ebene wird der Fokus verengt auf Treu und Glauben im Datenschutzrecht. Anschliessend wird analysiert, welche Impulse der Grundsatz dem Datenschutzrecht verliehen hat, aber auch, welche Defizite ihm eigen sind. 438

Bedeutsame Themen sind bei der Konkretisierung von Treu und Glauben die *culpa in contrahendo*, die Vertrauenshaftung und damit die Begründung vorvertraglicher Informationspflichten, die Inhaltskontrolle bei AGB sowie der Vertrag mit Schutzwirkung zugunsten Dritter.[651] Zudem kommt Treu und Glauben eine wichtige Funktion bei der *Interpretation* von Gesetzen, Verträgen und allgemeinen Willenserklärungen zu.[652] Entsprechend spielt *Treu und Glauben seit jeher eine zentrale Rolle im Zusammenhang mit informationsrechtlichen Fragen und Ansprüchen*. 439

Der Appell an *ein faires, loyales, vertrauenswürdiges, verlässliches, nachvollziehbares, redliches Verhalten* hat im Kontext von Information und Kommunikation einen prominenten Stellenwert.[653] Das Recht wird im Umgang mit Information, Kommunikation und Beziehungen mit ganz eigenen Herausforderungen konfrontiert.[654] Allgemein haben Informationen und deren Verarbeitung eine eigene Wirkungsmacht und -logik; Verstösse gegen informationelle Normen und Erwartungen sind schwieriger zu handhaben als beispielsweise der unrechtmässige Umgang mit einer Sache, einem körperlichen Gegenstand. Lassen sich «treuwidrige» Verhaltensweisen im Rahmen der Erfüllung eines Sachkaufes oder einer 440

651 Vgl. BGE 125 III 86, E 3.c.; BGE 121 III 350; BGE 116 II 431, E 3; vertiefend Kuonen, *passim*; BGE 140 III 200, E 5.2.: vgl. Honsell, BSK-ZGB, Art. 2 N 14 ff.; Auer, Materialisierung, 122; Druey, 525 ff.; kritisch zur Idee, wonach Information und Transparenz per se Vertrauen sowie Werte schaffen, Druey, in: Kramer/Nobel/Waldburger, 589 ff., 592 ff.; zur Vertrauenshaftung Bucher, in: Forstmoser/Honsell/Wiegand (Hrsg.), 231 ff.

652 Vgl. Druey, 232 ff., 155, 313 ff.; zu Art. 2 ZGB als rechtsdogmatischem Ansatz eines Vertraulichkeitsschutzes Häusermann, 107 ff.; Steinauer, 165 ff. und insb. 185 ff.; Tuor/Schnyder/Schmid/Jungo, 47 ff.; zur Confidentiality Harvey, U. Pa. L. Rev. 1992, 2385 ff.

653 Illustrativ insofern der Beitrag von Fried, Yale L.J. 1968, 475 ff.; Boll, 2.

654 Grundlegend hierzu namentlich Zech, *passim*.

Miete auf der «Sachebene» meist ausgleichen, steht eine entsprechend wirksame Mechanik im Umgang mit Information gerade nicht zur Verfügung. Bereits der Volksmund bringt die informationellen Besonderheiten mit Redewendungen wie «Es bleibt immer etwas hängen» oder «Ist der Ruf mal ruiniert, lebt es sich ganz ungeniert» eingänglich zum Ausdruck.

441 Entsprechend hat das Recht seit Längerem versucht, spezifische Instrumente zu schaffen: Im Kontext des Medienrechts ist vor diesem Hintergrund die Ausübung des Rechts auf Gegendarstellung, Art. 28g ff. ZGB von Bedeutung. Das Recht auf Gegendarstellung ermöglicht es dem Betroffenen, auf Tatsachendarstellungen in periodisch erscheinenden Medien, die ihn in einem schlechten Licht dastehen lassen, zu reagieren, vorab ohne behördliche Intervention. Ziel des Instruments der Gegendarstellung ist die Verwirklichung des Prinzips der «gleich langen Spiesse» im Medienkontext. Der Gesetzgeber hat insofern ein eigenes Rechtsinstrumentarium geschaffen, um eine «faire», «korrekte» Medienberichterstattung abzusichern und das Konzept von «audiatur et altera pars» auch unter Privaten wirksam werden zu lassen. Das Rechtsinstitut ist damit von Treu und Glauben mitinspiriert. Immerhin: Mit der Geltendmachung des Gegendarstellungsrechts wird allenfalls eine unliebsame Angelegenheit erneut in Erinnerung gerufen, was nicht immer von Vorteil ist. Erfolgte Informationsflüsse lassen sich nicht beliebig rückgängig machen.

442 Treu und Glauben ist untrennbar mit *Vertrauen* verbunden: Vertrauen wiederum bildet eine Grundbedingung zwischenmenschlicher Beziehungen. Beziehungen leben zu einem wesentlichen Teil von Kommunikation und Informationsaustausch. An dieser Stelle sei an das im ersten Teil dargestellte Arztgeheimnis erinnert, wobei die traditionsreichen Geheimhaltungspflichten als die frühesten «datenschutzrechtlichen» Instrumente beschrieben wurden. Das Arztgeheimnis schützt, wenn auch nicht ausschliesslich und isoliert, das *Vertrauensverhältnis* zwischen behandelnder Ärztin und Patienten.[655]

443 Heute gelten das Reputationsrisiko und der Vertrauensverlust aufgrund einer *medialen Berichterstattung* über Compliance-Verstösse und damit ebenso Datenschutzverstösse als Kernherausforderung.[656] In digitalen Netzwerken verbreiten sich entsprechende Informationen schnell und weit. Ein datenschutzrechtskonformer Umgang ist damit nicht nur unter Berücksichtigung von drohenden behördlichen Sanktionen oder zivilrechtlichen Klagen geboten, sondern ebenso wegen potentieller Vertrauensverluste, welche eine «negative Presse» bringen können.

655 Vgl. BGE 117 Ia 341, E 6.a. sowie BGE 87 IV 105, E 2.b.

656 Hierzu Vesting, in: Ladeur (Hrsg.), 155 ff., 182; dazu, dass auch die verschärften Sanktionen gemäss DSGVO ein beträchtliches Reputationsrisiko darstellen, Räther, ZHR 2019, 94 ff., 95 f.; vertiefend dritter Teil, VII. Kapitel, A.3.

Der kurze Abriss redet somit dem eingangs zitierten Druey das Wort: Treu und Glauben hat in Anbetracht der Bedeutung von Information und Kommunikation für soziale Beziehungen sowie der «Eigenarten» von Information als Schutzgegenstand in seiner *präventiven Rolle im Sinne von Handlungsanleitungen an das faire, redliche, korrekte Informations- und Kommunikationsverhalten besondere Relevanz*. Die *retrospektive Korrektur* und Kompensation von Verstössen gegen Informationserwartungen bleibt hingegen gerade aufgrund der «Natur» personenbezogener Daten, die «nicht-rivalisierend» sind sowie fluid, oft unmöglich.[657] Über den Grundsatz wird damit eine Erkenntnis transportiert, wonach der Umgang mit Information ebenso auf normativer Ebene spezifischen Logiken, Erwartungen und Enttäuschungen unterliegt. 444

Bevor auf Treu und Glauben in seiner *spezifischen Bedeutung als datenschutzrechtlicher Verarbeitungsgrundsatz* eingegangen wird, dient ein kurzer Überblick über die Theorien der Generalklauseln sowie Treu und Glauben der Bereitung des Bodens. 445

Die rechtswissenschaftlichen Studien zu den Generalklauseln für das Privat- und Verfassungsrecht im Allgemeinen und zu den «Obergeneralklauseln» wie Treu und Glauben sowie den guten Sitten im Besonderen füllen Bibliotheken. Hierbei wird versucht, die unbestimmten Rechtsbegriffe zu qualifizieren und zu systematisieren, zudem werden diese anhand ihrer jeweiligen Funktionen erörtert. Die Kernbestrebungen richten sich indes auf die jeweiligen inhaltlichen Konkretisierungen der einzelnen unbestimmten Rechtsbegriffe. Eine Sichtung der Literatur zu Treu und Glauben sowie anderen Generalklauseln führt zunächst eine breit angelegte Diskussion zur *Definierung von Generalklauseln selbst* zu Tage. 446

Die *Einheitstheorien* wollen die Generalklauseln anhand *eines einzelnen Kriteriums* einfangen, wobei allerdings das einschlägige Kriterium in den verschiedenen Beiträgen variiert.[658] In den sog. *Verbindungstheorien* werden *mehrere Definitionskriterien* (Generalklauseln als wertungsbedürftiger Tatbestand, als unbestimmte, abstrakte oder allgemeine Rechtsbegriffe, als Normbildungsauftrag an die Gerichte) kombiniert.[659] Eine teilweise neue Systematisierung und Interpretation zu den Generalklauseln legt Auer vor. Sie präsentiert *drei Grundwidersprüche in der Privatrechtsordnung*: erstens den materiellen zwischen Individualismus und Kollektivismus, zweitens den formalen zwischen Rechtssicherheit und Einzelfallgerechtigkeit und drittens den institutionellen zwischen Richterbindung 447

657 Ähnlich sowie zur Fluidität von Daten Flückiger, AJP 2013, 837 ff., 838 f.; zur Nichtrivalität von Daten insb. Zech/Hürlimann, sui-generis 2016, 89 ff., 90.

658 Vgl. Hellwege/Soniewicka, 8.

659 Vgl. vertiefend hierzu Teubner, Direktiven, 118; Auer, Materialisierung, 127 ff.; Röthel, in: Riesenhuber (Hrsg.), 225 ff.

und Richterfreiheit.[660] Generalklauseln wirken gemäss der Autorin als *Äquilibriums-Instrument,* als Puffer resp. bewegliche Zonen im statischen Gebäude, um der Beurteilung und Austarierung ebendieser Dichotomien Raum zu verschaffen. Die Qualifizierung als Generalklausel erfolgt dann, wenn ein offener oder unbestimmter Rechtsbegriff die *Funktion des Wertungsausgleichs* innerhalb der drei Grundwidersprüche wahrnimmt.[661]

448 Eine *Metapher*, die mit Generalklauseln und damit für Treu und Glauben auftaucht, ist das *Einfallstor.*[662] Generalklauseln öffnen das Recht gegenüber ausserrechtlichen Normen und Entwicklungen; so könne beispielsweise die gute Sitte als Verweis auf tatsächlich geltende Sitten und Gebräuche, also empirisch feststellbare soziale Normen, interpretiert werden.[663] Generalklauseln gelten als Öffnungsklauseln für Anpassungen an sich wandelnde Lebensverhältnisse.[664]

449 Neben Definitionsversuchen der Generalklauseln selbst steht im Zentrum der Auseinandersetzungen mit ihnen deren *Konkretisierung*. Als Kernherausforderung und -aufgabe gilt die Rationalisierung der Methode, um griffige Inhalte sowie standardisierte Funktionen zu umschreiben. Insofern wurden mehrere Ansätze entwickelt.[665] Die *Funktionstheorie* mit Wiackers rechtstheoretischer Präzisierung zu Treu und Glauben lautet «*iuris civilis invandi, supplendi, corrigendi gratia*».[666] Es sind damit mehrere Funktionen, die Treu und Glauben wahrnimmt, namentlich die *interpretative Funktion* für Rechtsgeschäfte und Erlasse (wobei Treu und Glauben im Rahmen der Interpretation von AGB eine besondere Bedeutung erlangt hat), die *ergänzende Funktion* für Rechtsgeschäfte und Erlasse (womit sich Treu und Glauben oft in der Zone der Auslegungsfragen bewegt) sowie die *anpassende resp. korrigierende und auflösende Funktion*.[667]

450 Weiter soll «Ordnung und Rechtssicherheit» generiert werden: Konkretisierte Anwendungsfälle von Treu und Glauben resp. des Rechtsmissbrauchs werden anhand von *Fallgruppen* systematisiert.[668] Die Zuweisung gewisser Tatbestände zu Art. 2 Abs. 1 resp. zu Abs. 2 ZGB wird allerdings teilweise kontrovers disku-

660 Auer, Materialisierung, 98.
661 Dies., a. a. O., 142.
662 Vgl. BverfG, Beschluss der 2. Kammer des Ersten Senats vom 14. September 2010 – 1 BvR 1504/10, E 13.
663 Vgl. hierzu Teubner, 29 ff., 61, 65 ff.; Walter, in: Ehrenzeller/Gomez/Kotzur/Thürer/Vallender (Hrsg.), 127 ff., 133 f.; BverfG, Beschluss der 2. Kammer des Ersten Senats vom 14. September 2010 – 1 BvR 1504/10, E 13.
664 Auer, Materialisierung, 55.
665 Dies., a. a. O., 144 ff.
666 Wiacker, zit. nach Auer, Materialisierung, 163.
667 M. w. H. auf die einschlägigen Quellen Pfaffinger, KuKo-ZGB, Art. 2 N 2 und N 7.
668 Vgl. Riemer, § 5 N 13; Hürlimann-Kaup/Schmid, N 266.

tiert.[669] Als Konsequenz wird Art. 2 ZGB denn auch als Gesamtkonzept für einen *allgemeinen Vertrauensschutz* dargestellt.[670]

451 Konkretisiert formuliert Treu und Glauben – das Bundesgericht spricht von einer Grundschutznorm[671] – einen allgemeinen, übergeordneten (objektiven) Massstab,[672] wobei die *gegenseitige Rücksichtnahme* im Rahmen der Ausübung resp. Achtung gesetzlicher wie rechtsgeschäftlicher Pflichten und Rechte verlangt wird. Treu und Glauben gebietet und schützt *loyales, redliches, korrektes Verhalten, das gegenseitige Vertrauen- und Glauben-Dürfen, die Fairness im Rechtsverkehr*.[673] Seit jeher und an erster Stelle wird Treu und Glauben als *Auffangklausel* beschrieben.[674] Treu und Glauben wurde und wird dort angerufen, wo positivierte Regeln und Grundsätze einen Sachverhalt nicht oder nicht befriedigend erfassen. Hat sich alsdann eine Praxis konsolidiert, werden nicht selten die vonseiten der Praxis und Wissenschaft über die Wendung von Treu und Glauben anerkannten Ansprüche vom Gesetzgeber rezipiert und in eigenständige Normen überführt.

452 Ebendiese Konstruktionen und Charakterisierungen spielen nachfolgend eine Rolle beim Unterfangen, die *spezifisch datenschutzrechtliche Bedeutung von Treu und Glauben* zu durchdringen. Hierfür wird vorab auf die Verortung von Treu und Glauben in den datenschutzrechtlichen Texten eingegangen. Kombiniert mit einer Analyse zu den jüngsten datenschutzrechtlichen Entwicklungen lassen sich (Entwicklungs-)Linien nachzeichnen, die massgeblich von Treu und Glauben geprägt wurden. Jeglicher Kritik zum Trotz gegenüber Treu und Glauben als «Leerformel» präsentiert sich diese vielmehr als «Lehrformel» und «Einfallstor» in einem produktiven Sinne für die Weiterentwicklung des Datenschutzrechts. Den nachfolgenden Ausführungen zu «Treu und Glauben» mit Fokus auf *seine spezifische informationelle Bedeutung* ist vorauszuschicken, dass die Gültigkeit von Treu und Glauben im Datenbearbeitungskontext selbst ohne seine explizite Verankerung in Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG sowohl für den privaten als auch für den öffentlichen Datenbearbeitungssektor gewährleistet wäre. Als Generalklausel durchdringt Treu und Glauben die gesamte Schweizer Rechtsordnung, vgl. Art. 2 Abs. 1 ZGB sowie Art. 4 aBV, Art. 9 BV und Art. 5 Abs. 3 BV. Vergleichbar zum Rechtmässigkeitsprinzip rezipiert das Schweizer Datenschutzgesetz mit Art. 4 Abs. 2 erster Satzteil DSG resp. Art. 6 Abs. 2 erster Satzteil nDSG ein allgemeines und fundamentales Rechtsprinzip und importiert

669 M. w. H. Pfaffinger, KuKo-ZGB, Art. 2 N 2.
670 So Schwander, OFK-ZGB, Art. 2 N 2; vgl. zum Zusammenspiel zwischen Vertrauen und Recht Druey, Rechtswissenschaftliche Abteilung der Universität St. Gallen (Hrsg.), 525 ff.
671 BGE 125 III 261.
672 Riemer, § 5 N 2.
673 Hierzu Ders., § 5 N 2.
674 M. w. H. Ders., § 5 N 4.

es in das Datenschutzrecht. Mit dieser Einschreibung von Treu und Glauben ins Datenschutzgesetz macht sich ebenso dessen «didaktischer Wert» bemerkbar.[675] Das DSG bringt mit der «Leerformel» (und Lehrformel) von Treu und Glauben als allgemeinem Verarbeitungsgrundsatz zum Ausdruck, dass *loyales Gebaren auch im Rahmen von Datenverarbeitungen initial handlungsanleitend* ist.

453 Die «Zählebigkeit»[676] und Breitenwirkung der Generalklauseln, die selbst in die Felder und Zeiten der Digitalisierung übergreifen, hat ebenso einen «psychologischen Effekt» – Teubner hat ihn exemplarisch für die guten Sitten, mit Referenz auf Topitsch, wie folgt umschrieben: Man suggeriere zum einen Konstanz von höchsten moralisch-politischen Prinzipien, zum anderen schaffe man eine «kollektive Wertungseinheit», vereine Gefühl und Verstand, Rationalistinnen und Irrationalisten.[677] Dieser integrative und beruhigende Effekt ist *a fortiori* für ein Rechtsgebiet willkommen, das sich mit dem «rasanten technischen Fortschritt» und hierbei mit künstlicher Intelligenz, Algorithmen, Minichips, Clouds sowie hoher gesellschaftlicher Ambivalenz, Freud und Leid, Chancen und Risiken dieser neuen Technologien konfrontiert sieht.[678]

2.2. Datenschutzrechtliche Bedeutung

2.2.1. Positivierungen

454 Dem Grundsatz Treu und Glauben kommt seit jeher ein fester Platz in der Datenschutzregulierung zu.[679] In der DSGVO findet er sich in Art. 5 Abs. 1 lit. a mit den Worten:

> «Personenbezogene Daten müssen auf rechtmässige Weise und nach Treu und Glauben und in einer für die betroffenen Personen nachvollziehbaren Weise verarbeitet werden.»

455 In der Schweiz wurde in den 1980er Jahren intensiv über den rechten Ort des Grundsatzes im ersten eidgenössischen Datenschutzgesetz verhandelt, nicht ohne inhaltliche Zuweisungen daran zu koppeln (Stichwort «Relevanz der Systematik für die Auslegung von Gesetzen»): Im ersten Bundesratsentwurf von Art. 4 Abs. 1 ging Treu und Glauben, wie erwähnt, Hand in Hand mit dem Rechtmässigkeitsgebot:

675 Zum Begriff Meier, N 630 und N 647.
676 Teubner, 22.
677 M. w. H. Ders., a. a. O.
678 Vgl. z. B. mit Blick auf das Cloud Computing Cavoukian, digma 2009, 20 ff., 21 ff.
679 Vgl. vor den gesetzgeberischen Anpassungen, die im Zuge der DSGVO erfolgten, z. B. § 6 Abs. 1 Ziff. 1 des Österreichischen Datenschutzgesetzes sowie die französische Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Version consolidée au 27 septembre 2016, wonach Art. 6 Abs. 1 lautete: «Les données sont collectées et traitées de manière loyale et licite».

> «Personendaten dürfen nur *mit rechtmässigen Mitteln und nicht wider Treu und Glauben* [Hervorhebung durch die Autorin] beschafft werden.»[680]

456 In Kraft gesetzt wurde am 1. Juli 1993 Art. 4 Abs. 2 DSG, der betreffs Personendaten vorschreibt:

> «Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.»

457 An Art. 4 Abs. 2 DSG selbst, welcher den Grundsatz von Treu und Glauben mit demjenigen der Verhältnismässigkeit vereint, wurde seit Inkrafttreten des DSG nichts geändert. An derselben Formulierung und Kombinierung mit dem Verhältnismässigkeitsprinzip wird abgesehen von einer minimalen sprachlichen Vereinfachung mit der Totalrevision festgehalten, vgl. Art. 6 Abs. 2 nDSG. Die Totalrevision führt indes mehrere neue Instrumente ein, deren Entwicklung in Treu und Glauben festzumachen sind. In ihrem Zentrum steht der *Ausbau spezifischer Informationsvorgaben und entsprechend der Transparenz*.[681] Ein Prozess der Ausdifferenzierung und Fortentwicklung datenschutzrechtlicher Vorgaben über Treu und Glauben lässt sich keineswegs erst im Zuge der jüngsten Entwicklungen im Zuge der Totalrevision nachzeichnen. Explizite Anerkennungen von eigenständigen *Transparenzvorgaben* gelten als Ableitungen von Treu und Glauben.[682] Vor Teilrevision des DSG 2008 und der Stärkung der Transparenzerfordernisse galt, wie erwähnt, eine *heimliche* Beschaffung von Daten oder eine solche unter Angabe einer falschen Identität oder eines falschen Zwecks als Verstoss gegen Treu und Glauben.[683]

458 Damit hat Treu und Glauben bislang im Kontext des Datenschutzes eine *Anstoss-* und damit *Rechtsfortbildungsfunktion* für die gesetzgeberische Konkretisierung, Ausdifferenzierung, Fortentwicklung und Spezifikation datenschutzgesetzlicher Rechte und Pflichten wahrgenommen. Einige der in der Schweiz (noch) über den Phraseologismus abgehandelten Vorgaben wurden in Deutschland, wo Hessen als erstes Bundesland früh ein eigenes Datenschutzgesetz verabschiedete und der Bund schon 1977 sein erstes Bundesdatenschutzgesetz erliess, bereits gesetzgeberisch spezifisch normiert. Augenfällig war allerdings, dass Treu und Glauben in seiner «abstrakten» Gestalt im Deutschen Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 nicht verankert war. Auf den ersten Blick erstaunt dies für ein Land, das als «Schrittmacher» für die

680 Vgl. BBl 1988 II 414 ff., 460 und 517.

681 Zum Ausbau der Transparenzvorgaben Botschaft DSG 2017–1084, 17.059, 6941 ff., 6972 ff.; Baeriswyl, digma 2020, 6 ff., 6.

682 Vgl. Art. 4 Abs. 4 DSG, Erkennbarkeit der Beschaffung und Erkennbarkeit des Zweckes, später Art. 7a DSG, inzwischen wieder aufgehoben; BBl 1988 II 414 ff., 449; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8; Rosenthal, HK-DSG, Art. 4 N 14; Meier, N 649.

683 Wiederum zeigt sich an dieser Stelle die Schwierigkeit der Abgrenzung zu Art. 4 Abs. 1 DSG, zumal die Beschaffung unter falschen Angaben gleichermassen als Täuschung und damit unrechtmässige Datenbeschaffung gemäss Art. 4 Abs. 1 DSG zu beurteilen ist.

Entwicklungen und Fortschritte im Datenschutzrecht gilt, wenn Treu und Glauben als Impulsgeber für die datenschutzrechtliche Weiterentwicklung und hierbei insb. für den Ausbau von Transparenzvorgaben verstanden wird. Der Verzicht ist erklärbar: Vorab beansprucht der Grundsatz in Deutschland bereits aufgrund allgemeiner Bestimmungen ausserhalb des DSG ebenso für das Datenschutzrecht Gültigkeit. Weitere spezifische Vorgaben sind als Konkretisierungen von Treu und Glauben zu lesen, so insb. der Grundsatz der *Direkterhebung*. Im Bundesdatenschutzgesetz vom 30. Juni 2017 findet sich der Grundsatz neu ausdrücklich in § 47 Ziff. 1 BDSG verankert, womit die Vorgabe gemäss Art. 5 Abs. 1 lit. a DSGVO rezipiert wird.

459 Für die Schweiz belegt sich die explizite Voranstellung von Treu und Glauben als allgemeiner Verarbeitungsgrundsatz gerade für den privaten Sektor als sinnvoll. Erst die «treuwidrige», also die qualifizierte Datenverarbeitung, wird im privatrechtlichen Bereich mit einer «roten Flagge» versehen.[684] Seit jeher haben Treu und Glauben, vgl. auch Art. 2 Abs. 1 ZGB, und namentlich das Verbot des Rechtsmissbrauchs, vgl. Art. 2 Abs. 2 ZGB, die Funktion, an den *äussersten Rändern* «Schranken» zu setzen. Interveniert wird bei «krass stossenden Verhaltensweisen oder Ergebnissen».[685] Gerade in Bezug auf die datenschutzgesetzliche Normierung für den privaten Bereich, die vom Grundsatz der freien Verarbeitung mit Schranken ausgeht und an der qualifizierten Verarbeitungshandlung ansetzt, ist es entsprechend gesetzgeberisch angezeigt, die Datenbearbeitenden eingangs an diese «äussersten Schranken» zu erinnern. Dagegen kommt Treu und Glauben in einem Datenschutzrecht, in dem der Grundsatz des Verarbeitungsverbotes mit Erlaubnistatbeständen implementiert ist und das zudem eine längere zeitliche Konsolidierungs- und Ausdifferenzierungsphase hinter sich hat, eine andere Rolle zu.

2.2.2. Rezeption in der Schweizer Lehre und Praxis

460 Wie wird Treu und Glauben in der datenschutzrechtlichen Lehre und Praxis der Schweiz rezipiert und inwieweit spiegelt sich der dem Prinzip im Informationskontext zugewiesene gewichtige Bedeutungsgehalt? Auf die zahlreichen Unklarheiten bzgl. der Bedeutung von Treu und Glauben im Datenbearbeitungskontext wird in der Doktrin hingewiesen: Hier wird die Frage aufgeworfen, ob der Grundsatz neben dem Zweckbindungs-, Verhältnismässigkeits-, aber auch Recht-

684 Zur Verwendung dieser Metapher im Datenschutzkontext Nissenbaum, 127 ff., 148 ff.; beachte sodann Art. 13 Abs. 2 BV, der – wenn auch nicht direkt auf den privaten Bereich anwendbar – den Schutz vor missbräuchlicher Datenverarbeitung und jedenfalls im Wortlaut gerade kein (Grund-)Recht auf informationelle Selbstbestimmung verbürgt; kritisch ebenso Gächter/Werder, in: Epiney/Fasnacht/Blaser (Hrsg.), 87 ff., 91 ff.

685 Vgl. Riemer, § 5 N 14; Bger 5A_304/2010 vom 27. August 2010, E 4.5.1.

mässigkeitsprinzip überhaupt eine eigene Bedeutung habe.[686] Umgekehrt wird der Grundsatz im datenschutzrechtlichen Kontext nicht nur von Meier als mehr denn ein didaktisches Lehrstück im Sinne eines ermahnenden Fingers taxiert.[687] Die Ausführungen zum Grundsatz von Art. 4 Abs. 2 DSG sind – trotz der *in abstracto* deklarierten hervorragenden Bedeutung von Treu und Glauben im Informationskontext – dennoch *punktuell* und stark *einzelfallbezogen*. Systemisch wird der Grundsatz – abgesehen von der Stärkung des Transparenzgebotes als tragende Säule zeitgenössischer Datenschutzregulierung – nicht fruchtbar gemacht.

461 Die erste Wortmeldung stammt vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeamten. Der EDÖB lässt zu Treu und Glauben verlautbaren:

> «Personendaten dürfen nicht ohne Wissen und gegen den Willen der betroffenen Person beschafft werden. Wer die betroffene Person bei der Datenbeschaffung absichtlich täuscht – z. B. wenn er die Daten unter Angabe einer falschen Identität beschafft oder falsche Angaben über den Zweck der Bearbeitung erteilt –, verletzt das Prinzip von Treu und Glauben. Dieses verletzt er auch, wenn er Personendaten verdeckt beschafft, beispielsweise durch Belauschen eines Gesprächs oder Abhören von Kommunikationsverbindungen.»[688]

462 Die Passage verleitet indes selbst eine redliche Leserschaft zu einer Fehlannahme betreffend die Bedeutung der Einwilligung des Datensubjektes: Nach Schweizer Datenschutzgesetz ist eine Bearbeitung selbst gegen den Willen des Datensubjektes zulässig, vgl. Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG, sofern hierfür ein Rechtfertigungsgrund vorliegt. Zugleich illustrieren die Erwägungen des EDÖB erneute Abgrenzungsschwierigkeiten zwischen den verschiedenen Bearbeitungsgrundsätzen und Verarbeitungsvorgaben, insb. dem Grundsatz der Erkennbarkeit sowie den sukzessive national wie international ausgebauten Transparenzgeboten.

463 Darüber hinaus rücken *zwei Rechtsfälle*, die den Umgang mit Personendaten betreffen, *Treu und Glauben in das Zentrum ihrer Argumentation*: zum einen der *Spamming-Entscheid* des Bundesverwaltungsgerichts, zum anderen die *Logistep-Entscheide* des Bundesverwaltungsgerichts und des Bundesgerichts. In ersterem wurde der Generalklausel Relevanz im Rahmen der *elektronischen Massenmedien* und der Bewerbung zugemessen. In seinem *Spamming-Entscheid* weist das Bundesverwaltungsgericht in E 5.5. auf die fundamentale Bedeutung von Treu und Glauben im Rechtsverkehr hin mit den Worten:

686 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8.
687 Meier, N 630 und N 647.
688 EDÖB, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/telekommunikation/telefonie/allgemeine-grundsaetze.html#886355380> (zuletzt besucht am 10. September 2021); Schlussbericht vom 1. Juni 2015 betreffend die Abklärung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB).

«Dieser Grundsatz […] gebietet ein loyales und vertrauenswürdiges Verhalten im Rechtsverkehr. Im Geschäftsverkehr hat Treu und Glauben eine herausragende Bedeutung. Das Gebot von Treu und Glauben im Geschäftsverkehr, welches wie das Rechtsmissbrauchsverbot eine Ausprägung des gleichen Grundsatzes ist, gehört zum Kreis der universell anerkannten Rechtsgüter, deren Schutz der positive „Ordre public" dient (BGE 128 III 207). Von einem loyalen und vertrauenswürdigen Verhalten im Geschäftsverkehr kann jedoch keine Rede sein, wenn eine an einer Geschäftsanbahnung interessierte Partei es in Kauf nimmt, zur Gewinnung einzelner Kunden systematisch eine Vielzahl von nicht einmal ansatzweise identifizierten Adressaten wahllos mit beliebiger Streuwerbung zu bedienen. Dies gilt erst recht, wenn dieser Vielzahl von Empfängern in voraussehbarer Weise gänzlich nutzlose Auslagen und Umtriebe anfallen, wie dies vorliegend der Fall ist. Insbesondere darf nicht vermutet werden, dass eine Person ihre E-Mail-Adresse bekannt gibt, damit ihr jeder beliebige Anbieter im World Wide Web seine Angebote für die Anbahnung von Geschäftsbeziehungen unterbreiten kann. Der Grundsatz von Treu und Glauben greift schon im vorvertraglichen Bereich. Daher hat die an einer Geschäftsanbahnung interessierte Partei die Privatsphäre und die Interessen des anderen zu respektieren. Dazu gehört, dass der Geschäftswillige nicht ungefragt und systematisch massenhaft nutzlose Auslagen und Umtriebe bei Dritten verursacht. Bei wahlloser Streuwerbung an nicht identifizierte Dritte ist zu beachten, dass der Anbieter nur über vage bzw. ganz und gar zufällige Aussichten auf eine Geschäftsmöglichkeit verfügt, wenn er seine Werbung an Personen und Unternehmen adressiert, von denen er nicht einmal im Ansatz weiss, um wen es sich dabei handelt und welche Interessenlage bei diesen herrscht. Es verstösst somit gegen Treu und Glauben, wenn ein an Geschäftsanbahnung Interessierter systematisch Tausenden von Adressaten ungefragt und nutzlos beachtliche Kosten und Umtriebe für die Zustellung seiner Werbung zumutet, nur um zufällig zu einzelnen Geschäftsabschlüssen zu gelangen. Ein solches Verhalten missachtet den Willen der Personen, die ihre E-Mail-Adressen im Internet für gezielte Kontaktaufnahmen und Werbung zugänglich gemacht haben. Demzufolge liegt in der Verwendung von wahllos gesammelten, nicht identifizierten E-Mail-Adressen zum Zweck der Zustellung unverlangter Streuwerbung ein Verstoss gegen den Grundsatz von Treu und Glauben im Sinne von Art. 4 Abs. 2 DSG (ebenso, wenn auch aus wettbewerbsrechtlicher Sicht, ZR 102 Nr. 39; sic! 7/8/2003).»[689]

464 Heute ist es Art. 3 lit. o UWG, in Kraft seit 2007, der Massenwerbung in besagter Form als unlautere Praxis taxiert – ein Beispiel, inwiefern über Treu und Glauben in der Praxis eine konkretisierte Vorgabe formuliert wird, die alsdann Eingang in ein Gesetz findet.

465 Ein anderer Aspekt von Treu und Glauben als Datenbearbeitungsgrundsatz wird in den *Logistep-Entscheiden* des Bundesverwaltungsgerichts resp. Bundesgerichts reflektiert.[690] Es ging um die Aufdeckung strafrechtlicher Handlungen, genauer um Urheberrechtsverletzungen im Internet durch Private.[691] Die Logistep AG, ein

689 Spamming-Entscheid des Bundesverwaltungsgerichts, JAAC 69.106, E 5.5.

690 BVGer A-3144/2008, Urteil vom 27. Mai 2009; BGE 136 II 508; vgl. zur rechtlichen Diskussion um das Internet und das Recht, die insb. die Bereiche des Urheber- und Datenschutzrechts, die Domain- und Verschlüsselungsdebatte, die elektronische Debatte und diejenige rund um schädliche Inhalte im Internet erfasse, Burkert, in: Drossu/van Haaren/Hensche et al. (Hrsg.), 185 ff., 185 f.

691 Aufschlussreich in diesem Zusammenhang die Ausführungen zu Spyware, auch mit Blick auf den Einsatz von Urheberrechtsverletzungen Bucher, 95 ff.; grundlegend zu DRM-Systemen im Zusam-

privates Unternehmen, sammelte in P2P-Netzwerken IP-Adressen von Personen, die urheberrechtlich geschützte Werke «schwarz», d. h. ohne Entrichtung der geforderten Gebühr, herunterluden. Entsprechende Angaben übermittelte sie in der Folge den Rechteinhabern, die alsdann Strafanzeige gegen Unbekannte einreichten. Im Rahmen des strafrechtlichen Akteneinsichtsrechts konnten die Identitäten der Inhaber der Internetanschlüsse erlangt werden und diese mit einer Schadenersatzforderung konfrontiert werden. Der EDÖB hatte gegenüber der Logistep AG eine Empfehlung gestützt auf Art. 29 Abs. 3 DSG erlassen, die indes nicht befolgt wurde. Daraufhin legte der EDÖB die Angelegenheit dem Bundesverwaltungsgericht zur Entscheidung vor. Dieses beschäftigte sich, nachdem es die Anwendbarkeit des DSG auf den Sachverhalt bejaht hatte, mit der Frage, ob eine Verletzung der Bearbeitungsgrundsätze vorliege. Hierbei ging es auch auf Treu und Glauben gemäss Art. 4 Abs. 2 DSG ein:

> «Dem Prinzip von Treu und Glauben kommt gerade bei der Datenbeschaffung besondere Wichtigkeit zu. Daten sollen nicht in einer Art erhoben werden, mit der die betroffene Person nicht rechnen musste und mit der sie nicht einverstanden gewesen wäre. Wider Treu und Glauben handelt namentlich, wer Daten durch absichtliche Täuschung beschafft, weil er beispielsweise die betroffene Person über seine Identität oder den Zweck seiner Bearbeitung falsch informiert, oder wer heimlich Daten beschafft, ohne dabei eine Rechtsnorm zu verletzen (vgl. Botschaft zum DSG, BBl 1988 II, S. 449). Aus dem Grundsatz von Treu und Glauben ist auch die Anforderung abzuleiten, dass eine Datenbearbeitung transparent erfolgen muss, das heisst grundsätzlich für die betroffene Person erkennbar sein muss […]. Im Zusammenhang mit der Prüfung einer Verletzung des Grundsatzes von Treu und Glauben ist daher auch die vom Kläger gerügte Verletzung des Erkennbarkeitsprinzips zu behandeln. Der Kläger macht geltend, dieses sei verletzt, weil die von der Beklagten durchgeführte Datenbearbeitung heimlich stattfinde und weder für den Urheberrechtsverletzer noch für den Inhaber des Internetanschlusses erkennbar sei. Würden die Daten als besonders schützenswerte Personendaten im Sinne von Art. 3 Bst. c DSG qualifiziert, käme der Beklagten sogar eine gesteigerte Informationspflicht zu, wonach die Einwilligung der betroffenen Person nach angemessener Information ausdrücklich zu erfolgen habe (Art. 4 Abs. 5 DSG).»[692]

Das Bundesverwaltungsgericht beurteilte das Vorgehen der beklagten Logistep AG im Lichte des Vertrauensprinzips als «diskutabel», um sodann anzufügen: 466

> «Angesichts der Umstände, die die Beklagte erst zur Datensammlung bewegten, hält diese aber vor dem Grundsatz von Treu und Glauben stand.»[693]

Allerdings: Da die Beschaffung der Daten ohne Wissen der Betroffenen erfolgte, liege in der Regel eine Verletzung des Erkennbarkeitsprinzips und damit eine Per- 467

menhang mit dem Urheberrecht Bechthold, 1 ff.; humoristisch zur Thematik der Abschnitt bei Schaar, 211 ff. unter dem Titel «Raubkopierer sind Verbrecher».

692 Vgl. BVGer A-3144/2008, Urteil vom 27. Mai 2009, E 9.3; zu den besonders schützenswerten Personendaten vgl. auch Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff.

693 Vgl. BVGer A-3144/2008, Urteil vom 27. Mai 2009, E 9.3.4. und E 9.3.6.

sönlichkeitsverletzung vor. Diese wurde als nicht widerrechtlich beurteilt, weil man in der Durchsetzung des Urheberrechtes ein überwiegendes öffentliches und privates Interesse gemäss Art. 13 DSG verortete.[694] Folglich wurden die Begehren des Klägers – sprich des EDÖB – vom Bundesverwaltungsgericht abgewiesen. Er legte das Urteil des Bundesverwaltungsgerichts alsdann *dem Bundesgericht zur Beurteilung* vor. Das Bundesgericht qualifizierte IP-Adressen nicht per se als Personendaten i. S. des DSG, ging indes im vorliegenden Fall ebenso von der Anwendbarkeit des DSG aus.[695] IP-Adressen, so das Bundesgericht, seien keine besonders schützenswerten personenbezogenen Daten, weshalb es auch keiner Einwilligung des Inhabers bedürfe. Bei der Überprüfung, ob die Vorgehensweise der Logistep AG im Einklang mit den Bearbeitungsgrundsätzen stehe, ging das Bundesgericht – anders als das Bundesverwaltungsgericht – nicht auf Art. 4 Abs. 2 DSG ein. Vielmehr stützte es seine Analyse auf Art. 4 Abs. 3 und 4 DSG und nahm eine Verletzung an.[696] Es verwarf die Argumentation im Urteil des Bundesverwaltungsgerichts und verneinte das Vorliegen eines Rechtfertigungsgrundes mit den Worten:

> «Wie bereits erwähnt, dürfen zudem Rechtfertigungsgründe beim Verstoss gegen die Grundsätze von Art. 4 DSG nur mit grosser Zurückhaltung bejaht werden (E. 5.2.4 hiervor). Mithin vermag auch das Interesse an der wirksamen Bekämpfung von Urheberrechtsverletzungen die Tragweite der Persönlichkeitsverletzung und der mit der umstrittenen Vorgehensweise einhergehenden Unsicherheiten über die Datenbearbeitung im Internet nicht aufzuwiegen. Ein überwiegendes privates oder öffentliches Interesse ist umso mehr zu verneinen, als dieses nur zurückhaltend bejaht werden darf.»[697]

468 Bezüglich Treu und Glauben als Datenverarbeitungsgrundsatz ist aus der Schweizer Doktrin besonders auf die Erwägungen von Epiney/Nüesch einzugehen. Sie weisen Treu und Glauben im Datenschutzrecht zunächst die allgemein beschriebene *Auffangfunktion* zu. Gemäss den Autorinnen handle es sich um eine Generalklausel, die dann greifen solle, wenn die anderen Bearbeitungsgrundsätze *nicht* wirksam werden.[698] Diese Auffangfunktion wird übrigens ebenso für den Bearbeitungsgrundsatz von Treu und Glauben gemäss DSGVO in der Kommentarliteratur anerkannt.[699] Die beiden Schweizer Autorinnen plädieren darüber hinaus dafür, aus dem abstrakten Bearbeitungsgrundsatz eine *individualrechtlich ange-*

694 Vgl. BVGer A-3144/2008, Urteil vom 27. Mai 2009, E 12.3.2.; zum Urteil insb. in Bezug auf die Rechtfertigungsgründe, die Rechtmässigkeit sowie den Instanzenzug Schäfer, medialex 2011, 142 ff.

695 Nach EUGH gelten dynamische IP-Adressen nicht nur für den Provider, sondern auch für den Websitebetreiber als personenbezogene Angaben, weil der Websitebetreiber über den Provider die Identität des Betroffenen erlangen kann, vgl. m. w. H. Daten:recht, BGH i. S. Breyer, Personenbezug dynamischer IP-Adressen, <https://datenrecht.ch/bgh-i-s-breyer-vi-zr-13513-16-5-17-personenbezug-dynamischer-ip-adressen/> (zuletzt besucht am 30. April 2021); zum Begriff der Personendaten bereits Bischof/Schweizer, digma 2011, 152 ff.

696 BGE 136 II 508, E 6.3.1.

697 BGE 136 II 508, E 6.3.3.

698 Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.72.

699 M. w. H. Herbst, BeckKomm-DSGVO, Art. 5 N 15.

legte Informationspflicht abzuleiten: Demgemäss könne aus dem Grundsatz von Treu und Glauben gemäss Art. 4 Abs. 2 DSG eine allgemeine Informationspflicht gegenüber Datensubjekten («den Betroffenen») hinsichtlich Datenbearbeitungen resultieren, sofern diese angesichts der Umstände aus Loyalitätserwägungen als geboten erscheine.[700] Wann sich allerdings konkret eine solche Informationspflicht aus Loyalitätserwägungen manifestieren soll, wird nicht ausgeführt. Die Totalrevision rezipiert diese Stossrichtung, indem es die Transparenzvorgaben und insb. die Informationspflichten ausbaut, vgl. Art. 19 nDSG.[701]

469 In Lehre und der Rechtsprechung zu Treu und Glauben im Datenschutz lassen sich entsprechend *zwei Akzente* feststellen:

470 *Erstens* die Bedeutung von *Transparenzvorgaben*, wobei einige sukzessive gesetzliche Spezifizierungen im informationellen Kontext ihre Quelle in Treu und Glauben finden. Aufschlussreich insofern der Blick auf die kantonalen Erlasse: Sie verzichten regelmässig auf eine abstrakte und explizite Inklusion von Treu und Glauben in ihren Datenschutzgesetzen.[702] Stattdessen verankern sie ausdrücklich den Grundsatz der Erkennbarkeit und der Informierung.[703] Auf Bundesebene soll der Ausbau von Transparenzvorgaben mit der Totalrevision des DSG einen richtungsweisenden Entwicklungsanstoss verleihen.[704] Die Totalrevision schlägt nebst weiteren Instrumenten, welche die Transparenz erhöhen, eine allgemeinere Informationspflicht vor, womit die Transparenz erhöht wird, vgl. insb. Art. 19 nDSG mit den Ausnahmen gemäss Art. 20 nDSG.

471 *Zweitens* wird über Treu und Glauben als Verarbeitungsgrundsatz erneut die Relevanz der *Umstände* bzw. des *Kontextes*, in welchen Personendatenverarbeitungen eingebettet sind, sichtbar. Über den Grundsatz wird datenschutzrechtlich die Einschlägigkeit der Verarbeitungszusammenhänge anerkannt. Der Logistep-Entscheid weist auf die Umstände hin und darauf, dass Personendatenverarbeitungen *im Lichte von Treu und Glauben dann problematisch seien, wenn die betroffene Person nicht damit rechnen müsse*. Ebendies wurde in jenem Fall angenommen aufgrund der Tatsache, dass Private auf intransparente Weise Strafverfolgungsfunktionen wahrnahmen, wobei die «verdeckt ermittelnde» Logistep AG wirtschaftliche Interessen verfolgte.[705]

700 Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.72.
701 M. w. H. Bühlmann/Lagler, SZW 2021, 16 ff.
702 Sie widmen sich entsprechend der in der Schweiz verfassungsrechtlich vorgeschriebenen Kompetenzausscheidung dem kantonalen öffentlichen Recht.
703 Meier, N 650.
704 Vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 6944 und 6974.
705 Vgl. auch unter Bezugnahme auf das Erkennbarkeitsgebot BGE 136 II 508, E 4, E 5.2.6., E 6.3.3.; vgl. zu Treu und Glauben nach DSG BVGer, A-3144/2008, Urteil vom 27. Mai 2009, E 9.

472 Beide Kernelemente von Treu und Glauben im Rahmen des DSG – Transparenz und Relevanz der Umstände – finden sich auch beim EDÖB im Schlussbericht i. S. Postfinance 2015:

> «Die Bearbeitung von Personendaten muss nach Treu und Glauben erfolgen (Art. 4 Abs. 2 DSG). Daten sollen nicht in einer Art erhoben und bearbeitet werden, mit der die betroffene Person aus den Umständen heraus nicht rechnen musste und mit der sie nicht einverstanden gewesen wäre. Gegen diesen Grundsatz verstösst beispielsweise derjenige, der Daten nicht offen bearbeitet, ohne dabei gegen eine Rechtsnorm zu verstossen (Botschaft DSG BBl 1988 II 449). Demzufolge muss eine Datenbearbeitung für die betroffenen Personen transparent erfolgen. Dies bedeutet gemäss Art. 4 Abs. 4 DSG, dass für betroffene Personen die Datenbeschaffung und jede weitere Datenbearbeitung (BSK-DSG, Urs Maurer-Lambrou/Andrea Steiner, Art. 4 N 8), der Zweck jeder (weiteren) Datenbearbeitung, die Identität des Datenbearbeiters und – bei einer Datenbekanntgabe an Dritte – die Kategorien von möglichen Datenempfängern erkennbar sein müssen (Botschaft DSG BBl 2003 2125). Auch die Beschaffung von Personendaten bei Dritten muss erkennbar sein (Botschaft DSG BBl 2003 2126).»[706]

473 Vom Grundsatz von Treu und Glauben gehen folglich wichtige Impulse für die Rechtsentwicklung aus, namentlich was *Transparenzvorgaben sowie die Integration kontextueller Erwägungen* anbelangt. Zu beiden Elementen ist immerhin zu ergänzen: Die Konkretisierung und Fortbildung des Rechts durch die *rechtsanwendenden Behörden*, die über die Generalklauseln erfolgen soll, vermag sich im Datenschutzrecht gerade auch für Treu und Glauben kaum zu entfalten. Zwar kam es in den letzten Jahren in der Schweiz zum einen oder anderen nennenswerten Urteil, das sich ebenso mit Treu und Glauben sowie den weiteren generalklauselartigen Verarbeitungsgrundsätzen beschäftigte. Gleichwohl müssen Quantität und Effekt behördlicher Datenschutzentscheide in Anbetracht der faktisch «grenzenlosen» Personendatenverarbeitungen als marginal qualifiziert werden.[707] Ursächlich für die bescheidene Rechtsdurchsetzung ist zum einen die Tatsache, dass die Kompetenzen des EDÖB für den privatrechtlichen Sektor (jedenfalls vor der Totalrevision) restriktiv gestaltet sind. Zum anderen ergreifen Einzelpersonen kaum je die privatrechtlichen Instrumente des Persönlichkeitsschutzes bei Verletzungen des Datenschutzgesetzes.[708] «Der Richterkönig», ein traditionelles Angstbild im Zusammenspiel mit den Generalklauseln, bleibt im Datenschutzrecht fiktiv.[709]

706 EDÖB, Schlussbericht Postfinance, 12.

707 Vgl. zur geografischen Grenzenlosigkeit von Personendatenverarbeitungen bereits Henke, 18 ff.; vgl. sodann die Beiträge insofern in Weber/Thürer/Zäch (Hrsg.); das sukzessive Entfallen von Grenzen aufgrund der technologischen Möglichkeiten wird im Zuge dieser Arbeit vertieft dargestellt.

708 Vgl. Rosenthal, in Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.20; hierzu auch Mayer-Schönberger, Delete, 165 ff.

709 Teubner, 42, mit dem Hinweis, dass umgekehrt hierfür durch die Freirechtsschule plädiert wurde; vgl. zum durch Weber gezeichneten Gegenbild des Gerichts als Paragrafenautomaten m. w. H. Baer, 30 f.

ROSENTHAL legt ein methodisches Rezept im Umgang mit der datenschutzrechtlichen Orientierungslosigkeit vor. Dieses Rezept ändert nichts an der Tatsache, wonach Lehre und Rechtsprechung sich lange wenig intensiv um datenschutzrechtliche Auslegungsfragen gekümmert haben. Immerhin lässt sich in den letzten Jahren auch für die Schweiz feststellen, dass dem Datenschutzrecht im Zuge der Revisionswellen von Lehre und Behörden erhöhte Aufmerksamkeit zugemessen wird. Wie aber lautet das Rezept des Datenschutzexperten? Es geht um einen «Rückgriff auf das Bauchgefühl»[710] – ein Rezept, das Juristinnen herausfordert, *a fortiori* dort, wo es um die Konkretisierung eines Terminus geht, bei dem die *vernünftig handelnde Person als Referenzperson* eine Hauptrolle spielt.[711] 474

Entsprechend liess auch für das Datenschutzrecht die Kritik an den Generalklauseln, wie sie mit der berühmten «Flucht in die Generalklauseln» in allgemeiner Weise von HEDEMANN beschrieben wurde, nicht lange auf sich warten. Früh schon wurde für den Datenschutz eine Gesetzgebung kritisiert, die per Generalklauseln Antworten zu finden suche, *weil* die neuen Technologien nicht durchschaubar und durch konkretisierte Normen dingfest gemacht werden konnten.[712] Hinzu kommt, dass als Folge der ungenügenden Wirksamkeit der prozeduralen Durchsetzungsinstrumente keine stabilisierende Praxis generiert wird. Der Mechanismus, wonach Generalklauseln wie Treu und Glauben als Normbildungsauftrag an die Gerichte figurieren, erlangt damit beschränkt Griffigkeit.[713] Ein solcher Befund ist für den privaten Bereich des DSG, für welchen kein allgemeines Verarbeitungsverbot eine markante Bearbeitungsschranke setzt, kritisch. 475

Denn: Wenn Treu und Glauben sich als primordiale Verarbeitungsvorgabe an die Datenbearbeitenden richtet, die im privaten Bereich grundsätzlich frei in der Verarbeitung sind, und die generalklauselartigen Verarbeitungsgrundsätze die Hauptschranken bilden, für diese indes kaum konkretisierte Handlungsanleitungen konsolidiert werden können, verfehlt der Grundsatz weitgehend eine seiner zentralen Funktionen. Für die datenverarbeitenden Stellen als Adressaten wird der Grundsatz mangels griffiger Konkretisierungen vonseiten der Lehre und Praxis in der Tat zur «Leerformel». 476

710 Vgl. ROSENTHAL, in: DATENSCHUTZ-FORUM SCHWEIZ, 69 ff.

711 Insb. relevant im Rahmen der Vertragsauslegung; vgl. m. w. H. MÜLLER, BK-OR, Art. 18, N 50 sowie zur weiteren Kommentarliteratur, insb. auch zu Art. 1 OR; BGE 105 II 1; BGE 133 III 406, E 2.2. in Bezug auf die allgemeinen obligationsrechtlichen Auslegungsregeln zwecks Interpretation eines Erbvertrages.

712 SIMITIS, NomosKomm.-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 20; vgl. zur schweren Verständlichkeit des Datenschutzrechts selbst für Expertinnen und Experten HOFFMANN-RIEM, AöR 1998, 513 ff., 516.

713 Zu den Generalklauseln als wichtigen Instrumenten der richterlichen Umbildung des Privatrechts TEUBNER, 9; kritisch zum Rückzug auf Generalklauseln im Datenschutzrecht unter Bezug auf das Recht auf informationelle Selbstbestimmung SIMITIS, NJW 1984, 394 ff., 400 f.

477 Nichtsdestotrotz greift es selbst für das Datenschutzrecht zu kurz, Treu und Glauben als inhaltsleere «Stirnschrift» zu bezeichnen. Seine Bedeutung liegt zwar weniger in konkretisierten Handlungsanleitungen gegenüber den personendatenverarbeitenden Stellen, die durch Lehre und Praxis bereitgestellt werden. Vielmehr sind dem Prinzip wichtige Impulse für den *gesetzgeberischen Ausbau* eines hoch ausdifferenzierten Instrumentariums zur Gewährleistung von «Transparenz» zuzuschreiben. Darüber hinaus haben die vorangehenden Ausführungen Elemente herausgearbeitet, die über Treu und Glauben die *Systemrelevanz und Kontextbezogenheit* des Datenschutzrechts sichtbar werden lassen. Das ist für die Weiterentwicklung des Datenschutzrechts von Interesse, zumal Treu und Glauben seit jeher die Rolle eines Motors für die Evaluation des Datenschutzrechts spielte.

2.3. Vertiefung der Entwicklungsimpulse und -linien

2.3.1. Ausbau von Transparenz-, Dokumentations- und Rechenschaftsvorgaben

478 Der Grundsatz von Treu und Glauben ist, wie gezeigt, Impulsgeber für die *Fortentwicklung* datenschutzrechtlicher Vorgaben, namentlich mit Blick auf den Ausbau und die Konkretisierung von *Transparenzvorgaben*. Treu und Glauben präsentiert sich als *Treiber für die Anerkennung von Informations- und Meldepflichten im Datenbearbeitungskontext*. Allerdings greift der Mechanismus der Rechtsfortbildung im Bereich des Datenschutzes, wie diese Studie zeigt, gerade nicht primär und effizient über die Gerichtspraxis.[714]

479 Vielmehr dient Treu und Glauben in erster Linie dem Gesetzgeber als *Vehikel zur Stärkung der Transparenz in Datenbearbeitungsprozessen*. Dass die Gewährleistung von Transparenz ein zentrales Anliegen der Datenschutzgesetzgebung ist, lässt sich als Antwort auf die «undurchsichtigen» Verarbeitungsprozesse sowie die Wahrnehmung der technologischen Prozesse als «Black-Box» lesen. Sie lösen Verunsicherung aus, zumal der Mensch von den Technologien zum Objekt degradiert werde. Verarbeitungsprozesse transparent(er) zu gestalten zielt auch darauf ab, den «Subjektstatus» der Person abzusichern.[715]

---

714 Vertiefend zum Vollzugsdefizit, mit welchem nicht nur die originäre (Nicht-)Einhaltung, sondern auch die ungenügende behördliche und hierbei insb. gerichtliche Durchsetzung nach Rechtsverletzungen thematisiert wird, dritter Teil, VII. Kapitel, A.2.

715 Zu diesem Zusammenhang die berühmten und viel zitierten Worte des Bundesverfassungsgerichts in seinem Volkszählungsurteil, BverfGE 65, 1, 154 – Volkszählung: «Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer

Untrennbar mit Treu und Glauben sowie der Garantie von Transparenz (aber auch Geheimhaltung) ist der Begriff des *Vertrauens* verbunden. Dies zu gewährleisten im Zusammenhang mit Personendatenverarbeitungsprozessen ist neuerdings zu einer wichtigen Aufgabe auch von Unternehmen geworden.[716] An dieser Stelle setzen die jüngsten rechtlichen Entwicklungen mit der Einführung neuer Konzepte und Instrumente an. Namentlich zu nennen sei das Rollenkonzept und die Einführung der Figur des «Verantwortlichen», vgl. Art. 5 lit. j nDSG. Hinzu treten weitere Instrumente wie die Datenschutz-Folgenabschätzung, das Verarbeitungsverzeichnis oder Dokumentations- und Rechenschaftspflichten, welche die Transparenz im Bereich Personendatenverarbeitung operationalisieren sollen. Die Instrumente sollen Verarbeitungsprozesse, Risiken sowie Massnahmen dokumentieren, womit die Konformität der Verarbeitungsprozesse mit den datenschutzrechtlichen Vorgaben navigiert werden soll. 480

Druey war es, der früh statuierte: Treu und Glauben habe eine hohe Relevanz im Informationsrecht – dies artikuliert sich namentlich in einer Kategorie von subjektiven Ansprüchen auf Information resp. reziprok: von Aufklärungspflichten.[717] Der Trend zur Fortentwicklung des Datenschutzrechts mittels Ausbaus von *Transparenzvorgaben,* die ihre Quelle in Treu und Glauben haben, konnte bereits im Rahmen der Teilrevision des DSG verzeichnet werden.[718] Die *Totalrevision* des DSG stärkt den Datenschutz über den Ausbau der Transparenzvorgaben in verschiedene Richtungen.[719] Die Gewährleistung von *Transparenz ist folglich als tragende Säule des Datenschutzrechts und seiner Entwicklungen auszumachen.* 481

Transparenz im Datenschutzrecht wird heute und insb. in Zukunft durch ein *Nebeneinander mehrerer Instrumente und Mechanismen*, materieller Rechte und Pflichten sowie prozeduraler und organisatorischer Vorgaben gewährleistet. Als klassisches Instrument gilt das *Auskunftsrecht* der Datensubjekte, vgl. Art. 8 DSG resp. Art. 25 f. nDSG. Zudem steht für das Datenschutzrecht am Anfang bekanntermassen die Anerkennung eines (abstrakten) *Erkennbarkeitsgrundsat-* 482

unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.»

716 M. w. H. statt mehrerer Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.; Dies., Schweizer Bank Mai 2018, 21 f.

717 Druey, 315.

718 Meier, N 649.

719 Botschaft DSG 2017–1084, 17.059, 6941 ff., 6944; EJPD, Bericht Begleitgruppe, 3; Rosenthal, Jusletter 16. November 2020, N 92 ff.

zes, Art. 4 Abs. 4 DSG und Art. 6 Abs. 3 nDSG, der in Treu und Glauben sein *Quellrecht* hat. Mit der ersten Teilrevision kamen weiter die Vorschriften über die Anforderungen betreffend eine gültige *Einwilligung* hinzu – vgl. Art. 4 Abs. 5 DSG, der das Instrument des «informed consent» festhält, das sein Hauptanwendungsgebiet im Arzt-, Medizin- und Biomedizinrecht findet.[720] Die Einwilligungsvorgaben finden sich nach Totalrevision in Art. 6 Abs. 6 und Abs. 7 nDSG. Erhöhte Bedeutung kommt gerade auch nach dem Inkrafttreten der DSGVO, aber auch des totalrevidierten DSG den Informationspflichten zu.

483 Aus prozeduraler Sicht seien im Zusammenhang mit Treu und Glauben sowie Transparenz im Datenschutz folgende Instrumente erwähnt, um das Bild abzurunden: Mit der Teilrevision wurde dazumals eine *Registrierungspflicht* für Datensammlungen eingeführt, vgl. Art. 11a DSG. Die Totalrevision wird das Instrument für den privaten Sektor aufgeben. Ein weiteres Instrument zwecks Schaffung von Transparenz ist die *Zertifizierung* gemäss Art. 11 DSG resp. Art. 13 nDSG, ein *Selbstregulierungsansatz:* Indem datenverarbeitende Stellen ihre Bearbeitungsprozesse gegenüber einer unabhängigen Zertifizierungsstelle offenlegen und durchleuchten lassen, wird ebenso Transparenz hergestellt. Die Verleihung eines Gütesiegels, Art. 11 Abs. 2 DSG resp. 13 Abs. 2 nDSG, schafft Transparenz nach aussen.[721] Abrundend zu nennen ist die Möglichkeit von *Abklärungen im privaten Sektor durch den EDÖB*, Art. 29 DSG, wobei er gemäss Art. 30 Abs. 2 DSG seine Empfehlungen und Feststellungen unter Umständen *öffentlich machen* kann.[722]

484 Allgemein ist ein *Akzent der Neuerung* durch die Totalrevision sowie die DSGVO darin zu sehen, dass die «Verantwortlichen» selbst nachhaltig und konkret Massnahmen zu implementieren haben, die *Transparenz* über ihre Verarbeitungsprozesse generieren und diese damit hinsichtlich ihrer Konformität mit Datenschutzvorgaben überprüfbar machen.[723] Das *Paradigma der erhöhten Transparenz* ist eine Konsequenz der Undurchschaubarkeit der informationstechnologischen Verarbeitungshandlungen. Es bleibt paradox, dass der Gesetzgeber als eine Hauptstrategie die Transparenz verfolgt, wohl wissend, dass die technologisch unterstützten Personendatenverarbeitungen kaum durchschaubar sind.

720 Vgl. Körner, in: Simon/Weiss (Hrsg.), 131 ff., 134 ff.; zur Selbstbestimmung im Abtreibungsdiskurs Krähnke, 147 ff.

721 Zu diesem vgl. Belser, in: Weber/Thouvenin (Hrsg.), 143 ff., wobei der Autor einen eigentlichen Mehrwert der Zertifizierung in der Sensibilisierung im Unternehmen verortet, die im Zuge der Zertifizierungsprüfung entsteht, 151; beachte sodann die Verordnung über die Datenschutzzertifizierung vom 27. September 2007, AS 2007 5003.

722 Zu den Kompetenzen des EDÖB nach Totalrevision vgl. Art. 49 ff. nDSG.

723 Zum Paradigmenwechsel, wonach Datenschutz zu einer Aufgabe der Compliance und des Risikomanagements wird sowie zum sog. Accountability-Ansatz, vgl. dritter Teil, VIII. Kapitel, A.2.6. und A.2.7.

Gleichwohl lässt sich feststellen, dass *Treu und Glauben* im Sinne der Schaffung von Rechenschaftsvorgaben, Transparenz sowie Gewährleistung des rechtskonformen Verhaltens datenschutzrechtlich einen starken Entwicklungsanstoss gegeben hat. Der Befund bezieht sich nicht nur auf die Massnahmen zur Erhöhung von Transparenz, sondern auch auf das Ziel, den Datenschutz faktisch griffiger zu gestalten. An dieser Stelle eine *Tour d'Horizon* über die Vorgaben nach den neuen Erlassen, die auch, aber nicht nur das Ziel verfolgen, Transparenz als Element des Datenschutzes auszubauen – Redundanzen an dieser Stelle werden aufgrund der Bedeutsamkeit des Entwicklungstrends in Kauf genommen: 485

Verankert werden *aktive Informationspflichten*, Art. 12 ff. DSGVO (vgl. auch ErwG 39) und Art. 19 nDSG.[724] Mit der Totalrevision beschränkt sich die aktive Informationspflicht nicht länger auf besonders schützenswerte Daten. Gleichwohl ist der Gegenstand der Informationspflicht gemäss Art. 19 nDSG gegenüber dem Regime in der DSGVO weniger nuanciert und detailliert. Die DSGVO differenziert zwischen direkter Erhebung, Art. 13 DSGVO (Personendaten werden beispielsweise im Rahmen des Kundenmeetings direkt beim Kunden erhoben), und indirekter Erhebung, Art. 14 DSGVO (Personendaten werden aus anderen Quellen erhoben).[725] Der Katalog von Angaben, die zum Informationsgegenstand gemacht werden, ist weit gefasst. Er umfasst insb. die vollständigen Kontaktangaben des Verantwortlichen, Angaben zum Datenschutzbeauftragten (sofern eingesetzt), Quellen sowie Kategorien der Angaben, Rechtsgrundlagen für die jeweiligen Bearbeitungen und insb. die berechtigten Interessen, sofern die Bearbeitung auf diesem Legitimationsgrund beruht, alle zur Zeit der Erhebung angestrebten Zwecke in hinreichender Detailliertheit, allfällige Empfänger, ggf. das Thema Auslandstransfer, die Speicherdauer und Kriterien zur Festlegung dieser Dauer (erfordert Löschungskonzept), Hinweise auf die Betroffenenrechte, das Beschwerderecht und Widerspruchsrecht, namentlich auch das Widerrufsrecht der Einwilligung bei den einwilligungsbedürftigen Verarbeitungshandlungen (insb. bei besonders schutzwürdigen Angaben). Zudem ist eine Risikoaufklärung vorzunehmen, mit der betroffene Personen angemessen über Risiken, Vorschriften, Garantien und Rechte sowie deren Ausübung im Zusammenhang mit der Datenverarbeitung informiert werden (ErwG 39). Weiter sind die erforderlichen Angaben bei automatisierten Einzelfallentscheidungen zu erteilen. Die Informierung muss gemäss Art. 13 Abs. 1 DSGVO vor oder bei der Erhebung der Personenda- 486

724 Zu den Neuerungen auch im Zusammenhang mit den Informationspflichten gemäss Totalrevision DSG vgl. Rosenthal, Jusletter vom 16. November 2020, N 92 ff.; Bühlmann/Lagler, SZW 2021, 16 ff.; nach DSGVO Passadelis/Roth, Jusletter vom 4. April 2016, N 6, N 24 ff., N 63 ff.; zur Totalrevision und insb. zur Dokumentation auch Sury, SJZ 2021, 458 ff.; Frei, Jusletter vom 17. September 2018; mit einer Gegenüberstellung von DSGVO und totalrevidiertem DSG Baeriswyl, SZW 2021, 8 ff.

725 Beachte insofern die einschlägige Kommentarliteratur.

ten erfolgen. Eine Ausnahme mit Blick auf den Informierungszeitpunkt gilt für die Direkterhebung, sofern die betroffene Person bereits über die Information verfügt, Art. 13 Abs. 4 DSGVO. Einzuhalten ist zudem eine Pflicht zur Nachinformation gemäss Art. 13 Abs. 3 DSGVO, beispielsweise bei Zweckänderungen. Sodann ist zu beachten, dass die Anforderungen an die Wirksamkeit der Einwilligung, die nach DSGVO ein Erlaubnistatbestand ist, hoch sind, vgl. Art. 6 Abs. 1 lit. a DSGVO. Einwilligungserklärungen müssen verständlich und in klarer sowie einfacher Sprache abgefasst sein, wobei es in der EU etablierte Praxis ist, eigenständige Datenschutzerklärungen in spezifischen Dokumenten vorzusehen. Datenschutzerklärungen im Kleindruck genügen den strengen Vorgaben der DSGVO nicht mehr.[726]

487 Neu sind zudem *umfassende Dokumentations- und Rechenschaftspflichten*, welche den Personendatenverarbeitenden auferlegt werden, vgl. insb. auch Art. 24 DSGVO. Sie zielen nicht nur auf erhöhte Transparenz hinsichtlich der Einhaltung der Datenschutzvorgaben ab, sondern auch darauf, das Datenschutzrecht seiner «formellen» Existenz zu entheben und in der Praxis griffig zu machen («Operationalisierung des Datenschutzrechts»).[727] Herzstück sowohl der *DSGVO* als auch der *Totalrevision des DSG* ist die Pflicht zur Erstellung eines *Verarbeitungsverzeichnisses*, vgl. Art. 30 DSGVO und Art. 12 nDSG. Die Erfassung und Abbildung der Landschaft von Datenverarbeitungsprozessen ist Dreh- und Angelpunkt für die Einhaltung der datenschutzrechtlichen Vorgaben und deren Überprüfung. Das Inventar ist Basisinstrument zur Verwirklichung des breiten Fächers an Instrumenten und Vorgaben, die der Schaffung von Transparenz mit Blick auf Personendatenverarbeitungen dienen. Allgemein verlangt die DSGVO gemäss Art. 24, dass *jederzeit Rechenschaft* über die *Datenschutzkonformität der Verarbeitungstätigkeiten* abgelegt werden können muss, womit auch umfassende Dokumentationspflichten einhergehen. Gesprochen wird vom sog. *Accountability-Ansatz*.[728] Es sind die datenverarbeitenden Stellen, die jederzeit in der Lage sein müssen, darzulegen, dass ihre Verarbeitungstätigkeiten datenschutzrechtlich regelkonform sind. Die Totalrevision des DSG sieht nicht ausdrücklich ein Pendant vor. Allerdings ist davon auszugehen, dass sich auch in der Schweiz ein entsprechender Ansatz als Element der Data Governance durchsetzen wird.

488 *Rechenschaftspflichten* wurden bisher ausserhalb des Datenschutzrechts insb. für Konstellationen vorgesehen, in denen jemand ein Geschäft für einen anderen erledigt.[729] Die Person, die das Geschäft für einen anderen besorgt, kennt sich

726 Vgl. Passadelis/Roth, Jusletter vom 4. April 2016, N 22.
727 Hierzu Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.; vertiefend dritter Teil, VIII. Kapitel, A.2.5.
728 Vgl. Art. 24 DSGVO; Hartung, BeckKomm-DSGVO, Art. 24 N 20; vgl. zum Accountability-Ansatz und zum Data Mapping Schröder, digma 2020, 16 ff.; Sury, SJZ 2021, 458 ff., 462 f.
729 Die folgenden Ausführungen basieren auf Druey, 230.

in aller Regel in der Sache besser aus, verfügt über eine spezifische Expertise und kennt die Usanzen der Branche. Rechenschaftspflichten überbrücken eine Distanz, in der die Geschäftsherrin zu ihrer Angelegenheit infolge unzureichender Ressourcen (Expertise, Zeit, Nähe) steht. Die geschäftsführende Person legt zudem gegenüber der beauftragenden Person wie auch gegenüber sich selbst Rechenschaft darüber ab, dass sie sich bewusst ist, mit der Besorgung eines fremden Geschäftes resp. der Verwaltung eines fremden Gutes betraut zu sein. Weiter beinhaltet die Rechenschaft eine bewertende Überprüfung, ob die Handlungen in Einklang mit den normativen Erwartungen und Vorgaben stehen. Zugleich gelten Rechenschaftspflichten als *Entlastungsstrategie*:[730] Die Geschäftsherrin ersucht darum, den Eindruck zu erlangen, dass ihre Angelegenheit in guten Händen, der Geschäftsgang regelmässig ist. Sie tut dies im Sinne eines Appells an das erwiesene *Vertrauen*. Die geschäftsführende Person liefert mit der Rechenschaft ggf. auch den Beleg, sich des Vertrauens würdig zu erweisen. Verweigerte, ausweichende, lückenhafte, widersprüchliche Rechenschaftsauskünfte gelten als Hinweise, wonach ein Prozess oder Vorgehen nicht regelkonform ist. Sie geben Anlass, allfällige Defizite aufzudecken. Die regelmässige Rechenschaft ermöglicht es, Zeitpunkt, Inhalt, Ort und Ansatz defizitärer Entwicklungen zu lokalisieren. Bestätigen sich Fehlentwicklungen, wird in der Regel nicht nur das Vertrauen, sondern auch das Geschäft entzogen. Rechenschaftspflichten und -rechte sind folglich hocheffiziente und zugleich niederschwellige *Kontrollinstrumente*. Sie verzichten (vorab) auf eine rigide, engmaschige, interventionistische Kontrolle, die eine effiziente Geschäftsführung im Ergebnis behindern. Vielmehr geht das Konzept der Rechenschaft davon aus, was sowohl Treu und Glauben als auch die Expertise des Geschäftsführenden nahelegen: Ausgangspunkt ist die Annahme eines *redlichen Verhaltens*, eines vertrauensvollen Umgangs im Allgemeinen; reflektiert wird die Vertrauenswürdigkeit mit Blick auf Kenntnisse, Ernsthaftigkeit und Umsicht eines Experten oder einer Expertin. Als Garanten für die Expertise kommen sodann nicht zuletzt Ausbildung, Diplome, Standesregeln usf. zum Einsatz.[731]

Entsprechende Ideen werden jüngst datenschutzrechtlich rezipiert, sind es doch 489
an *erster Stelle* die Verarbeitenden, die dafür sorgen können und müssen, dass ihre Personendatenverarbeitungen den datenschutzrechtlichen Vorgaben entsprechen. Die DSGVO verankert unter dem Titel «*Verantwortung des für die Verarbeitung Verantwortlichen*» in Art. 24 DSGVO einen eigentlichen Generalauftrag des Verantwortlichen zur Gewährleistung der Datenschutz-Compliance.[732] Den Verantwortlichen obliegt es, dokumentieren zu können, dass ihr Handeln im Ein-

730 Druey, a. a. O.
731 Teubner, in: Brüggemeier (Hrsg.), 303 ff., 318 ff.
732 Raschauer, NomosKomm-DSGVO, Art. 24 N 10.

klang mit den datenschutzrechtlichen Vorgaben steht. Mit den jüngsten datenschutzrechtlichen Neuerungen werden folglich an erster Stelle die *Personendatenverarbeitenden* in die Pflicht genommen, wobei diese in Bezug auf die Einhaltung der datenschutzrechtlichen Vorgaben und die getroffenen Massnahmen dokumentations- und rechenschaftspflichtig sind.[733]

490 Dieser *neue Accountability-Ansatz* steht in einem engen Zusammenhang zu Treu und Glauben. Datenschutzrechtlich betrachtet lässt sich damit weiter feststellen: Zum einen lässt sich der Accountability-Ansatz in einer individualrechtlichen Richtung sehen, indem die entsprechenden Dokumentationen auch der Umsetzung und Gewährleistung der Betroffenenrechte dienen. Zum anderen wird sichtbar, dass der Datenschutz mit diesem Ansatz zu einer Aufgabe im Interesse der Good Governance der jeweiligen Unternehmen, Organisationen resp. Institutionen wird.

491 Im Rahmen der Relevanz von Treu und Glauben, der erhöhten Transparenz sowie der Aufgabe, die Datenschutz-Compliance und Data Governance zu installieren, ist auf das Instrument der *Datenschutz-Folgenabschätzung* hinzuweisen: Dort, wo Datenbearbeitungen mit einem erhöhten Risiko für Persönlichkeitsverletzungen einhergehen, muss eine entsprechende Analyse erstellt werden, die auf Verlangen der Datenschutzaufsichtsbehörde resp. dem EDÖB vorgelegt werden soll, vgl. Art. 35 DSGVO und Art. 22 nDSG.

492 Ein jüngeres spezifisches Aktivitätsfeld von Treu und Glauben lässt sich im *Umgang mit sog. Datensicherheitsvorfällen mit ihren entsprechenden Notifikationspflichten* verorten, vgl. Art. 33 f. DSGVO und Art. 24 nDSG.[734] Bis zum Inkrafttreten der Totalrevision wurde eine sinngemässe Informationspflicht aus Art. 4 Abs. 2 erster Satzteil DSG abgeleitet, womit sich die rechtsfortbildende Kraft von Treu und Glauben im Datenschutzrecht bestätigt. Der Hauptimpuls für die Integration einer ausdrücklichen gesetzlichen Notifikationspflicht nach totalrevidiertem DSG scheint indes von der DSGVO auszugehen: Die DSGVO statuiert eine entsprechende Meldepflicht gemäss Art. 33 f. Hierbei legt Art. 33 DSGVO die Notifikation an die Behörden nieder, Art. 34 DSGVO darüber hinausgehend die

733 Ein Beispiel soll das Erörterte datenschutzrechtlich umreissen: Die DSGVO verankert einen extraterritorialen Ansatz, vgl. Art. 3 Abs. 2 lit. a und lit. b DSGVO, womit auch Unternehmen in der Schweiz in ihren Anwendungsbereich fallen können. Viele Fragen sind derzeit mit Blick auf die Tatbestandselemente des Anwendungsbereiches unklar. Indes erscheint es geboten, für Schweizer Unternehmen mit EU-Ausrichtung eine Basisanalyse vorzunehmen, in welcher die Frage erörtert wird, ob und inwiefern man in den Anwendungsbereich der DSGVO fällt. Wird die Anwendbarkeit der DSGVO aufgrund einer entsprechenden Analyse verneint und kommt indes eine Europäische Behörde zu einem anderen Ergebnis, wird die Verantwortlichkeit des Verantwortlichen anders beurteilt werden als diejenige eines Verarbeitenden, der keine entsprechende Analyse vorgenommen hat; vgl. Pfaffinger, in: Emmenegger (Hrsg.), 17 ff.; zur Accountability resp. Ablegung von Rechenschaft auch Cichocki, Jusletter IT vom 21. Mai 2015, N 49 ff.

734 Vgl. Rosenthal, HK-DSG, Art. 4 N 16; Meier, N 657.

Benachrichtigung an die Datensubjekte, sofern ein qualifiziertes Risiko mit der Verletzung des Schutzes von Personendaten einhergeht.

493 Mehrere weitere Transparenzinstrumente vervollständigen die Landschaft: Im Zusammenhang mit der Totalrevision sind die Vorgaben im Zusammenhang mit den automatisierten Einzelfallentscheidungen zu nennen, vgl. z. B. Art. 21 nDSG. Auch Zertifizierungen zielen darauf ab, die Transparenz von Datenverarbeitungen zu verbessern sowie die Einhaltung der datenschutzrechtlichen Vorgaben zu erhöhen.[735] Im Rahmen des Zertifizierungsverfahrens wird sachkundig die Konformität der Datenverarbeitungen der sich ihm freiwillig unterwerfenden Verantwortlichen überprüft und ggf. Verbesserungspotential aufgezeigt. Erfolgt der Nachweis der Rechtskonformität, wird ein Zertifikat ausgestellt, das als Gütesiegel nach aussen den Datensubjekten und Konsumentinnen, Klientinnen, Versicherten usf. das erfolgreich durchlaufene Prüfungsverfahren ausweist. Im Ergebnis vermittelt man damit auch den Datensubjekten, die den datenverarbeitenden und zertifizierten Unternehmen in verschiedenen Rollen begegnen, die Information und daraus folgend das Vertrauen, dass das Unternehmen den Datenschutz ernst nimmt und sich datenschutzkonform aufstellt. Die Datensubjekte, denen weiterhin Individualrechte inklusive Haftungsansprüche infolge von Datenschutzverstössen zukommen, erlangen mit dem Zertifikat resp. dessen Fehlen eine bedeutsame Entscheidungsgrundlage für die Gestaltung ihrer Geschäftsbeziehungen. Das Instrument ist in anderen Bereichen, z. B. in der Lebensmittel- oder Textilbranche, gut etabliert. Es dient nicht nur der Qualitätssicherung; vielmehr dient es auch dazu, Konsumentinnen und Konsumenten die Informationen zu vermitteln, um informierte und verantwortungsvolle Entscheidungen zu treffen.

494 *Zusammenfassend* lässt sich feststellen, dass *Treu und Glauben eine treibende Kraft im Zusammenhang mit der Rechtsfortbildung ist,* namentlich in Bezug auf die Anerkennung und den Ausbau von Transparenzvorgaben. Das Prinzip der Transparenz, das untrennbar mit dem Gebot von Treu und Glauben in Verbindung steht, wird namentlich im Zuge der DSGVO, aber auch der Totalrevision des DSG mit einem dichten Netz *unterschiedlicher Instrumente* ausgebaut: mittels aktiver Informationspflichten, Meldepflichten, ggf. Register, Auskunftsrechten, Dokumentations- und Rechenschaftspflichten, aber auch Zertifizierungsverfahren. Der *Trend*, im Rahmen des Datenschutzes über Treu und Glauben *Transparenzerfordernisse* und Rechenschaftsinstrumente, verknüpft mit prozeduralen und organisatorischen Massnahmen auszubauen, *entspricht den Erwartungen einer Wissens- und Informationsgesellschaft*.[736] Wenn im Zuge der

735 Vgl. Raschauer, NomosKomm-DSGVO, Art. 42 N 1.

736 Vgl. zum Trend im Familienrecht, Informationsrechte sukzessive auszubauen, Pfaffinger, FamPra.ch 2014, 604 ff.; vgl. mit Blick auf Informationspflichten in einem spezifischen Kontext, dem

jüngsten Neuerungen die Transparenz- und Rechenschaftsvorgaben durch mehrere neue Instrumente, die sich als «Umsetzungsinstrumente» beschreiben lassen, gesetzlich ausgebaut werden, dann darf zugleich angenommen werden, dass Treu und Glauben als allgemeiner und abstrakter Verarbeitungsgrundsatz und Auffangtatbestand an Bedeutung verlieren wird.

2.3.2. Integration kontextueller Erwägungen

495 Neben der Bedeutung von Treu und Glauben im Kontext der *Gewährleistung von Transparenz* ist ein *weiterer Aspekt von diesem Grundsatz* mitgeprägt. Der Zugriff auf diesen zweiten Aspekt erfolgt seinerseits über die soeben beleuchtete Transparenz- und Informationsthematik im Zusammenhang mit Treu und Glauben. Der Ausbau der Informationspflichten und damit der Transparenz ist, wie dargelegt, ein Kernanliegen der Totalrevision.[737]

496 Bislang wurde in der Schweizer Lehre im Rahmen des noch geltenden Datenschutzgesetzes aus dem Bearbeitungsgrundsatz von Treu und Glauben ein Informationsrecht resp. eine Informationspflicht wie folgt abgeleitet: Aus dem Grundsatz von Treu und Glauben gemäss Art. 4 Abs. 2 DSG könne eine *Informationspflicht gegenüber Datensubjekten* («den Betroffenen») hinsichtlich Datenbearbeitungen resultieren, sofern diese *angesichts der konkreten Umstände aus Loyalitätserwägungen geboten erscheine*.[738]

497 An dieser Stelle soll die Bedeutung und Einschlägigkeit von «vernünftigen Erwartungen», die eng mit Treu und Glauben verbunden sind, im Lichte der Umstände von Personendatenverarbeitungen angesprochen werden. Der Aspekt hat in der Datenschutzdebatte der Schweiz bislang keine besondere Aufmerksamkeit gefunden.

498 Ganz anders präsentiert sich die Situation in den USA, wo die Doktrin der *«reasonable expectations of privacy»* Gegenstand zahlreicher Gerichtsentscheide bildet.[739] Sie wird als Instrumentarium eingesetzt, um Privacy-Herausforderungen, die sich infolge des Einsatzes neuer Technologien ergeben, zu bewältigen. Die Rechtsfigur findet über die Rechtsprechung des EGMR zu Art. 8 EMRK auch im europäischen Rechtsraum Einsatz.[740] Aber auch im Zusammenhang mit der

---

Bankenbereich, und zu Informationspflichten des Bankiers, abgeleitet aus Art. 2 ZGB, Emmenegger, in: Chappuis/Winiger, 67 ff., 70.

737 Vgl. BBl 2017–1084, 17.059, 6941 ff., 6944 und 6972 ff.

738 Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.72.

739 Mit Hinweisen auf das Urteil Katz v. United States und das Votum von Justice Harlan Nissenbaum, 241.

740 Hierzu vertiefend dritter Teil, IX. Kapitel; dazu, dass in Grossbritannien Prominente lange quasi Freiwild waren für die Regenbogenpresse, diese Situation sich allerdings mit dem Entscheid Campbell v. Mirror Ltd. änderte, wobei das Gericht seine Argumentation auf die *«reasonable expectations of privacy»* stützte, Hoppe, ZUM 2005, 41 ff., 43.

DSGVO findet die Konstruktion Erwähnung. Eine vertiefende Auseinandersetzung mit diesem Ansatz wird im dritten Teil dieser Arbeit erfolgen.[741]

499 Zu vermerken ist, dass sich die *«reasonable expectations of privacy»* nicht auf eine individuelle, subjektive Sicht und Einschätzung des adressierten Individuums beschränken. Vielmehr wird über die Figur eine objektive sowie gesellschaftliche Komponente integriert. Die *Vernünftigkeit der Erwartung* wird ihrerseits anhand der jeweiligen *spezifischen gesellschaftlichen Kontexte* mit den sie mitstrukturierenden Erwartungen eruiert. Es ist somit die Verletzung von kontextrelativen Normen, die als Verstoss gegen vernünftige Privacy-Erwartungen taxiert wird.[742]

500 In Europa zeigt sich der Einfluss kontextueller Erwägungen über die Figur der vernünftigen Privatheitserwartungen in einem Dokument der WP 29 zur DSGVO, der «Opinion 2/2017 on data processing at work». Das Dokument befasst sich bereichsspezifisch mit Fragen des Datenschutzes und der Datenschutz-Grundverordnung im Arbeitskontext:

> «This opinion makes a new assessment of the balance between legitimate interests of employers and the reasonable privacy expectations of employees by outlining the risks posed by new technologies and undertaking a proportionality assessment of a number of scenarios in which they could be deployed.»[743]

501 Über die Figur wird darauf abgezielt, im Vorfeld vom konkret betroffenen Datensubjekt in seiner Rolle als Arbeitnehmer zu abstrahieren und zugleich bereichsspezifisch anhand von Szenarien die Auswirkungen bestimmter Personendatenverarbeitungsprozesse zu evaluieren. Treu und Glauben und die daran ankoppelbaren «vernünftigen Erwartungen» des Datensubjektes lassen sich somit als Einfallstor bezeichnen, über welches die *Relevanz des Verarbeitungszusammenhanges und -kontextes* in die datenschutzrechtlichen Erwägungen integriert wird.[744]

502 Wenn aus dem Verarbeitungsgrundsatz von Treu und Glauben Informationspflichten angesichts der Umstände aus Loyalitätserwägungen abgeleitet wurden, schliesst das die Anerkennung ein, wonach *kontextrelative Erwägungen für das Datenschutzrecht* einschlägig sind. Die vernünftigen Erwartungen des Datensubjektes sind indes im Rahmen von Personendatenverarbeitungen differenziert, die vernünftige Person keine einheitliche Figur.[745] Vielmehr hängen sie vom *Verarbeitungszusammenhang* ab, vom jeweiligen gesellschaftlichen Kontext, in welchen

741 Vgl. auch Paefgen, 33 ff.; vertiefend dritter Teil, IX. Kapitel.
742 Nissenbaum, 233.
743 Vgl. <ec.europa.eu/newsroom/document.cfm?doc_id=45631, 3> (zuletzt besucht am 30. April 2021).
744 Auf die Bedeutung des Verarbeitungszusammenhanges und der Relationen, in denen Informationsverarbeitungen stattfinden, wies früh bereits Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 30, hin, wobei sich sein Fokus gleichwohl auf die Person als Subjekt richtet.
745 Zum vernünftigen Menschen als (hypothetische) Figur des Obligationenrechts vgl. Gauch, in: Steinauer (Hrsg.), 177 ff., 179 auch zu verschiedenen Rollen.

die Personendatenverarbeitungen eingebettet sind, und von den Rollen, in denen agiert wird.[746]

503 Die Korrelation zwischen Treu und Glauben und der Beachtlichkeit kontextueller Bezüge von Personendatenverarbeitungen deutet sich im Logistep-Fall an. Es waren der EDÖB und das Bundesverwaltungsgericht, nicht aber das Bundesgericht, die Treu und Glauben sowie die Umstände zur Beurteilung beizogen. Wie bereits dargestellt, handelte es sich um einen Konflikt zwischen Privaten. Hierbei wurde die Logistep AG vertraglich damit beauftragt, Personen resp. deren Surfverhalten auszuspionieren, um damit Urheberrechtsverletzungen aufzudecken. Im Ergebnis nahmen Private eine Aufgabe wahr, die der Strafverfolgung der öffentlichen Hand vorbehalten sein soll. Das Vorgehen wurde, wie dargetan, als Verstoss gegen datenschutzgesetzliche Vorgaben taxiert. Das Bundesverwaltungsgericht hielt fest, dass Personendaten nicht in einer Art erhoben werden dürfen, mit der die betroffene Person nicht rechnen musste. Mit anderen Worten: Geheime Ausforschungen eines privaten Lebensbereiches aus ökonomischen Interessen und zwecks Strafverfolgung durch Private wurden als Verstoss gegen den Verarbeitungsgrundsatz von Treu und Glauben taxiert, weil die betroffenen Personen damit nicht rechnen mussten. Die Konstellation des Logistep-Falles ist übrigens der bei den Versicherungsbetrugsfällen und den dort erfolgenden Observationen ähnlich.[747] Der letzte Teil dieser Arbeit wird sich zwecks Entwicklung eines Vorschlages zur Rekonfiguration eines Datenschutzrechts der Zukunft vertieft damit befassen.

504 Die getätigte Analyse führt vor Augen, dass bereits unter geltendem Recht, namentlich auch über «Treu und Glauben», die *vernünftigen Erwartungen* der von Personendatenverarbeitungen betroffenen Personen adressiert werden. Als Verarbeitungsgrundsatz und Handlungsanleitung an die personendatenverarbeitenden Stellen allerdings bleibt Treu und Glauben wenig ergiebig, namentlich, weil weder über die Praxis noch Lehre konkrete Konsolidierungen des sehr abstrakten Grundsatzes generiert werden. Treu und Glauben beschränkt sich insofern für das Datenschutzrecht auf eine flankierende Rolle an den äussersten Rändern, wie es Treu und Glauben, namentlich aber dessen Spiegelbild, dem Rechtsmissbrauchsverbot, entspricht.

505 Es ist nunmehr auf den zweiten in Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG niedergelegten Verarbeitungsgrundsatz, das Verhältnismässigkeitsprinzip, einzugehen. Auch zu diesem gibt es markige Einschätzungen:

746 Hierzu vertiefend Nissenbaum, 129 ff.; Simitis, in: Schlemmer (Hrsg.), 67 ff., 74 f.

747 Blick, Aargauer Justizdirektor ist gegen das Schnüffler-Gesetz, Zürich 2018, <https://www.blick.ch/politik/unterstuetzung-fuer-sybille-berg-und-co-aargauer-justizdirektor-ist-gegen-das-schnueffler-gesetz-id8247397.html> (zuletzt besucht am 30. April 2021).

«Der Grundsatz der Verhältnismässigkeit scheint heute in der Welt des Rechts omnipräsent zu sein.»[748]

Fest steht: Für das duale Regime des DSG ist die Voranstellung eines Verhältnismässigkeitsprinzips, das ebenso für Personendatenverarbeitungen im privaten Bereich gilt, erklärungsbedürftig. 506

3. Das Verhältnismässigkeitsprinzip

3.1. Aspekte und kontextualisierte Analyse

> «Der Grundsatz der Verhältnismässigkeit hat eine spektakuläre Erfolgs- und Rezeptionsgeschichte hinter sich. Von seinen eher diffusen verwaltungsrechtlichen Ursprüngen hat er sich unter dem Grundgesetz zu einem der zentralen Elemente der Grundrechtsdogmatik emanzipiert und greift auch in andere Bereiche, nicht nur des Verfassungsrechts, aus.»[749]

Im DSG ist das Verhältnismässigkeitsprinzip als «gemeinsamer» Verarbeitungsgrundsatz gleichermassen für den öffentlichen wie den privaten Sektor zusammen mit Treu und Glauben in Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG niedergelegt.[750] Rosenthal weist dem Prinzip eine Art «Scharnierposition» zu, wonach dieses nicht nur eng mit dem Zweckbindungsgrundsatz verknüpft sei, sondern sich stattdessen ebenso mit weiteren Grundsätzen überschneiden könne.[751] 507

In der Lehre wird dem Grundsatz hohe praktische Relevanz zugewiesen. Gleichwohl gilt er als der am häufigsten verletzte Grundsatz.[752] Die Sichtung der vorhandenen (rudimentären) Gerichts- und Verwaltungspraxis sowie der Wissenschaft zeigt, dass das Verhältnismässigkeitsprinzip als datenschutzrechtlicher Verarbeitungsgrundsatz für den öffentlichen wie den privaten Sektor *identisch interpretiert wird*. Die Botschaft von 1988 gab bereits eine eindeutige Anweisung: 508

> «Mit dem in diesem Absatz statuierten Verhältnismässigkeitsgebot wird das im öffentlich-rechtlichen Bereich ohnehin geltende Verhältnismässigkeitsprinzip auch für den privaten Bereich als anwendbar erklärt. Der Datenbearbeiter ist demnach gehalten, nur diejenigen Daten zu erheben und weiter zu bearbeiten, die für einen bestimmten Zweck geeignet sind und die er tatsächlich benötigt. Wer z. B. Autos vermietet, darf zwar die Personalien des Mieters erheben; übermässig wäre es aber, wenn der Mieter zusätzlich Auskünfte über seine Familienverhältnisse oder seine Beziehungen zu weiteren Drittper-

748 Jestaedt/Lepsius (Hrsg.), Vorwort, VII.
749 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 261 ff., 276.
750 Vgl. zum Grundsatz der «Datenminimierung» auch Art. 5 Abs. 1 lit. c DSGVO; jüngst erwähnt in BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 3; zu den Erwägungen des Gerichts in Bezug auf die verschiedenen Vorgaben gemäss DSG Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f. und zur Empfehlung des EDÖB Dies., digma 2018, 154 ff.; Vasella/Ziegler, digma 2019, 80 ff.; Pärli, SZS 2018, 107 ff. kritisch zur verordneten Selbstverantwortung.
751 Rosenthal, HK-DSG, Art. 4 N 26.
752 Ders., HK-DSG, Art. 4 N 19 und N 27; Meier, N 669.

sonen verlangt. Bei Kreditauskünften wiederum können neben Angaben über Vermögensverhältnisse und Zahlungsmoral auch die Familienverhältnisse wesentlich sein; übermässig wären aber Auskünfte über die Religionszugehörigkeit oder politische Auffassungen der überprüften Person. Des Weiteren muss aber auch zwischen dem Bearbeitungszweck und der mit Blick darauf nötigen Persönlichkeitsbeeinträchtigung ein vernünftiges Verhältnis bestehen. So ist es etwa unzulässig, im Hinblick auf einen Wahlkampf das Privatleben eines politischen Gegners umfassend und systematisch auszuforschen.»[753]

509 Das Verhältnismässigkeitsprinzip kann entsprechend als «Import» vom öffentlichen Recht in das Privatrecht bezeichnet werden. Personendatenverarbeitungen durch öffentliche Stellen des Bundes wie durch Private müssen *geeignet* sein, einen fixierten Zweck zu erreichen, und insofern *erforderlich* sowie *verhältnismässig im engeren Sinne*.[754] Die Trias der Verhältnismässigkeit, wie sie für das öffentliche Recht entwickelt wurde, gilt im Datenschutzrecht für den privaten Bereich gleichermassen: Demnach muss im privaten Sektor die Art und Weise jeder Personendatenverarbeitung zur Verwirklichung eines bestimmten Zwecks objektiv geeignet und notwendig sein; zudem soll der angestrebte Zweck in einem vernünftigen Verhältnis zu den Beeinträchtigungen stehen.[755]

510 Die *datenschutzrechtliche Verhältnismässigkeit* wird vorab *generisch als prinzipielle Verhältnismässigkeit* umrissen: Angeführt werden hierbei die Gebote der Datensparsamkeit und -minimierung sowie das Verbot der Vorratsdatensammlung, vorbehältlich seiner Durchbrechung mittels ermächtigender gesetzlicher Grundlage.[756]

511 Meier beschreibt als ein *Unterprinzip* des allgemeinen Verhältnismässigkeitsgebots die *materielle Verhältnismässigkeit*. Unter dem Begriff thematisiert er die Art der Verarbeitungsmethode und die Ausbreitung der gesammelten Personendaten über verschiedene Felder hinweg, im Sinne des Zugriffes von einem Kontext auf einen anderen.[757]

512 Als weiteres *Unterprinzip* wird die *temporelle Verhältnismässigkeit* genannt. Hierbei wird allem voran danach gefragt, wie lange Datenbestände gespeichert werden dürfen resp. wann eine Löschung oder Anonymisierung angezeigt ist.[758] Die Löschung von Personendaten ist folglich nicht nur und nicht erst aufgrund der Geltendmachung des entsprechenden Betroffenenrechts vorzunehmen, son-

753 BBl 1988 II 414 ff., 450.
754 Hierzu namentlich Maurer-Lambrou/Steiner, Art. 4 N 11; Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.78 ff.; Rampini, BK-DSG, Art. 12 N 4.
755 Vgl. Pedrazzini, in: Schweizer (Hrsg.), 19 ff., 27; Steinauer, in: Schweizer (Hrsg.), 43 ff., 45; zum Verhältnismässigkeitsprinzip sodann BBl 1988 II 414 ff., 450 und BBl 2017–1084, 17.059, 6941 ff., 7026 f.
756 Vgl. Meier, N 633 und N 661 ff.; Bolliger/Féraud/Epiney/Hänni, 12; Rosenthal, HK-DSG, Art. 4 N 19 ff.; vgl. zudem Bereits, 132 ff.
757 Meier, N 676 ff.
758 Hierzu neben Ders., N 679 f. weiter auch Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.79; ein Verfallsdatum für Daten schlägt Mayer-Schönberger, Delete, 201 ff. vor.

dern stets dann, wenn die Verhältnismässigkeit entfällt. In diesem Zusammenhang sind Vorgaben aus anderen Rechtsbereichen zu beachten, namentlich Archivierungspflichten, wie sie für verschiedenste Bereiche anerkannt sind.[759] Die Totalrevision des DSG greift diesen temporellen Aspekt ausdrücklich mit Art. 6 Abs. 4 nDSG auf. Entsprechend ist nach Totalrevision das Verhältnismässigkeitsprinzip an zweierlei Stellen, Art. 6 Abs. 2 und Art. 6 Abs. 4 nDSG, verankert.[760]

513 Die griffigste Konkretisierung zum datenschutzrechtlichen Verhältnismässigkeitsprinzip findet sich bei Rosenthal: Der Grundsatz setze vorab, gemeinsam mit dem Zweckbindungsgrundsatz, das datenschutzrechtliche *Prinzip der Datensparsamkeit* resp. das *Need-to-know-Prinzip* um.[761] So verbietet das Kriterium der Erforderlichkeit das Sammeln von Daten, das in sachlicher, zeitlicher, räumlicher oder persönlicher Hinsicht objektiv über das zur Zweckerreichung Notwendige hinausgeht.[762] Vorratsspeicherungen sind also nicht verhältnismässig, da diese Verarbeitungshandlungen gerade keinen bestimmten Zweck verfolgen. Zudem verlangt der Grundsatz eine wiederholte Überprüfung der Personendatenbestände.[763]

514 Ursprünglich wurde der Verhältnismässigkeitsgrundsatz, wie eingangs zitiert, im öffentlichen Recht installiert. In der Schweiz gilt der Grundsatz allgemein aufgrund von Art. 5 Abs. 2 BV, sodann Art. 36 Abs. 3 BV. Das Prinzip zielt darauf ab, staatliche Macht gegenüber den Bürgerinnen und Bürgern zu regulieren; das *Verhältnis Bürger – Staat ist ein asymmetrisches*. Das Verhältnismässigkeitsprinzip spielt seit jeher eine Schlüssel- oder Hauptrolle im öffentlichen Recht.

515 Anders kommt ihm im Privatrecht eine *Nebenrolle* zu. Im Aufsatz von Kähler mit dem humoristischen Titel «Raum für Masslosigkeit. Zu den Grenzen des Verhältnismässigkeitsgrundsatzes im Privatrecht» ist zu lesen:

> «So triumphal der Siegeszug des Verhältnismässigkeitsprinzips im öffentlichen Recht verlaufen ist, so klar sind ihm im Privatrecht Grenzen gesetzt.»[764]

516 Die Bedeutung des Verhältnismässigkeitsprinzips im nicht-öffentlichen Bereich ist folglich keineswegs trivial. Ein *funktionales Äquivalent* findet das Verhältnismässigkeitsprinzip im Privatrecht in erster Linie im *Rechtsmissbrauchsverbot gemäss Art. 2 Abs. 2 ZGB*. Allerdings formuliert der privatrechtliche Rechtsmissbrauch die *Grenzen deutlich weiter aussen*, als es das öffentlich-rechtliche Verhältnismässigkeitsgebot tut: Nach Art. 2 Abs. 2 ZGB ist es das «krass stossende Verhal-

759 Zum Datenschutzrecht, seinen Grundprinzipien und den Herausforderungen der Archivierung vgl. Husi-Stämpfli/Gisler, in: Epiney/Nüesch (Hrsg.), 103 ff., insb. 110 ff.
760 Hierzu Rosenthal, Jusletter vom 16. November 2020, N 33 f. und N 51.
761 Vgl. Ders., HK-DSG, Art. 4 N 19 ff.; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 11.
762 Rampini, BSK-DSG, Art. 4 N 11; zum Ganzen Rosenthal, HK-DSG, Art. 4 N 20 ff.
763 Peter, 134.
764 Kähler, in: Jestaedt/Lepsius (Hrsg.), 210 ff., 233.

ten», das untersagt wird.[765] Zur Konkretisierung von Art. 2 Abs. 2 ZGB wurden verschiedene Fallgruppen strukturiert.[766]

517 Die Verhältnismässigkeit ist für das Privatrecht im Zusammenhang mit dem Grundsatz der Privatautonomie zu sehen: Dem Grundsatz der Privatautonomie mit seinen verschiedenen Aspekten (z. B. Vertragsfreiheit) setzt der Privatrechtsgesetzgeber in erster Linie mittels *zwingenden Rechts Schranken*. Solche Schranken qua zwingendem Recht finden sich namentlich im sog. sozialen Privatrecht und hierbei im privatrechtlichen Arbeitsrecht oder Mietrecht, zudem im Konsumentenschutzrecht.

518 Weiter ist zur Erfassung der Bedeutung des Verhältnismässigkeitsprinzips mit privatrechtlichen Bezügen in Feldern wie dem Kindes- und Erwachsenenschutz[767] oder im Kartell- und Wettbewerbsrecht anzusiedeln.[768] – Rechtsgebiete, welche vor Augen führen, dass die Idee einer scharfen Trennung zwischen öffentlichem und privatem Recht rein theoretischer Natur ist.

519 Erwägungen zur *Verhältnismässigkeit* fliessen folglich m. E. in Konstellationen *struktureller Ungleichgewichte und Asymmetrien in gesellschaftlichen Beziehungen* in das Privatrecht ein.

520 Dies ist der Hintergrund, vor dem sich der Verhältnismässigkeitsgrundsatz als gemeinsames Verarbeitungsprinzip für den privaten und öffentlichen Bereich gemäss Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 und Abs. 4 nDSG verstehen lässt. Aufgrund der in Personendatenverarbeitungszusammenhängen, unterstützt durch neue Technologien, verorteten *Machtasymmetrien* zwischen Verarbeitenden – ungeachtet der Frage, ob es öffentliche Stellen oder private Personen sind – liegt die Begründung für den Transfer des Verhältnismässigkeitsprinzips vom öffentlichen Bereich in den privaten Bereich. Der Grundsatz wird datenschutzrechtlich konsequent ebenso für den Bereich der privaten Datenbearbeitung analog der öffentlich-rechtlichen Struktur – Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne – interpretiert.[769] Insofern liesse sich von einer *monistischen Interpretation* sprechen. Ob der Verhältnismässigkeitsgrundsatz im *Lichte des Dualismus* für die beiden Bereiche gemäss DSG und nDSG datenschutzrechtlich *unter-*

765 Vgl. Riemer, § 5 N 14; vgl. BGE 125 II 275, E 2.c., wonach «der formalen Rechtsordnung eine ethisch materielle Schranke» gesetzt wird, wo «durch die Betätigung eines behaupteten Rechts offenbares Unrecht geschaffen würde», vgl. BBl 1904 IV 14.

766 Insofern sei auf die zivilrechtliche Kommentarliteratur und die einschlägige Rechtsprechung verwiesen.

767 Beschränkungen des persönlichen Verkehrs beispielsweise haben verhältnismässig in dem Sinne zu sein, dass sie geeignet und erforderlich sind, um das Kindeswohl zu schützen, Art. 273 ZGB; Michel, KuKo-ZGB, Art. 273 N 19; allgemein Cottier, KuKo-ZGB, Vor Art. 307–317, N 7.

768 Vgl. Urteil des EuGH, C-441/07 P, Urteil vom 29. Juni 2019 – Alrosa.

769 Vgl. BBl 1988 II 414 ff., 450; Rosenthal, HK-DSG, Art. 4 N 19 ff.; Rampini, BSK-DSG, Art. 4 N 9, mit Hinweis in N 10 auf die Partikularität der Übernahme dieses öffentlich-rechtlichen Grundsatzes im Bundeszivilrecht.

schiedlich zu interpretieren sei, wurde bislang nicht grundlegend diskutiert.[770] Die Ansicht, wonach der Inhalt des Verhältnismässigkeitsprinzips in seiner gemeinsamen Verankerung in Treu und Glauben für den privaten Bereich im Sinne des Rechtsmissbrauchs zu lesen wäre, wird – soweit ersichtlich – nicht vertreten. Vielmehr wird das Verhältnismässigkeitsprinzip identisch für den privaten Bereich wie für den öffentlichen Bereich interpretiert, und zwar, wie gezeigt, im Sinne des öffentlich-rechtlichen Prinzips. Damit trägt das DSG – trotz seines Dualismus – dem Aspekt der *Beziehungsasymmetrie im Kontext der Personendatenverarbeitung Rechnung*. Indem auch für Datenverarbeitungen durch Private verlangt wird, dass ihre Handlungen geeignet sein müssen, um den vordefinierten Verarbeitungszweck zu erreichen, trägt man der *Machtasymmetrie* zwischen datenverarbeitenden Unternehmen und privaten Datensubjekten Rechnung.[771]

521 Ein Machtungleichgewicht zwischen den personendatenverarbeitenden Verantwortlichen und den Datensubjekten im privaten Bereich dürfte heute kaum mehr ernsthaft bestritten werden. Nichtsdestotrotz *variieren* die aus einem solchen Befund gezogenen rechtlichen *Schlussfolgerungen*.

522 Für die *Schweiz* wurden diese namentlich bereits im IV. Kapitel dieses zweiten Teils, der den Dualismus des eidgenössischen Datenschutzgesetzes darstellt, herausgearbeitet. Mit der Totalrevision wird an dem Dualismus festgehalten. Gleichwohl ist eine Vereinheitlichung dergestalt zu verzeichnen, dass die gemeinsam für beide Bereiche geltenden Anforderungen und neuen Instrumente ausgebaut werden.

523 Anders lautet die Antwort vonseiten der *EU mit der DSGVO*: Der Machtasymmetrie, der das Datensubjekt sowohl in seiner Beziehung zu privaten als auch zu öffentlichen Verarbeitenden ausgesetzt ist, wird mit der Implementierung eines monistischen Ansatzes entgegengetreten. Dieser Monismus sieht identische Regeln für Personendatenverarbeitungen durch Private und öffentliche Stellen vor. Der Übergang zu einem monistischen Modell, den die DSGVO vollzieht, markiert einen datenschutzrechtlichen *Paradigmenwechsel*.[772] In Deutschland wurde der Ansatz bereits einige Jahre zuvor debattiert.[773] Im Zusammenhang mit dem *Verhältnismässigkeitsgrundsatz* ist nicht nur das für beide Bereiche geltende grundsätzliche Verarbeitungsverbot gemäss Art. 6 DSGVO relevant. Einschlägig ist zudem der sog. Grundsatz der Datenminimierung gemäss Art. 5 lit. c DSGVO.

770 Für eine Ausdifferenzierung im Einzelfall tritt Epiney, in: Belser/Epiney/Waldmann (Hrsg.), 530, ein.

771 Vgl. insofern Buchner, 26 ff., insb. 28; zur Problematik der Machtasymmetrie im Vertragsrecht und den Reaktionen vonseiten des Rechts und der Rechtsprechung Derleder, in: Jestaedt/Lepsius (Hrsg.), 234 ff., 236 f.

772 Hierzu Pfaffinger, Vortrag vom 31. Januar 2019, Deloitte Zürich. Die Schweiz weicht im Zuge der Totalrevision des DSG nicht von ihrem dualistischen System ab.

773 Vgl. Buchner, 26 ff.

Ein *prinzipielles Verarbeitungsverbot* ist *das einflussreichste Instrument*, um die Datenminimierung zu implementieren. Gleichwohl wurde eine *Vereinheitlichung datenschutzrechtlicher Vorgaben* wegen einer parallel für den privaten und öffentlichen Bereich gedachten Beziehungsasymmetrie bereits vor der Ära der DSGVO selbst in Deutschland namentlich von Vesting und Buchner kritisch beleuchtet: Vesting legt die Ausrichtung und Orientierung einer vereinheitlichenden Datenschutzgesetzgebung an einem staatszentrierten Leitbild frei, in welchem er das Datenschutzrecht tief verhaftet sieht. Er weist auf die Schwächen des Vergleichs sowie des Transfers von Leitbildern vom öffentlich-rechtlichen in den privatrechtlichen Kontext hin. Ebendieser Transferprozess wurde gerade auch von der Rechtsprechung des Bundesverfassungsgerichts angeleitet.[774] Ähnlich kommt Buchner zu dem Schluss, dass sich die *Gefährdungslagen nicht* vergleichen lassen, zumal der Staat auf einen Zwangsapparat zur Durchsetzung seiner Ansprüche zurückgreifen kann.[775] Er plädiert für ein konsequent dem *privaten Interessenausgleich verpflichtetes Datenschutzrecht* für den privaten Sektor, dessen Ausgangspunkt ein Recht auf informationelle Selbstbestimmung sei.

524 Für die *Schweiz* nun lässt sich im Rahmen einer Analyse des Verhältnismässigkeitsprinzips und der Vorgabe der Datenminimierung im DSG eine bemerkenswerte Differenziertheit attestieren. Mit dem Dualismus und dem Ausgangspunkt der Verarbeitungsfreiheit mit Schranken für den privaten Bereich wird ausgedrückt, dass datenschutzrechtlich die Beziehung zwischen Datensubjekt und verarbeitenden öffentlichen Stellen gegenüber jener zwischen Privaten unter dem Aspekt der Machtasymmetrie *nicht identisch* gedacht wird. Gleichwohl wird die *Machtasymmetrie* auch in den gesellschaftlichen Beziehungen anerkannt, indem das Prinzip der Verhältnismässigkeit mit seinem im öffentlichen Recht geprägten Inhalt importiert wird. Ein solcher Transport eines Prinzips, das seinen Ursprung im öffentlichen Recht hat, in den privaten Sektor ist im Zusammenhang der Personendatenverarbeitung durchaus *sachgerecht*. Im *öffentlichen Bereich* erfolgt die Datenminimierung *doppelstufig: erstens* über das allgemeine Verarbeitungsverbot mit Ausnahmen gemäss Art. 17 DSG resp. Art. 33 nDSG und *zweitens* über das Verhältnismässigkeitsprinzip gemäss Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG in seiner öffentlich-rechtlichen Tradition und Trias. Für den *privaten Bereich* wird die Datenminimierung *einstufig* implementiert: Das Verhältnismässigkeitsprinzip mit seiner Trias der Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne setzt der prinzipiellen Verarbeitungsfreiheit im privaten Bereich eine recht konkrete und einschneidende Schranke. Der Verarbeitungsgrundsatz der Verhältnismässigkeit formuliert gegenüber privaten Verantwortlichen *präzise Handlungsanleitungen*. Die Datenverarbeitenden werden in

774 Vesting, in: Ladeur (Hrsg.), 155 ff.
775 Vgl. Buchner, 64 ff., 80 ff.

die Pflicht genommen, ihre Personendatenverarbeitungen auf ihre Eignung und Erforderlichkeit hin zu überprüfen. In dieser Zweck-Mittel-Relation markiert der Grundsatz der Verhältnismässigkeit die Grenze zwischen zulässiger und unzulässiger Datenverarbeitung.

525 In die Kritik, wonach das Verhältnismässigkeitsprinzip der grosse «Gleich- und Weichmacher» ist, der zur Auflösung des «sicheren Rechts in ein allgemeines Werten und Wägen führt»,[776] sollte im datenschutzrechtlichen Zusammenhang nicht eingestimmt werden. Mit diesem über das Verhältnismässigkeitsprinzip in der Schweiz weiter ausdifferenzierten Mechanismus wird die Dichotomie von öffentlich und privat aufgeweicht, aber keineswegs aufgegeben. Denn für den öffentlichen Bereich ist vorgeschaltet das Legalitätsprinzip zu beachten, vgl. datenschutzgesetzlich Art. 17 DSG resp. Art. 33 nDSG. Entsprechend ist es der Gesetz- oder Verordnungsgeber, der das zu verfolgende öffentliche Interesse, an das die Bearbeitungszwecke gekoppelt sind, *vordefiniert*.

526 Ein zusätzlicher Differenzierungsaspekt findet sich im DSG wie folgt: Unverhältnismässige Datenbearbeitungen im privaten Sektor können gerechtfertigt werden, nicht aber im öffentlichen Bereich.[777] Zur Rechtfertigung eines Verstosses gegen das Verhältnismässigkeitsprinzip kommen im privaten Bereich namentlich Gesetz und Einwilligung in Frage.[778] Die Koordinierung des Verarbeitungsgrundsatzes der Verhältnismässigkeit i. S. v. Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2 nDSG mit dem Rechtfertigungsgrund des überwiegenden privaten oder öffentlichen Interesses, vgl. Art. 13 Abs. 1 und Abs. 2 DSG resp. Art. 31 Abs. 1 und Abs. 2 nDSG, fällt schwer. Insofern wird die Meinung vertreten, dass die Abwägungen von Art. 4 Abs. 2 und Art. 13 Abs. 1, Abs. 2 DSG zusammenfallen: Ist eine Datenbearbeitung unverhältnismässig, könne sie nicht durch ein überwiegendes Interesse nach Art. 13 DSG gerechtfertigt werden. Eine unverhältnismässige Datenbearbeitung i. S. v. Art. 4 Abs. 2 DSG sei widerrechtlich, es sei denn, es läge eine Einwilligung oder gesetzliche Grundlage vor.[779] In dieser Interpretation fallen Tatbestandsmässigkeit und (Nicht-)Rechtfertigung, was das Thema der Interessenabwägungen anbelangt, punktuell zusammen.

527 Ebendieser Auslegungsvorschlag vermag nicht zu überzeugen. Vielmehr verfolgt der Verhältnismässigkeitsgrundsatz gemäss Art. 4 Abs. 2 DSG resp. Art. 6 Abs. 2

776 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 276 ff., 277; insofern auch Ladeur, Kritik.

777 Rosenthal, HK-DSG, Art. 4 N 19, der unter N 28 f. für die Rechtfertigungsmöglichkeit des verletzten Verhältnismässigkeitsgrundsatzes eintritt. Er begründet dies ebenso mit unterschiedlichen Funktionen des Grundsatzes sowie der Rechtfertigungsgründe.

778 Immerhin ist darauf hinzuweisen, dass die Einwilligungsmöglichkeit eingeschränkt werden kann, was namentlich über Art. 328b OR von Relevanz ist. Aufgrund der spezifischen Machtasymmetrie gilt die Einwilligung im arbeitsrechtlichen Kontext als kritisch.

779 So Epiney/Civitella/Zbinden, 24; strenger vertritt Peter, 134, dass eine Einwilligung in eine unverhältnismässige Personendatenverarbeitung nicht möglich sein soll.

nDSG als Verarbeitungsgrundsatz eine andere Stossrichtung, als sie die Interessenabwägung im Rahmen der Rechtfertigung aufweist. Die Verletzung des Verhältnismässigkeitsprinzips markiert für den privaten Bereich einen Tatbestand der Persönlichkeitsverletzung, vgl. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Die Rechtfertigung gemäss Art. 13 Abs. 1 und Abs. 2 DSG resp. Art. 31 Abs. 1 und Abs. 2 nDSG infolge überwiegender Interessen hat eine andere Ausrichtung. Während es bei der Verhältnismässigkeit als Verarbeitungsgrundsatz um die Relation zwischen Verarbeitungszweck und Verarbeitungshandlung geht, geht es bei den überwiegenden Interessen im Rahmen der Rechtfertigungsgründe um die Interessenabwägung zwischen den Parteien, den Datenverarbeitenden («Verantwortliche») und den Datensubjekten.[780] Man stellt mithin die ggf. gegenläufigen Interessen von Datenbearbeitenden und Datensubjekten einander abwägend gegenüber. Es mag richtig sein, dass bei einer Verletzung der «Mittel-Zweck-Relation» solche überwiegenden Interessen nur ganz selten angenommen werden können. Das mit dem Verhältnismässigkeitsprinzip unweigerlich assoziierte Abwägungsparadigma bleibt damit bestehen; allerdings wird es aufgrund der vorangehenden Eignungs- und Erforderlichkeitsprüfung in einen engen Rahmen verwiesen.[781]

528 *Zusammenfassend:* Die Vorgabe, wonach Personendatenverarbeitungen geeignet und erforderlich für die Zweckerreichung sowie verhältnismässig im engeren Sinne sein müssen, bildet *für den privaten Bereich* die konkreteste und engste Schranke der prinzipiellen Verarbeitungsfreiheit. Mit dem Import eines im öffentlich-rechtlichen Verständnis definierten Verhältnismässigkeitsprinzips wird dem Befund Rechnung getragen, wonach auch in gesellschaftlichen Beziehungen im Umgang mit Personendaten *Machtasymmetrien* zwischen Datensubjekten und Verarbeitenden bestehen. Insofern wird die Vorstellung von der «Reinheit» des privaten Bereiches und des im ersten Kapitel beschriebenen Dualismus relativiert. Die für beide Bereiche im Kontext der Personendatenverarbeitung anerkannte Machtasymmetrie wird nach schweizerischem DSG indes nicht synchron gedacht: Für den öffentlichen Bereich wird das grundsätzliche Verarbeitungsverbot vorgeschaltet, was ein klares Gebot der Minimierung von Personendatenverarbeitungen markiert; ebendieses wird alsdann in einem zweiten Schritt durch den Verarbeitungsgrundsatz der Verhältnismässigkeit weiter umgesetzt. Die hier etablierte *Trias* von Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne soll gleichermassen für den öffentlichen wie den privaten Bereich gelten. Nimmt man für den Bereich der privaten Datenverarbeitung die Verhält-

780 Ausdrücklich hierzu Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.76; ähnlicher Ansicht wohl auch Rosenthal, HK-DSG, Art. 4 DSG N 28.

781 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 276 ff., 277; zum Verhältnismässigkeitsprinzip im Rahmen der Bearbeitung von Personendaten auch Glass, 55 ff.

nismässigkeit im Sinne der Eignungs- und Erforderlichkeitsprüfung ernst, dann wird dem beklagten Risiko «willkürlicher, irrationaler» Entscheidungen viel von seiner Sprengkraft genommen.[782] Wenn sich die Verhältnismässigkeit als gemeinsamer Verarbeitungsgrundsatz auf die Mittel-Zweck-Relation konzentriert, dann gewinnen die jeweiligen Verarbeitungszusammenhänge beträchtliche Bedeutung. Im Verhältnismässigkeitsprinzip zeigt sich erneut mit Deutlichkeit die Relevanz, ob und inwiefern das Datenschutzrecht für die Personendatenverarbeitung durch Private resp. öffentliche Stellen identisch, vereinheitlichend oder ausdifferenziert gestaltet werden soll. Das DSG sieht hierbei, wie dargelegt, auch wenn es die Verhältnismässigkeit als Verarbeitungsprinzip für beide Bereiche in seiner öffentlichrechtlichen Gestalt vorsieht, ein beachtliches Mass an Differenzierung vor. Wie relevant die Berücksichtigung des Verarbeitungskontextes für die datenschutzrechtliche Normierung ist, zeigt sich in markanter Weise in dem Grundsatz. Das DSG zeigt eindrücklich, dass die Machtasymmetrie der Beziehung, wie sie für beide Bereiche gesehen wird, durch den Transport des Verhältnismässigkeitsprinzips in den privaten Bereich anerkannt wird. Sogleich aber werden die Spezifika der Bereiche, wie sie sich auch im Dualismus ausdrücken, via die Gewährleistung anderer, ausdifferenzierender Mechanismen geschützt. Der Argumentationsfaden ist: Machtasymmetrie in beiden Bereichen ja, Legitimation der Gültigkeit des Verhältnismässigkeitsprinzips in seiner öffentlichen Trias-Konzeption ja, gleichwohl weitere Anerkennung der Differenzierungswürdigkeit, selbst über Instrumente, die mit dem Verhältnismässigkeitsprinzip im Zusammenhang stehen.

Die datenschutzrechtliche Relevanz des Verarbeitungskontextes wird sodann 529
über die «Gegenspieler» von den untrennbar mit dem Verhältnismässigkeitsprinzip verbundenen Löschungspflichten und -ansprüchen, vgl. neu auch Art. 6 Abs. 4 nDSG sowie spezialgesetzliche Aufbewahrungs- und Archivierungspflichten, sichtbar. Die Relevanz kontextueller Bezüge für das Datenschutzrecht, mit der eine Abwägung individueller Interessen für den Einzelfall in den Hintergrund rückt, wird vertiefend im Rahmen der zweckgebundenen Verarbeitungsgrundsätze analysiert.

3.2. Faktische Herausforderungen und rechtliche Entwicklungen

Das Verhältnismässigkeitsprinzip wird insb. vom Phänomen «Big Data» auf eine 530
harte Probe gestellt. Auch in der Schweiz ist Big Data weder aus der öffentlichen Verwaltung noch aus dem privaten Sektor wegzudenken. Den unter diesem

782 Von Arnauld, in: Jestaedt/Lepsius (Hrsg.), 276 ff., 279.

Schlagwort eingefangenen Praktiken kommt nicht nur in der Praxis, sondern auch im Schrifttum grosse Aufmerksamkeit zu.[783]

531 Der Einsatz von Big-Data-Analysen gilt z. B. als wirksames Instrument zur Bekämpfung von Staus im Strassenverkehr. Staus verursachen enorme Kosten. Der wohl häufigste Einsatz von Big-Data-Analysen findet bei der Verkehrsplanung und -steuerung durch staatliche Behörden statt. So nutzt das Bundesamt für Strassen (Astra) Big Data, um Stauprognosen und dem Verkehrsfluss angepasste Tempo-Limits zu generieren. Hierfür kommen Videosensoren und eine Datenbasis der Swisscom mit (anonymisierten) Positionsdaten der Mobiltelefone von Swisscom-Kunden zum Einsatz. Darauf basierend lässt sich eruieren, wo der Strassenverkehr mit welcher Geschwindigkeit fliesst. Auf diesem Weg werden Staus und Stautendenzen frühzeitig erkannt; Navigationssysteme können Daten nutzen, um die Nutzerinnen und Nutzer auf Alternativrouten aufmerksam zu machen. Die Stauregulierung und -prävention ist nicht nur aus umweltschützerischen Gründen, sondern auch aus wirtschaftlichen Erwägungen interessant: Volkswirtschaftlich verursachen Staus nach Berechnungen des Bundesamts für Raumentwicklung und des Bundesamts für Strassen jährlich Kosten in der Höhe von gegen zwei Milliarden Franken.[784]

532 Ein weiteres Einsatzfeld findet Big Data im Bereich «öffentliche Sicherheit». Ein Beispiel wird in der NZZ vom 22. Dezember 2015 unter dem Titel «Kommissar Kristallkugel» dargestellt.[785] Wie kaum ein Verbrechen hat der Vierfachmord von Rupperswil am 21. Dezember 2015 die Schweiz erschüttert. Erst im Juni 2016 konnte der Zugriff auf den Täter erfolgen, wobei neben dem Fingerabdruck und der DNA-Analyse das Schlüsselinstrument zur Aufklärung der Tat die akribische Auswertung von Handydaten war. So wurden die Registrierungen über die Antennen in unmittelbarer Umgebung zum Tatort untersucht: Jedes eingeschaltete Handy loggt sich, sobald dessen Träger sich in der Nähe der entsprechenden Antenne befindet, in diese ein. Anschliessend konnte anhand einer riesigen Menge von Handydaten, die über die Antenne gesammelt wurden, ermittelt werden, wer zum relevanten Zeitpunkt in der Umgebung des Tatortes war. Die Auswertung

783 Culik/Döpke, ZD 2017, 226 ff.; Hoeren, Int. J. Law Inf. Technol. 2017, 26 ff.; Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff.; sodann die Beiträge in Kalyvas/Michael (ed.); Weber/Thouvenin (Hrsg.) und Fasel/Meier (Hrsg.); Epiney, Jusletter IT vom 21. Mai 2015; unlängst hierzu auch Heuberger, N 31 ff.; zu Big Data Analytics Baeriswyl, in: Weber/Thouvenin (Hrsg.), 45 ff.; Mayer-Schönberger/Cukier, *passim*; eine kursorische Analyse führt Prieur, AJP 2015, 1643 ff. zu dem Schluss, dass sich Big-Data-Unternehmen, die im Internet und über soziale Plattformen Personendaten zusammentragen und auswerten, um das Datenschutzrecht foutieren; vgl. zu den datenschutzrechtlichen Herausforderungen am Beispiel von Big Data Burkert, in: Epiney/Fasnacht/Blaser (Hrsg.), 1 ff.; de Werra, RSDA 2020, 365 ff.

784 Vgl. Tagesanzeiger, So viel kosten Staus auf Schweizer Strassen, Zürich 2018, <https://www.tagesanzeiger.ch/schweiz/standard/so-viel-kosten-staus-auf-schweizer-strassen/story/21144070> (zuletzt besucht am 30. April 2021).

785 Przybilla, NZZ vom 22. Dezember 2015.

wurde polizeilich nach einem Gesuch der Staatsanwaltschaft an die Swisscom vorgenommen.[786]

In Zürich setzt die Stadtpolizei seit November 2013 auf die Prognosesoftware Precobs (Precrime Observation System).[787] In das Programm werden ermittlungstechnische Daten von bereits begangenen Einbrüchen wie der Tatort, die Tatzeit, Beute und Vorgehensweise eingegeben. In der Folge macht sich die Software eine Erkenntnis aus der Kriminologie zunutze: Auch professionelle Einbrecher haben ihre jeweils eigene Handschrift, die Delikte werden nach bestimmten Mustern begangen. Darauf basierend erstellt ein Software-Programm Prognosen hinsichtlich unmittelbar zu erwartender Folgeeinbrüche. Entsprechend lässt sich z. B. eine Erhöhung der Polizeipräsenz planen. 533

Big-Data-Analysen kommen sodann im Versicherungswesen zur Anwendung: Unfall- und Krankenversicherungen müssen pro Jahr Millionen von Arzt- und Spitalrechnungen kontrollieren, was eine finanzielle und bürokratische Herausforderung darstellt.[788] Um diese Arbeit zu bewältigen, setzen Schweizer Versicherer wie die Suva bereits heute auf Big Data.[789] Millionen von Rechnungsdaten können mithilfe einer Software kontrolliert werden. Die Software kann feststellen, ob eine Konsultation richtig verrechnet oder ob der Ansatz für Schmerzmittel eingehalten wurde. Der Einzelfall wird durch das Programm mit tausenden ähnlich gelagerten Fällen verglichen, wobei beispielsweise Medikamente als auffällig eingestuft werden, die in einem solchen Fall für gewöhnlich nicht verschrieben werden. Durch die Nutzung von Big Data kann allein die Suva jährlich CHF 200'000'000.00 einsparen. 534

Die Einsatzmöglichkeiten von Big Data erscheinen alle sehr nützlich – Staus umfahren, Verbrechen bekämpfen, Unfälle verhindern, vor Versicherungsbetrug und Kreditkartenmissbrauch schützen, effizientere Markt- und Konsumbeziehungen aufbauen sowie pflegen. Die Einsatzbereiche von Big-Data-Analysen erstrecken sich damit über weite Felder.[790] 535

786 In diesem Zusammenhang ist das neue BÜPF zu erwähnen, vgl. <https://www.ejpd.admin.ch/ejpd/de/home/aktuell/meldungen/2017/vuepf-faq.html> (zuletzt besucht am 30. April 2021).

787 Vgl. Institut für musterbasierte Prognosetechnik Verwaltungs-GmbH, Pre-crime observation system, Bern 2016, <https://www.swisspoliceict.ch/getattachment/04e4ca1a-cf03-4c89-973d-a822cb7e7539/.aspx> (zuletzt besucht am 30. April 2021); zum Predictive Policing in der Schweiz und Precobs Camavdic, Jusletter IT vom 26. September 2019, N 1 ff., insb. N 4; zur rechtsstaatlichen Verarbeitung von Personendaten im Bereich der Polizei Glass, 244 ff.

788 Eindrücklich mit Blick auf Personendatenflüsse, wie sie innerhalb von Spitälern, aber auch nach aussen zwecks Forschung, Abwicklung von Sozialversicherungsleistungen oder zu Bundesbehörden erfolgen, Gogniat, Jusletter vom 20. Juni 2016, N 35 ff.

789 Vgl. hierzu NZZ vom 8. März 2016 – Suva schöpft Kraft aus Big Data, abrufbar unter: <https://www.nzz.ch/wirtschaft/suva-schoepft-kraft-aus-big-data-1.18708611?reduced=true> (zuletzt besucht am 30. April 2021).

790 Bereits an der Jahrtausendwende wurden Personendaten in unzähligen Bereichen gesammelt; vgl. hierzu den Überblick bei Eckhardt/Fattebert/Keel/Meyer, 17 ff.; vgl. zu den Anwendungsberei-

536 Was aber ist Big Data? So vielfältig die Beispiele daherkommen, so vielfältig sind auch die vorgeschlagenen Definitionen.[791] Regelmässig wird Big Data anhand von vier resp. fünf Charakteristika definiert. Varianten finden sich auch hier. Als definitionsrelevant gelten die sog. «vier resp. fünf Vs»: *Volume*, *Velocity*, *Variety*, *Veracity* und *Value*.[792]

537 Zunächst beschreibt Big Data enorme Datenmengen – *Volume* –, die durch den technischen Fortschritt mit höchster Geschwindigkeit – *Velocity* – verarbeitet werden (Echtzeitsammlung).[793] Vielfältig ist die Beschaffenheit der Daten sowie der Quellen – *Variety* –, wobei an Audio- oder Videodateien, Tweets, Dokumente, Fotos zu denken ist, um nur einige Beispiele zu nennen, aber eben auch an Datenbestände, die in unterschiedlichen Systemen oder Kontexten gesammelt wurden. Mit *Veracity* wird die Korrektheit der Daten eingefangen. *Value* ist das Merkmal des (ökonomischen) Mehrwerts, der durch die Verarbeitung und Verknüpfung von Daten geschaffen wird.[794]

538 Durch die weiträumige Analyse von Einkaufsgewohnheiten von Konsumierenden kann beispielsweise Werbung individualisiert auf den Einzelnen zugeschnitten werden.[795] Damit einher geht die Monetarisierung von Daten, wobei die Kundschaft den Rohstoff selbst liefert. An dieser Stelle gewinnt die Dimension von Value – gerade auch für die Privatwirtschaft – einen besonderen Wert.[796]

539 Bei Banken kamen früher personenbezogene Daten der Klientel in erster Linie zur Kontoführung und – rudimentärer – zur Pflege der Kundenbeziehung zum Einsatz. Heute bieten die Banken Tools zur Erfassung von Auslagen an, die deren Einordnung nach Sport, Familie usf. ermöglichen. Das kann dazu dienen, spezifische Angebote, ggf. auch in Kooperation mit anderen Unternehmen, zu unterbreiten. Ein weiteres Beispiel zu Value ist die Registrierung von Kreditkartenbezügen: Mit der exakten Erfassung entsteht ein Bild über Kaufverhalten und

chen von Big-Data-Analysen auch Epiney, Jusletter IT vom 21. Mai 2015; zu Big Data mit den Risiken spezifisch für den Arbeitskontext Nebel, ZD 2018, 520 ff.

791 Vgl. auch Prieur, AJP 2015, 1644 ff.

792 Vgl. m. w. H. (ohne Value als Definitionselement) Wespi, in: Weber/Thouvenin (Hrsg.), 3 ff., 4 f.; zu den fünf Vs Meier, in: Meier/Fasel (Hrsg.), 5 ff.; vgl. zu Definitionen von Big Data auch Wenhold, 32 ff.; zur Korrelation von Volume sowie Value Odlyzko, Int. J. Commun. 2012, 920 ff.; zum Value, gerade von Daten im Internet, auch Cavoukian/Chibba/Williams/Ferguso, Jusletter IT vom 21. Mai 2015, N 7; zu den Begriffen von Big Data und Data Mining Cichocki, Jusletter IT vom 21. Mai 2015, N 4 ff.; vgl. auch die Beschreibung des Soziologen Coll, in: Epiney/Nüesch (Hrsg.), Separatum, 1 ff., 2 f.; als charakteristisch gilt insb. die Verknüpfung von Daten aus diversen Quellen; vgl. Epiney, Jusletter IT vom 21. Mai 2015, N 6; vgl. Fasel/Meier, in: Fasel/Meier (Hrsg.), 3 ff., 5 ff.

793 Hierzu m. w. H. auch Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 87; Mayer-Schönberger/Cukier, 11 f.

794 Meier, in: Meier/Fasel (Hrsg.), 37.

795 Zur personalisierten Werbung Auf der Mauer/Fehr-Bossard, in: Thouvenin/Weber (Hrsg.), ITSL 2017, 23 ff.

796 Vertiefend hierzu dritter Teil, VII. Kapitel, B.2.

Lokalität der Inhaberin. Verzeichnet das Kreditkartenunternehmen den Einsatz an einem überraschenden Ort oder deckt sich ein Konsumverhalten ganz und gar nicht mit den bisherigen Verhaltensweisen des Karteninhabers, geht man der Angelegenheit nach und interveniert. So können Kartenbetrüge verhindert oder rascher unter Kontrolle gebracht werden.

Der Begriff «Big Data» wird als «Phänomen» beschrieben.[797] Ein Phänomen, das mit Schlagworten von «Big Brother» über «Big is beautiful» bis zum «neuen Goldrausch» besetzt ist.[798] Realitätsnäher erfasst steht der Terminus eher für ein Paradigma denn eine Technologie, Methode oder Praxis.[799] 540

Big Data fordert das Datenschutzrecht und präziser die datenschutzrechtlichen Verarbeitungsgrundsätze heraus. Augenfällig ist dies nicht nur mit Blick auf das Verhältnismässigkeitsprinzip, verstanden als Datensparsamkeit. Big-Data-Analysen streben nach maximalen Datenbeständen. Der Analyseerfolg wird in Abhängigkeit von der Grösse der Datenmengen beurteilt.[800] Dies steht in einem scharfen Kontrast zum Verhältnismässigkeitsgrundsatz. Zugleich ist ein neuralgischer Punkt in der Mittel-Zweck-Relation sowie der Zweckbindung zu verorten. Denn der Pool von Personendaten für Big-Data-Analysen wird regelmässig aus diversen Quellen gespeist. Damit einher gehen meist auch Zweckänderungen.[801] Die Personendaten stammen oft aus diversen Quellen, wobei mit ihnen zahlreiche Zwecke verfolgt werden, die im Vorfeld meist nicht definiert sind. Werden sie potentiell an einen unbestimmt offenen Empfängerkreis weitergeleitet, stehen über das Verhältnismässigkeitsprinzip und das Verbot der Vorratsdatenspeicherung hinaus auch die Einhaltung von Transparenzvorgaben auf dem Spiel.[802] 541

An dieser Stelle geht es weniger darum, die Kollision von Big Data im Hinblick auf die datenschutzrechtlichen Vorgaben *de lege lata* abzuhandeln.[803] Dargestellt werden vielmehr die jüngsten rechtlichen Entwicklungen und die Weiterentwicklung von datenschutzrechtlichen Vorgaben. 542

Auf die zugleich produktiven wie auch disruptiven Folgen von Big-Data-Analysen bezog sich der Europarat mit «Guidelines on the protection of individuals 543

797 So Epiney, Jusletter IT vom 21. Mai 2015.
798 Cichocki, Jusletter IT vom 21. Mai 2015, N 1.
799 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 44 und 46.
800 Nissenbaum, 41 ff.
801 Hierzu Helbing, K&R 2015, 145 ff.
802 Vgl. Passadelis, Vortrag vom 13. April 2016, Universität Luzern.
803 Zu den Datenschutzrisiken von Big Data z. B. Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 92 ff. und insb. 106 ff.; dazu, dass das aktuelle Datenschutzrecht den Herausforderungen von Big Data nicht gewachsen ist, Cavoukian/Chibba/Williams/Ferguso, Jusletter IT vom 21. Mai 2015; als «contradiction manifeste» mit den datenschutzgesetzlichen Prinzipien wird Big Data beschrieben von Coll, in: Epiney/Nüesch (Hrsg.), Separatum, 1 ff., 9; Epiney, Jusletter IT vom 21. Mai 2015, N 9 ff.; eine kursorische rechtliche Reflexion von Big Data im Lichte des DSG findet sich auch bei Prieur, AJP 2015, 1644 ff., 1647 ff.

with regard to the processing of personal data in a world of Big Data».[804] Es handelt sich um Empfehlungen, welche die Bedeutung der *Zweckbindung* betonen. Sie halten fest, dass entsprechende Verfahren nicht zu einer Personendatenverarbeitung führen sollen, die für die Datensubjekte *unerwartet* ist sowie zu diversifizierten Risiken führt.[805] Die Empfehlungen weisen auf die Bedeutung *präventiver Massnahmen* hin. Dazu gehören die Risiko-Analysen sowie der Privacy-by-design-Ansatz.[806] Zudem wird das Instrument der Anonymisierung und die Notwendigkeit der Integration der Datensubjekte im Rahmen von automatisierten Entscheidungen aufgeführt.[807]

544 Entsprechende Instrumente finden sich ebenso in der DSGVO sowie in der Totalrevision des DSG: Anonymisierungsvorgaben, Anforderungen an die informierte Einwilligung sowie solche im Rahmen der automatisierten Entscheidungen, das Instrument der Datenschutz-Folgenabschätzung sowie «privacy by design and default» gelten gemäss dieser Rechtstexte.[808] Es handelt sich hierbei um Vorgaben und Instrumente, die auch, aber nicht nur, der Verwirklichung des Grundsatzes der Verhältnismässigkeit dienen.

545 Spezifisch für den Verhältnismässigkeitsgrundsatz hält die Totalrevision an der nicht überzeugenden Systematik fest, wonach die Verhältnismässigkeit mit Treu und Glauben in einem Absatz verankert wird, vgl. Art. 6 Abs. 2 nDSG. Er entspricht dem bisherigen Art. 4 Abs. 2 DSG. Allerdings finden sich Konkretisierungen mit Art. 6 Abs. 3 und Abs. 4 nDSG, welche die Korrelation zwischen dem Verhältnismässigkeitsprinzip und dem Verarbeitungszweck verdeutlichen. Abs. 4 konkretisiert die *zeitliche* Dimension der Verhältnismässigkeit, wonach Daten nicht beliebig lange mit ihrem Personenbezug gespeichert werden dürfen.[809] Neu lauten die Absätze:

> «[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.»
>
> «[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.»

546 Die gesetzgeberischen Anpassungen verdeutlichen, dass der Grundsatz der *Verhältnismässigkeit* dazu dient, die Eignung und Erforderlichkeit von Personenda-

804 Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data vom 23. Januar 2017, abrufbar unter: <https://rm.coe.int/16806ebe7a> (zuletzt besucht am 30. April 2021).
805 Vgl. Council of Europe, Guidelines, Ziff. 3.1.
806 Vgl. Council of Europe, Guidelines, Ziff. 2. und 4.
807 Vgl. Council of Europe, Guidelines, Ziff. 6. f.
808 Siehe Art. 4 Nr. 3–5, Art. 12., Art. 25 und Art. 35 f. DSGVO.
809 Vgl. zum Niedergang des Vergessens im Zuge der Digitalisierung und seiner Problematik Mayer-Schönberger, Delete, 64 ff.

tenverarbeitungen zu den damit anvisierten Zwecken zu gewährleisten. Offensichtlich weist der Verarbeitungsgrundsatz der Verhältnismässigkeit damit eine nähere Verbindung zu den *Zweckvorgaben* als zu Treu und Glauben auf. Neu wird zudem namentlich das zeitliche Element des Verhältnismässigkeitsprinzips ausgearbeitet, indem eine *Anonymisierung* resp. *Vernichtung resp. Löschung* verlangt wird, sobald die Erforderlichkeit nicht mehr gegeben ist. Betreffend die Vorgaben zur Löschung resp. Vernichtung ist auf das Recht der Betroffenen auf Löschung hinzuweisen, vgl. Art. 32 Abs. 2 lit. c nDSG, wobei dieses Betroffenenrecht nicht an Verhältnismässigkeitsvorgaben gebunden ist.

Auch die DSGVO widmet den *Löschungsvorgaben* und damit der zeitlichen Di- 547
mension von Personendatenverarbeitungen, namentlich der Speicherung, erhöhte Aufmerksamkeit: Den Betroffenen kommt gemäss Art. 17 DSGVO ein Recht auf Löschung zu, das unter dem Recht auf Vergessen in das kollektive Bewusstsein eingeht.[810] Die EU-Aufsichtsbehörden können den Anspruch autoritativ durchsetzen, vgl. Art. 58 lit. g DSGVO. Zudem geht die DSGVO vom grundsätzlichen Verbot der Personendatenverarbeitung und der Erforderlichkeit eines Rechtfertigungsgrundes für die Datenverarbeitung gemäss Art. 6 DSGVO aus, womit Personendatenverarbeitungen generell beschränkt und auf ein gerechtfertigtes Mass reduziert werden. Alsdann verankert Art. 5 lit. c DSGVO den Grundsatz der Datenminimierung, wonach Datenverarbeitungen in Korrelation zum verfolgten Zweck relevant, angemessen und auf das notwendige Mass beschränkt sein müssen. Ergänzend statuiert Art. 5 lit. e DSGVO eine Speicherbegrenzung dahingehend, dass Personendaten nur so lange in einer Form, welche die Identifizierung einer Person ermöglicht, gespeichert werden dürfen, wie dies zur Zweckerreichung erforderlich ist. Ist der Verarbeitungszweck erreicht worden und stehen keine Archivierungs- und Aufbewahrungspflichten entgegen, sind die Daten entweder zu löschen oder endgültig zu anonymisieren. Im Lichte der Vorgaben der DSGVO und namentlich von Art. 24 DSGVO empfiehlt es sich, ein eigentliches Löschkonzept zu entwickeln und entsprechende Vorgänge zu dokumentieren. Im

810 Löschungsvorgaben werden in der Schweiz durch weitere Bestimmungen umgesetzt werden, vgl. auch Art. 32 Abs. 2 lit. c nDSG; hierzu vertiefend Hunziker, 15 ff., auch kritisch zur Frage einer Utopie des Löschens und des dahinterstehenden Idealbildes der Kontrolle, 213 ff.; das Bild der Kontrolle ist auch im Konzept informationeller Selbstbestimmung mächtig, trifft indes auch ebenda auf Grenzen im Lichte digitaler Technologien; vgl. illustrativ hierzu z. B. Cavoukian, digma 2009, 20 ff., 20; zum Recht auf Speicherbegrenzung, zur Löschungspflicht resp. zum Recht auf Löschung gemäss DSGVO und zu den Begrifflichkeiten auch nach Schweizer DSG Rosenthal, digma 2019, 290 ff., 291 ff.; vgl. zur Bedeutung des Vergessens resp. Löschens im digitalen Zeitalter grundlegend Mayer-Schönberger, Delete, 10 ff., mit dem einleitenden Illustrationsbeispiel der betrunkenen Piratin: Einer jungen Frau, die Lehrerin werden wollte und sämtliche Prüfungen erfolgreich bestanden hatte, wurde der Zugang zum Beruf verweigert. Da sie im Internet ein Foto von sich selbst mit einem Piratenhütchen, einem Plastikbecher sowie den Worten «Drunken Pirate» hochgeladen hatte, wurde sie als nicht geeignet für den Lehrerinnenberuf beurteilt.

Rahmen der Löschungs- und Anonymisierungsprozesse kommt automatisierten und technischen Massnahmen eine wichtige Rolle zu.[811]

548 Die Umsetzung der Löschungs- aber auch Anonymisierungsvorgaben stellt die Verantwortlichen in der Praxis oftmals vor beträchtliche, auch technisch bedingte Schwierigkeiten.[812] Um den entsprechenden rechtlichen Anforderungen nachkommen zu können, bedarf es an erster Stelle der Kenntnis der Personendatenverarbeitungsprozesse in der Organisation mit ihren jeweiligen Zwecken. Basisinstrument ist bezüglich der Vorgaben gemäss Verhältnismässigkeitsprinzip, aber auch der Gewährleistung der Betroffenenrechte, das Inventar (sog. Verarbeitungsverzeichnis, vgl. Art. 30 DSGVO und Art. 12 nDSG). Hinsichtlich der Löschungsvorgaben und der Anonymisierung ist ein kritischer Hinweis angezeigt: Die Anonymisierung eliminiert ein Element für die Anwendbarkeit der Datenschutzgesetzgebung, den Personenbezug.[813] Folglich erscheint sie als eine attraktive Lösung für Big-Data-Analysen. Allerdings wurden Schwächen des Konzeptes freigelegt: Die Anonymisierung ist kaum je unangreifbar resp. so robust, dass der Personenbezug nicht wieder herstellbar wäre. Zudem eliminiert die «Anonymität» nicht die «Erreichbarkeit» der Subjekte, den «Zugriff» auf diese und in der Folge beispielsweise die Manipulierbarkeit.[814]

3.3. Resümee

549 Der Verarbeitungsgrundsatz der Verhältnismässigkeit wird in der Schweiz gemeinsam mit Treu und Glauben verbürgt, vgl. Art. 4 Abs. 2 resp. Art. 6 Abs. 2 nDSG. Neu widmet sich auch ein Art. 6 Abs. 4 nDSG dem zeitlichen Aspekt der Verhältnismässigkeit ausdrücklich.

550 Das Verhältnismässigkeitsprinzip wird für den privaten Bereich mit dem Inhalt der Eignung sowie Erforderlichkeit mit Blick auf den angestrebten Zweck sowie die Verhältnismässigkeit im engeren Sinne angewandt. Wird das Verhältnismässigkeitsprinzip als allgemeiner Datenverarbeitungsgrundsatz eingebettet betrachtet, zeigt sich, wie ausdifferenziert das datenschutzgesetzliche System der Schweiz ist.

551 Mit dem prinzipiellen Verarbeitungsverbot für den öffentlichen Bereich anerkennt es die Machtasymmetrie im Verhältnis Bürger und Staat. Dadurch wird auf einer ersten Stufe eine *Minimierung der Personendatenverarbeitung* erzielt.

811 Vgl. Art. 25 DSGVO; zum Verhältnis zwischen Regulierung und Technologie insb. auch Nissenbaum, Berkeley Tech. L.J. 2011, 1367 ff.; vgl. zur technischen Umsetzung von Löschungsvorgaben Hunziker, 118 ff.; vgl. Waidner/Karjoth, digma 2004, 18 ff., 19 f.

812 Zur Herausforderung der Datenlöschung mit Praxisbezügen Pisà, RR-COMP 2019, 8 ff.; Rosenthal, digma 2019, 290 ff., 290.

813 Vgl. Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 49 und 56 f.

814 Dies., in: Dies. (ed.), a. a. O.; m. w. H. Heuberger, N 77 ff.

Im Sinne einer zweiten Stufe greift im öffentlichen Bereich sodann das Verhältnismässigkeitsgebot als allgemeiner Verarbeitungsgrundsatz.

552 Der Aspekt der Machtasymmetrie im Zusammenhang von Personendatenverarbeitungen wird ebenso im *privaten Bereich* anerkannt, allerdings *einstufig:* Das Verhältnismässigkeitsprinzip wird nicht in Gestalt einer Rechtsmissbrauchsschranke interpretiert (was aufgrund der vereinten Regelung mit Treu und Glauben gefolgert werden könnte), stattdessen mit seinem «engen» öffentlich-rechtlichen Inhalt, der die Trias der Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne gleichermassen für den privaten Bereich verlangt. Das setzt der prinzipiellen Verarbeitungsfreiheit eine enge und griffige Schranke. Entsprechend kommt dem Verhältnismässigkeitsprinzip im privaten Bereich eine bedeutsame Rolle zu, Personendatenverarbeitungen zu limitieren.

553 Indem das DSG zwar einen Dualismus vorsieht, zugleich aber das Verhältnismässigkeitsprinzip für den privaten Bereich mit dem für den öffentlichen Bereich geltenden analogen Gehalt gilt, wird eine machtasymmetrische Beziehung im Kontext der Personendatenverarbeitung im privaten Bereich anerkannt. Diese Machtasymmetrie wird indes aufgrund des Dualismus für den privaten Bereich anders gedacht als für das Verhältnis zwischen Bürger und Staat. Damit hat sich gezeigt, dass der im IV. Kapitel beschriebene Dualismus nicht rein verwirklicht ist, sondern durch den Verhältnismässigkeitsgrundsatz punktuell korrigiert wird.

554 Die vorangehenden Ausführungen haben zudem sichtbar gemacht, dass mit den jüngsten datenschutzrechtlichen Entwicklungen durch mehrere Instrumente der Einhaltung des Verhältnismässigkeitsgrundsatzes in der Praxis Nachachtung verschafft werden soll. Zudem wird der Grundsatz selbst mit der Totalrevision weiter konkretisiert. Von zentraler Bedeutung ist die Korrelation zwischen Verhältnismässigkeit und Verarbeitungszweck, wobei auch die zeitliche Dimension ausdrücklicher adressiert wird, Art. 6 Abs. 3 und Abs. 4 nDSG. Werden Personendaten zur Erfüllung eines bestimmten Zweckes nicht mehr gebraucht, sind diese zu löschen oder zu anonymisieren. Löschungsvorgaben ist folglich nicht erst und nur bei Ausübung eines entsprechenden Betroffenenrechts nachzukommen. Vielmehr haben die Verantwortlichen Prozesse und Massnahmen zur Löschung und Anonymisierung im Rahmen der Datenschutz-Compliance zu implementieren. Hierbei ist allfälligen Archivierungs- und Aufbewahrungspflichten Rechnung zu tragen.[815]

555 Nachdem im Rahmen der Analyse zum Verhältnismässigkeitsprinzip die Bedeutung des Verarbeitungszweckes sichtbar wurde, ist nunmehr auf die datenschutzrechtlichen Zweckvorgaben einzugehen. Die Bedeutung des Verarbeitungszweckes zeigte sich in einer ersten Facette im Rahmen des Verhältnismässigkeitsprin-

815 Insofern empfiehlt sich für Unternehmen auch, entsprechende Retention-Policies zu erlassen.

zips: In der Schweiz wird dieses durch die Zweck-Mittel-Relation ebenso für den privaten Bereich anerkannt. Personendatenverarbeitungen müssen zur Erreichung des Zweckes geeignet und erforderlich sowie verhältnismässig im engeren Sinne sein. Trotz seiner gemeinschaftlichen Regelung in einem Absatz mit Treu und Glauben steht das Verhältnismässigkeitsprinzip somit in einem engen Konnex zum Verarbeitungszweck. Darin erschöpft sich aber seine Relevanz für die Datenschutznormierung nicht, wie die nachfolgenden Erörterungen zeigen.

4. Die Zweckvorgaben

4.1. Vorbemerkungen

4.1.1. Hypothese – Schlüssel zu den datenschutzrechtlichen Schutzzwecken

556 Die Zweckvorgaben spielen in verschiedener Hinsicht eine Schlüsselrolle im zeitgenössischen Datenschutzrecht. Sie sind zwischen den generalklauselartigen Verarbeitungsgrundsätzen, namentlich der Verhältnismässigkeit, und konkretisierten Bearbeitungsvorgaben angesiedelt, vgl. Art. 4 Abs. 3 DSG und Art. 6 Abs. 3 nDSG. Anhand der *Gebote im Zusammenhang mit dem Verarbeitungszweck* lässt sich zunächst die sukzessive Ausdifferenzierung nachzeichnen. Der Zweckbindungsgrundsatz ist weiter dazu geeignet, eine datenschutzrechtliche *Grundsatzfrage aufzuwerfen: Die Frage nach dem Zweck der Datenschutzregulierung*. Ansätze für die Antwort lassen sich in erster Linie anhand einer Analyse des Volkszählungsurteils des Bundesverfassungsgerichts mit seinen Erwägungen zur Zweckbindung generieren.

557 Den datenschutzgesetzlichen Zweckvorgaben kommt, wie zu zeigen sein wird, sowohl aus einer *materiellrechtlichen als auch aus einer prozeduralen und organisatorischen Perspektive* herausragende Bedeutung für den Datenschutz zu. Der Befund lässt sich neuerdings anhand der DSGVO und der Totalrevision des DSG bestätigen.

558 Unter dem Titel der Zweckvorgaben werden nachfolgend zuerst *seine anerkannten Teilgehalte* behandelt. Dazu gehören die initiale Zweckdefinierung resp. -fixierung, die Zwecktransparenz sowie die Zweckbindung. Anhand einer Analyse des Verarbeitungsgrundsatzes der Zweckbindung sollen die inhaltliche Bedeutung und die hohe Relevanz der Zweckvorgaben für das Datenschutzrecht freigelegt werden. Im Zentrum steht hierbei eine Auseinandersetzung mit dem mittlerweile in die Jahre gekommenen *Volkszählungsurteil des Bundesverfassungsgerichts*, dessen Argumentation gleichwohl nichts an seiner Aktualität eingebüsst

hat.[816] Bis heute geht die Nennung des Volkszählungsurteils untrennbar mit der ebenda erfolgten Anerkennung des Rechts auf informationelle Selbstbestimmung einher. Mit der informationellen Selbstbestimmung wird ein subjektives Recht assoziiert, wobei die Einwilligung des Datensubjektes eine zentrale Rolle spielt. Dieser Tage gelten Einwilligungskonstruktionen stärker denn je als «Patentrezept» zur Lösung datenschutzrechtlicher Herausforderungen.[817]

559 Die Aufmerksamkeit der anschliessenden Ausführungen allerdings richtet sich gerade nicht auf das *subjektive Recht auf informationelle Selbstbestimmung*, für dessen Anerkennung besagtes Urteil in die Rechtsgeschichte einging. Vielmehr soll eine *systemische Schutzdimension des Datenschutzrechts herausgearbeitet werden,* die im Urteil angelegt ist. Sie lässt sich anhand einer Analyse der bahnbrechenden Erwägungen zu den Zweckvorgaben erschliessen. Ebendiese *systemische Dimension des Urteils* blieb bislang – im Gegensatz zur stark beleuchteten *subjektiven Dimension des Rechts auf informationelle Selbstbestimmung* – weitgehend unterbeleuchtet. Eine Auseinandersetzung mit den Erwägungen des Bundesverfassungsgerichts zum Zweckbindungsgrundsatz erhellt indes, dass das Datenschutzrecht seit jeher als Instrument des Schutzes nicht nur von Individuen, sondern auch von Systemen und Kontexten gesehen wird.[818]

560 Die herausragende Bedeutung der *Zweckbindung* im und für das Datenschutzrecht wurde somit *gerichtlich vom Deutschen Bundesverfassungsgericht* in seinem berühmten Volkszählungsurteil aus dem Jahr 1983 herausgearbeitet. Es ist die *Fixierung des Verarbeitungszweckes auf die Statistik,* das Statistikgeheimnis, welche den Angelpunkt der Argumentation bildet. Das Statistikgeheimnis implementiert ein Verbot, die zum Zweck der Volkszählung erhobenen Personendaten dem *weiteren Verwaltungsvollzug* dienlich zu machen.[819]

561 Vonseiten der Wissenschaft wurde die Relevanz der Zweckbindung früh von Simitis mit den folgenden Worten anerkannt:

> «[D]ie unmissverständliche Forderung nach einer klaren Zweckbindung schränkt den Verarbeitungsradius von vornherein nachhaltig ein […].»[820]

816 Vgl. BverfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983.

817 Zum Recht auf Kontrolle der eigenen Personendaten vgl. Buchner, 207 und 230 f.; m. w. H. und kritisch Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 26; kritisch ebenso zu der dominanten Vorstellung, wonach ein Kontrollrecht an eigenen Daten die Lösung sei, Solove, Stan. L. Rev. 2001, 1393 ff., 1445 ff.; zum Recht an eigenen Daten vertiefend dritter Teil, VIII. Kapitel, B.

818 Richtungweisend hierzu Nissenbaum, *passim;* auf die Relevanz des Verarbeitungszusammenhanges hingewiesen hat früh Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 18, N 20; Ders., in: Schlemmer (Hrsg.), 67 ff., 74 f.; vgl. auch Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 29.

819 Vgl. BverfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 178. ff. und E 222. ff.

820 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 38.

562 In der schweizerischen Lehre und Rechtsprechung wird dem *Zweckbindungsgrundsatz* zumindest punktuell hohe Relevanz zugemessen.[821] Im Logistep-Urteil richtete das Bundesgericht den Fokus auf die (fehlende) *Transparenz des Bearbeitungszwecks*.[822] Die nachfolgenden Ausführungen beschreiben – nach einer Übersicht über die datenschutzrechtliche Positivierung – die rechtlich anerkannten Teilgehalte der zweckorientierten Datenschutzbestimmungen. Anschliessend wird vertiefend der Frage nach dem Schutzzweck des Datenschutzrechts nachgegangen.

4.1.2. Übersicht über die Positivierung

563 Die Kategorie des Verarbeitungszweckes zeigte sich bereits in seinem Zusammenspiel mit dem datenschutzrechtlichen Verarbeitungsgrundsatz der *Verhältnismässigkeit*. Die Vorgaben der Verhältnismässigkeit mit der Trias Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne richten sich am Verarbeitungszweck aus. Darüber hinaus sind in Bezug auf den Verarbeitungszweck *Transparenzvorgaben*, die sich auch, aber nicht nur auf diesen beziehen, einschlägig. Innerhalb der zweckbasierten Verarbeitungsvorgaben ist an vorab der *Grundsatz der Zweckbindung* relevant. Die Gebote der Zwecktransparenz wie Zweckbindung sind fester Bestandteil gesetzgeberischer Positivierungen und gerichtlicher Entscheidungen.

564 Vorgaben, die sich am Verarbeitungszweck orientieren – neben der Zweck-Mittel-Relation sind dies die Zwecktransparenz sowie die Zweckfixierung und -bindung –, sind frühe Elemente der Datenschutzregulierung. Sie bilden einen festen Bestandteil des Datenschutzrechts und finden sich im geltenden nationalen, europäischen, aber auch US-amerikanischen Datenschutzrecht.

565 In den USA wurde der Grundsatz bereits im Privacy Act von 1974 aufgenommen, der allerdings einzig Agenturen der Bundesregierung adressierte.[823] Zudem implementieren sektorielle Erlasse im privaten Bereich Vorgaben zu den Verarbeitungszwecken, so beispielhaft der Fair *Credit Reporting Act* und dessen § 604.

566 Die DSGVO statuiert Vorgaben im Zusammenhang mit dem Verarbeitungszweck innerhalb der allgemeinen Verarbeitungsgrundsätze, vgl. Art. 5 Abs. 1 lit. b–e DSGVO. Auch die Erlaubnistatbestände gemäss Art. 6 DSGVO, die festlegen, aufgrund welcher Tatbestände eine Verarbeitung von Personendaten rechtmässig ist, orientieren sich in massgeblicher Weise an Verarbeitungszwecken: So sind

821 Vgl. BGE 136 II 508, E 6.3.1.; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 13.
822 Gemäss derzeit noch in Kraft stehendem DSG genügt die Zweckerkennbarkeit, wobei allerdings mit den jüngsten Entwicklungen und im Zuge der DSGVO sowie der Totalrevision die Transparenzvorgaben markant angehoben werden.
823 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 38.

Personendatenverarbeitungen zwecks Vertragserfüllung nach Art. 6 Abs. 1 lit. b DSGVO oder zwecks Erfüllung rechtlicher Pflichten nach Art. 6 Abs. 1 lit. c DSGVO (beispielsweise zur Verhinderung von Geldwäscherei) rechtmässig.

Im geltenden schweizerischen Datenschutzgesetz kommt die Bedeutung, die dem Zweck als Instrument datenschutzrechtlicher Regulierung beigemessen wird, nicht zuletzt in dessen *dreifacher Thematisierung* zum Ausdruck: Neben seiner Relevanz im Rahmen des Verhältnismässigkeitsprinzips werden Vorgaben an den Verarbeitungszweck im DSG in Gestalt des Zweckbindungsgrundsatzes («Zweckidentität») in Art. 4 Abs. 3 DSG geregelt sowie an ein Transparenzgebot («Zweckerkennbarkeit») in Art. 4 Abs. 3, 4 DSG geknüpft. 567

Art. 4 Abs. 3 DSG lautet in seiner heute noch in Kraft stehenden Version: 568

> «Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.»

In Abs. 4 schliesst Art. 4 DSG die Vorgabe an: 569

> «Die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein.»

In diesen noch geltenden Fassungen enthalten Art. 4 Abs. 3 und 4 DSG mehrere *Teilgehalte*, wobei Meier in Abs. 3 einen *Dualismus* verortet: Der Absatz beinhalte den Grundsatz der *Zweckbestimmung* (an sich) sowie den Grundsatz der Unabänderlichkeit dieses zuvor festgelegten Zwecks der Datenbearbeitung, was ebenso mit dem Begriff der Zweckbindung resp. -fixierung erfasst wird.[824] Den engen Zusammenhang von Art. 4 Abs. 3 und Abs. 4 DSG betont Rosenthal, der die Erkennbarkeit des Zweckes weitestgehend und in überzeugender Weise unter Abs. 3 abhandelt, unter Abs. 4 indessen auf die *Erkennbarkeit der Beschaffung* fokussiert.[825] 570

Zwei Anmerkungen zur nicht geglückten Gesetzesredaktion, die mit der Totalrevision und insb. Art. 6 Abs. 3 nDSG ausgemerzt wird: 571

Erstens: Wird der hinreichend konkretisierte Verarbeitungszweck gegenüber dem Datensubjekt transparent gemacht, geht damit in aller Regel zugleich Transparenz hinsichtlich der Datenbeschaffung einher. Das separate Transparenzerfordernis betreffend die Datenbeschaffung verdeutlicht gleichwohl, dass dem Moment der Erhebung als «neuralgischem» Augenblick im Zyklus der Personendatenverarbeitung besondere Aufmerksamkeit zugemessen wird: Mit der Erhebung werden Personendaten in kaum mehr kontrollierbare Netze von Datenverarbeitungsflüssen eingespeist.[826] Sodann ist zwischen Art. 4 Abs. 3 und Abs. 4 DSG eine 572

824 Meier, N 722.
825 Zur Abgrenzung der beiden Absätze Rosenthal, HK-DSG, Art. 4 N 64.
826 Für Deutschland in den Worten von Scholz/Sokol, NomosKomm-BDSG, § 13 N 5: «In dem Moment, da Daten erhoben sind, hat das Datensubjekt weitgehend die Herrschaft über seine Daten ver-

Überlappung des Regelungsinhaltes hinsichtlich der Forderung festzustellen, wonach der Bearbeitungszweck im Zeitpunkt der Datenbeschaffung transparent zu machen ist.

573 Zweitens scheint der Gesetzgeber in Bezug auf den Zweck «interne resp. externe Pflichten» zu unterscheiden. Überzeugender allerdings wäre eine chronologische Systematisierung entlang des Verarbeitungszyklus: Zweckdefinierung nach innen, Transparenzmachung des bzw. der Verarbeitungszwecke nach aussen gegenüber dem Datensubjekt, Bindung der Verarbeitungshandlungen an diesen transparent gemachten Zwecken (nach innen, als eine Art Selbstverpflichtung). Die besagten zweckbasierten Vorgaben werden in Art. 4 Abs. 3 und Art. 4 DSG geregelt, wozu das allgemeine Transparenzgebot betreffend Datenbeschaffung tritt.

574 Im Einzelnen lassen sich nach DSG vor Totalrevision demnach *vier Inhalte aus Art. 4 Abs. 3 und Abs. 4 DSG* destillieren, die alle als Pflichten der datenverarbeitenden Verantwortlichen gestaltet sind: erstens die interne *Festlegung resp. Definierung* des Bearbeitungszwecks (Abs. 3). Sie ist Vorbedingung für die zweite Vorgabe, die *Zweckerkennbarkeit* resp. *Transparentmachung* des definierten Bearbeitungszwecks nach aussen (Abs. 3, *aber auch* Abs. 4). Drittens die *Bindung resp. Fixierung* an die definierten und transparent gemachten Verarbeitungszwecke im Rahmen der Datenverarbeitungen nach innen (Abs. 3), und viertens die Gewährleistung der Erkennbarkeit der Datenbeschaffung an sich (Abs. 4). Bei Zweckänderungen sind zudem Nachinformierungen erforderlich.

575 Die Totalrevision schafft eine systematische Bereinigung in Bezug auf die Regelungen der Zweckvorgaben. Diese werden in Art. 6 Abs. 3 nDSG gebündelt. Weiter sind Art. 6 Abs. 2 sowie Abs. 4 nDSG zu beachten.[827] Die Zweckvorgaben gemäss Art. 6 Abs. 3 und Abs. 4 nDSG lauten mit der Totalrevision des DSG wie folgt:

> «[3] Personendaten dürfen nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden; sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist.»
>
> «[4] Sie werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.»

loren.» Ebendem Rechnung tragend verbürgte das Deutsche Datenschutzgesetz in seiner Version i. K. bis zum 25. Mai 2018 den Grundsatz der Direkterhebung gem. in § 4 Abs. 2 BDSG, § 6 Abs. 1 lit. b BDSG – ein solcher Grundsatz war dem Eidgenössischen Datenschutzgesetz stets fremd.

827 EJPD, Erläuternder Bericht, 46.

4.2. Die zweckbasierten Verarbeitungsvorgaben – Teilgehalte

4.2.1. Zweckdefinierung resp. -fixierung

576 Der Verarbeitungszweck resp. die Verarbeitungszwecke müssen im Zeitpunkt der Verarbeitung und damit insb. auch der Beschaffung hinreichend konkret bestimmt sein, vgl. unmissverständlich Art. 6 Abs. 3 nDSG.

577 Unter noch geltendem DSG wird in an dieser Stelle das Verbot der *Vorratsdatenspeicherung* akzentuiert.[828] Die Vorratsdatenspeicherung ist prinzipiell unzulässig. Sie wird unter dem hier gewählten Untertitel resp. -begriff der Zweckfixierung (sowie dem Grundsatz der Verhältnismässigkeit) thematisiert: Nach dieser ist es unzulässig, Personendaten *ohne einen im Vorfeld bestimmten resp. definierten und fixierten Zweck* zu erheben. Eine «Blanko-Erhebung», eben auf Vorrat hin, um gesammelte Personendaten erst später zu jeweils ad hoc festgelegten Zwecken zu bearbeiten, ist nicht rechtens.[829] Der Verhinderung der sog. Vorratsdatenspeicherung dienen weiter die Transparenzvorgaben betreffend den Verarbeitungszweck. Bereits im Zeitpunkt der Beschaffung von Personendaten muss der Zweck, zu dem die Personendaten verarbeitet werden sollen, hinreichend präzis fixiert sein, um alsdann gegenüber dem Datensubjekt transparent gemacht zu werden, vgl. neben Art. 6 Abs. 3 nDSG auch Art. 19 Abs. 2 lit. b nDSG.

578 In Bezug auf eine dergestalt initiale Zweckfixierung ist auf Art. 5 Abs. 1 lit. b DSGVO hinzuweisen. Die Bestimmung verlangt, dass Personendatenverarbeitungen zu einem *vorab festgelegten*, für das Datensubjekt überschaubaren Zweck erfolgen müssen. Diese Anbindung muss für die Aufsichtsbehörde kontrollierbar sein.[830] Die «interne» Zweckfixierung hat hinreichend granular zu erfolgen, damit die Rechtmässigkeit der Verarbeitungshandlung überprüfbar wird. Bezüglich der Zweckfixierung sind keine Formerfordernisse vorgesehen. Immerhin müssen die Verarbeitungszwecke im Verarbeitungsverzeichnis, vgl. Art. 30 Abs. 1 lit. b DSGVO und Art. 12 Abs. 2 lit. b nDSG, aufgeführt werden. Zudem bildet der Verarbeitungszweck ein Element einer allfälligen Datenschutz-Folgenabschätzung, vgl. Art. 35 Abs. 7 lit. a DSGVO und Art. 22 Abs. 2 nDSG.

828 Vgl. Rosenthal, HK-DSG, Art. 4 N 31.
829 Vgl. Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.85; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 14.
830 Herbst, BeckKomm-DSGVO, Art. 5 N 22.

4.2.2. Zwecktransparenz

4.2.2.1. Gesetzliche Anforderungen

579 Die vorgängige «interne» Festlegung des Zweckes der Personendatenverarbeitung für bestimmte Personendaten ist sodann gegenüber den Datensubjekten *transparent* zu machen. Die von Personendatenverarbeitungen betroffenen Personen sollen wissen, wofür ihre Personendaten erhoben und verarbeitet werden.[831]

580 Das noch geltende *Erkennbarkeitsgebot* gemäss Art. 4 Abs. 4 DSG, das auch spezialgesetzlich verankert ist (vgl. für den Bereich der Privatversicherungen Art. 3 Abs. 1 lit. g und Art. 3a VVG) hat einen *doppelten Bezug*. Es verlangt erstens, dass die Beschaffung von Personendaten an sich erkennbar ist, und zweitens, dass der Bearbeitungszweck erkennbar ist. Ratio legis von Art. 4 Abs. 4 DSG ist die Erhöhung der Transparenz.[832] Mit der Totalrevision ist die Zwecktransparenz in Art. 6 Abs. 3 nDSG niedergelegt. In Art. 19 Abs. 2 lit. b nDSG findet sich eine explizite Informationspflicht über den Verarbeitungszweck bei der Beschaffung von Personendaten. Die Erkennbarkeit genügt nicht mehr, womit sich ebenso in diesem Punkt das mit der Totalrevision verfolgte Ziel der erhöhten Transparenz niederschlägt.

581 Das Transparenzgebot betreffend den Verarbeitungszweck beanspruchte bereits vor dessen ausdrücklicher Fixierung in Art. 4 Abs. 4 DSG Gültigkeit. Das Gebot der Erkennbarkeit von Beschaffung wie Bearbeitungszweck wurde – wie gezeigt – auch aus Treu und Glauben resp. – in der Terminologie der Europaratskonvention 108 oder derjenigen der EG-Richtlinie 95/46 – aus dem Loyalitätsgebot abgeleitet.[833] Der Ausbau der Transparenzvorgaben als Instrument datenschutzrechtlicher Regulierung lässt sich spezifisch mit Blick auf den Bearbeitungszweck nachzeichnen. In den ausgebauten Transparenzvorgaben hinsichtlich des Bearbeitungszwecks werden zwei Kernelemente zeitgemässer Datenschutzregulierung fusioniert: die Transparenz und der Zweck. Die *Transparenz hinsichtlich des Verarbeitungszweckes* bildet ein Kernanliegen des Datenschutzes.[834]

582 Anzugeben ist ein *korrekter* Zweck. Der Versuch, unter Vorspiegelung falscher Zielsetzungen an Daten zu gelangen, ist unzulässig.[835] Zudem müssen Bearbeitungszwecke hinreichend konkret umschrieben werden, um dem Transparenzge-

831 Peter, 126 f.; BBl 1988 II 414 ff., 451; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 13; vgl. Abschnitt 4.1.3. zur Zwecktransparenz.
832 Botschaft DSG 2003, 2101 ff., 2124.
833 Vgl. Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8; zum Ausbau von Transparenzvorgaben namentlich über Treu und Glauben vgl. zweiter Teil, V. Kapitel, B.2., insb. B.2.3.
834 Hannich/Jenni/Beerli/Mandl, in: ZHAW (Hrsg.), 45; zur Wichtigkeit dieses Grundsatzes BGE 136 II 508, E 6.3.1.
835 Vgl. Buchner m. w. H., 148.

bot zu genügen.[836] Mehrere Zwecke sind möglich, sofern jeder einzelne jeweils genügend granular umrissen wird.[837]

583 Gemäss Art. 4 Abs. 3 und Abs. 4 DSG muss die Beschaffung von Personendaten sowie der Verarbeitungszweck *erkennbar* sein. Nicht verlangt wird damit von Gesetzes wegen eine aktive oder schriftliche Informierung. Allerdings wird eine solche aus Beweisgründen regelmässig vorgenommen.[838] In Art. 4 Abs. 3 und Abs. 4 DSG werden unterschiedliche Wendungen eingesetzt, die folglich zu harmonisieren sind: Der bei der Datenbeschaffung erkennbare Zweck muss dem bei der Datenbearbeitung verfolgte Zweck entsprechen.[839] Immerhin: Mit der expliziten und separaten Vorgabe in Art. 4 Abs. 4 DSG, wonach der Zweck der Datenbearbeitung im Zeitpunkt der *Erhebung* erkennbar sein muss, symbolisiert der Gesetzgeber die Relevanz des Zeitpunktes der Datenerhebung und der insofern notwendigen Transparenz. Ebendies hat namentlich für den privaten Bereich Bedeutung, der gerade nicht von einem grundsätzlichen Verarbeitungsverbot ausgeht. Sobald personenbezogene Daten erhoben worden sind, verlieren Subjekte – Datenschutzgesetz und *behauptetem* Recht auf informationelle Selbstbestimmung zum Trotz[840] – weitgehend die Kontrolle über die sie betreffenden Angaben.[841]

584 Wenn das in Kraft stehende DSG zumindest für den privaten Bereich auf eine aktive Informationspflicht dem Grundsatz nach verzichtet, ist zweierlei hervorzuheben:

585 Erstens ist in Bezug auf das duale System und den öffentlichen Bereich die Gesetzesänderung aus dem Jahr 2010 in Erinnerung zu rufen. Mit dem BGG vom 19. März 2010 über die Umsetzung des Rahmenbeschlusses 2008/977/JI über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen wurden die Art. 18a und 18b ins DSG eingefügt. Art. 18a DSG verlangt, dass Bundesbehörden die betroffenen Personen über die Beschaffung und den Zweck der Verarbeitung der personenbezogenen Daten *zu*

836 Für eine normative Betrachtung tritt ein Rosenthal, HK-DSG, Art. 4 N 34; vgl. hierzu Art. 5 Abs. 1 lit. b DSGVO, wonach personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden müssen; zur hinreichenden Bestimmtheit vgl. Art. 29 Datenschutzgruppe WP 203, 16 mit Beispielen.

837 Vgl. implizit Rosenthal, HK-DSG, Art. 4 N 25; nach DSGVO Herbst, BeckKomm-DSGVO, Art. 5 N 36.

838 Vgl. auch Rosenthal, HK-DSG, Art. 4 N 36.

839 Was das Transparenzerfordernis bezüglich des Zwecks im Zeitpunkt der Datenbeschaffung anbelangt, geht Art. 4 Abs. 4 in Abs. 3 DSG auf. Zur synonymen Verwendung von *aus den Umständen* ersichtlich i. S. v. Abs. 3 und erkennbar i. S. v. Abs. 4 auch Rosenthal, HK-DSG, Art. 4 N 34. Die Datenbeschaffung ist bereits eine Datenbearbeitung. Der bei der Datenbeschaffung erkennbare Zweck von Art. 4 Abs. 4 DSG wird über Art. 4 Abs. 3 DSG perpetuiert. Eine Änderung des bei der Beschaffung erkennbar gemachten Zweckes ist grundsätzlich nicht zulässig.

840 EJPD, Bericht Bundesrat, 38 f.; BGE 140 I 2, E 9.1.

841 Vertiefend hierzu zweiter Teil, VI. Kapitel.

informieren haben. Ebendiese Pflicht gilt auch, wenn Daten bei Dritten beschafft werden. Sie beschränkt sich keineswegs auf die Verarbeitung personenbezogener Daten im Kontext der polizeilichen oder justiziellen Zusammenarbeit.[842] Immerhin kann die Informationspflicht gemäss Art. 18a Abs. 4 sowie Art. 18b DSG entfallen oder eingeschränkt sein. Denn Art. 18a DSG sieht gemäss der im Nachvollzug erfolgten Novellierung des Datenschutzgesetzes von 2010 dem Grundsatz nach für den öffentlichen Sektor eine Informationspflicht unabhängig von der Datenart vor.[843] Der Erkennbarkeitsgrundsatz gemäss Art. 4 Abs. 3 und Abs. 4 DSG ist somit im öffentlichen Bereich zur Ausnahme geworden, die Ausnahme zum Grundsatz.

586 Zweitens gilt für den privaten Bereich eine aktive Informationspflicht über den Verarbeitungszweck gemäss Art. 14 Abs. 2 lit. b DSG bei der Beschaffung *besonders schützenswerter Daten oder Persönlichkeitsprofile*, vgl. Art. 3 lit. c und lit. d DSG. Eine Verletzung der Informationspflicht kann gemäss Art. 34 Abs. 1 lit. a DSG strafrechtlich mit einer Busse in Höhe von bis zu CHF 10‘000.00 sanktioniert werden.

587 Folglich greift im noch geltenden DSG eine graduelle Abstufung der Transparenzvorgaben hinsichtlich den Verarbeitungszweck: Je umfassender, komplexer und längerfristiger die Bearbeitung, je sensibler die Daten, desto höher die Anforderungen an die Erkennbarkeit. Zu berücksichtigen sind weiter die Möglichkeiten des Datenbearbeiters und die Gepflogenheiten einer Branche.[844] Für eine eigentliche Informationspflicht wird im Anwendungsgebiet des Customer Relationship Management (CRM) plädiert:

> «Die Transparenz der Datenbearbeitung stellt ein fundamentales Prinzip des Datenschutzes dar. Aus datenschutzrechtlicher Sicht ist die Verwendung der Personendaten zu Werbe- und Direktmarketingzwecken insofern problematisch, als sie für die betroffenen Kunden zum Zeitpunkt, an dem deren Daten gesammelt werden, nicht ohne weiteres ersichtlich ist. Die Kunden müssten zum Datenschaffungszeitpunkt somit insofern informiert werden.»[845]

588 Folglich wird für Situationen, in denen Beschaffung und Zweck nicht resp. nicht eindeutig erkennbar sind, eine aktive Informationspflicht selbst ausserhalb von Art. 14 Abs. 2 lit. b DSG eingefordert.[846]

842 Taormina, BSK-DSG, Art. 18a N 1.
843 Zum Ganzen auch Meier, N 692 ff.
844 Ders., N 708.
845 Vgl. Passadelis, ZHAW (Hrsg.), 51; früh zu Marketing und Datenschutz die wirtschaftswissenschaftliche Dissertation von Schineis, *passim*.
846 Vgl. Rosenthal, HK-DSG, Art. 4 N 51 m. w. H. auf Erläuterungen des EDÖB; die Transparenz wird im Rahmen von Kundenbindungssystemen neben der individuellen Ansprache als Interesse der Kundinnen und Kunden ebenso beschrieben von Eckhardt/Fattebert/Keel/Meyer, 4 ff.

589 Das *abgestufte Transparenzsystem des noch geltenden DSG* – in Bezug auf den Verarbeitungszweck für den privaten Sektor – bildet konzeptionelle eine Orientierung an den Auswirkungen ab, die Personendatenverarbeitungen auf die *Persönlichkeitsrechte* zugemessen werden.[847]

590 Das Transparenzgebot will der Vorstellung zum Durchbruch verhelfen, wonach der Mensch als Subjekt und die Persönlichkeit ebenso im Rahmen der Datenbearbeitungsprozesse zu schützen ist. Transparenzvorgaben werden als Garant wahrgenommen, den Menschen nicht zum blossen Objekt der Datenbearbeitung verkommen zu lassen.[848] Das Transparenzgebot (und dessen Parameter) gemäss Art. 4 Abs. 4 DSG geben dem Individuum die Möglichkeit, Ansprüche nach Art. 12 Abs. 2 lit. b oder Art. 8 DSG geltend zu machen.[849] Sodann werden die Anforderungen an die Transparenz mit der Schwere der Persönlichkeitsbeeinträchtigung zu korrelieren gesucht. Hierbei orientiert man sich an einer dichotomisch gedachten Struktur: Bei «gewöhnlichen Personendaten» müssen die Beschaffung sowie der Zweck gemäss Art. 4 Abs. 4 DSG bloss erkennbar sein.[850] Nur bei besonders schutzwürdigen Personendaten und Persönlichkeitsprofilen greifen *de lege lata* qualifizierte Transparenzerfordernisse. Im Ergebnis beschränkt sich Art. 4 Abs. 4 DSG damit in seiner Anwendbarkeit auf Personendatenverarbeitungen durch Private, welche keine sensiblen Daten sammeln oder Persönlichkeitsprofile bearbeiten.[851] *De lege lata* wird somit hinsichtlich der Transparenzvorgaben auch betreffend den Verarbeitungszweck ein höheres Schutzniveau für den öffentlichen gegenüber dem privaten Bereich vorgesehen.[852]

591 Wie aber wird unter dem DSG vor seiner Totalrevision rechtsgenügend Transparenz bezüglich den Verarbeitungszweck geleistet? Für den öffentlichen Sektor spielt insofern das Legalitätsprinzip eine Rolle, über welches eine gewisse Transparenz, Rechtssicherheit sowie Normenkonkretheit geschaffen wird. Die Frage, *wann* eine Datenbearbeitung und deren Zweck als erkennbar gelten können, ist dennoch und gerade für den privaten Bereich nicht geklärt.[853] Die Entwicklung einer kohärenten Praxis, die justiziable Kriterien für das Erkennbarkeitserfordernis herausbildet, wird durch die Forderung, dass dieses für jeden Einzelfall zu prüfen sei,[854] durchkreuzt. Im Logistep-Urteil hatte das Bundesgericht einen

847 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 8; Meier, N 708.
848 BBl 2003, 2126.
849 Vgl. Rosenthal, HK-DSG, Art. 4 N 57; ablehnend Meier, N 697.
850 Bereits früh trat der Datenschutzbeauftragte für die Einführung einer allgemeinen Informationspflicht auch im Lichte der internationalen Regelungen ein, was indes von der Arbeitsgruppe abgelehnt wurde. Die Erkennbarkeit solle bei «normalen Daten genügen, eine Informationspflicht wäre eine unverhältnismässige Belastung für die Datenbearbeiter», Botschaft DSG 2003, 2101 ff., 2124 f.
851 Meier, N 694.
852 Mit der Totalrevision wird für beide Bereiche eine aktive Informationspflicht auch mit Blick auf den Verarbeitungszweck eingeführt, Art. 19 Abs. 2 lit. b nDSG.
853 Botschaft DSG 2003, 2101 ff., 2125.
854 Vgl. Epiney/Civitella/Zbinden, 27.

Grundsatzverstoss moniert, ohne die Anforderungen an das Erkennbarkeitsgebot zu umreissen.[855]

592 Aspekte der Datenbeschaffung, die erkennbar sein müssen, sollen gemäss Botschaft zum ersten DSG nach den Grundsätzen der Verhältnismässigkeit sowie von Treu und Glauben definiert werden.[856] Hinsichtlich die Zweckerkennbarkeit wird Unterschiedliches vertreten. Eine Meinung geht dahin, dass der Zweck aus den Umständen ersichtlich sei, wenn die betroffene – am Schicksal ihrer Daten interessierte, aufmerksame – Person bei der Bearbeitung in guten Treuen von einem bestimmten Zweck ausgehen musste –, selbst wenn sie nicht explizit über den Zweck informiert worden war oder keine Kenntnis davon genommen hatte.[857] So sollen beispielsweise beim Antrag für eine Kundenkarte die Kontaktangaben zur Abwicklung des Vertrags, zur Buchführung und allenfalls auch zur Durchsetzung von Ansprüchen auf dem Rechtsweg verwendet werden können.[858] Trotz Fehlens eines Hinweises müsse wohl auch mit der Verwendung zu Werbe- und Marketingzwecken durch das betreffende Unternehmen gerechnet werden.[859]

593 Anders der EDÖB, nach welchem verdeckte kommerzielle Datenerhebungen, bei welchen Werbezwecke nicht klar ersichtlich werden, unzulässig sind.[860] Im Übrigen ist es nicht die Aufgabe des Betroffenen, danach zu «suchen»[861]; vielmehr ist das Transparenzgebot eine Pflicht der Verantwortlichen. Dem Betroffenen werden von Gesetzes wegen – ausser aus Treu und Glauben – keine Aufgaben zugewiesen; es ist allein der Datenbearbeiter, der potentiell in die Persönlichkeit des Betroffenen eingreift, weshalb auch er derjenige ist, der für die Erkennbarkeit gemäss Art. 4 Abs. 4 DSG zu sorgen hat. Ist Zweck des Datenschutzgesetzes der Schutz der Persönlichkeit, entspricht eine solche Auslegung der ratio legis.

594 An die Datensubjekte dürfen als Folge davon keine zu hohen Erwartungen gestellt werden, auch nicht über eine Standardformulierung, wonach eine Person vorausgesetzt wird, welche «eine gewisse Aufmerksamkeit und ein Interesse am Schicksal ihrer Daten aufweisen muss».[862]

595 Datenschutzrechtliche Transparenzvorgaben werden in der Praxis meistens standardisiert gewährleistet. Das DSG vor seiner Totalrevision äussert sich *nicht zu Modalitäten oder Formen*, beispielsweise, wie die Erkennbarkeit zu gewähr-

855 BGE 136 II 508, E 6.3.1.
856 Botschaft DSG 2003, 2101 ff., 2125.
857 Rosenthal, HK-DSG, Art. 4 N 34 ff.; Botschaft DSG 2003, 2101 ff., 2124.
858 Botschaft DSG 2003, 2101 ff., 2125; vgl. Rosenthal, HK-DSG, Art. 4 N 35.
859 Rosenthal, HK-DSG, Art. 4 N 35 und 47; Botschaft DSG 2003, 2101 ff., 2125; a. M. Althaus Stämpfli, 95.
860 EDÖB, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/merkblaetter/erhebung-von-personendaten-fuer-marketingzwecke.html> (zuletzt besucht am 30. April 2021) mit vielen Hinweisen zum Marketing.
861 Zum Ausdruck Rosenthal, HK-DSG, Art. 4 DSG N 36.
862 Ders., a. a. O., Art. 4 N 34 ff.; Botschaft DSG 2003, 2101 ff., 2124.

leisten oder einer Informationspflicht nachzukommen ist. Unter der Ära des DSG vor Totalrevision kommt allgemeinen Geschäftsbedingungen eine zentrale Rolle zu. Es gilt als zulässig, die Erkennbarkeit auch des Zecks mittels AGB zu gewährleisten, sofern diese zugänglich sind. Die Erkennbarkeit gelte selbst dann als gegeben, wenn die betroffene Person diese nicht gelesen habe.[863] Gleichwohl liess sich ebenso in der Schweiz die Etablierung einer Praxis beobachten, wonach datenschutzrechtliche Transparenzvorgaben und Einwilligungstatbestände aus allgemeinen Geschäftsbedingungen ausgelagert und in separate, spezifische Datenschutzerklärungen integriert werden.

596 Betreffend Gestaltung und Granularität, gerade auch der Zwecktransparenz, finden sich mit Blick auf das geltende DSG viele Unklarheiten: Umstritten ist, inwieweit ein ungewöhnlicher Zweck speziell hervorzuheben ist.[864] Es scheint zulässig, mehrere Bearbeitungszwecke (in einer einzigen Klausel) anzuführen, es sei denn, es resultiere ein eigentlicher Zwang für das Datensubjekt infolge einer monopolartigen Machtstellung der datenverarbeitenden Stelle. Für den Fall, dass Bearbeitungszwecke nicht abschliessend aufgeführt werden (was m. E. allerdings bereits unter geltendem Recht problematisch ist), habe eine Interpretation nach Treu und Glauben zu erfolgen.[865] Innerhalb der Auslegungsfragen wird für die Anwendbarkeit der Interpretationsregel «in dubio contra stipulatorem» eingetreten. Eine Klausel «Bearbeitung zu Werbezwecken» wäre dementsprechend wohl als «Bearbeitung zu eigenen und nicht auch zu fremden Werbezwecken» zu verstehen.

597 Mit der Totalrevision verlangt Art. 19 Abs. 2 lit. b nDSG eine *Informierung über den Zweck*. Die Gewährleistung der Erkennbarkeit wird mit dem Inkrafttreten der neuen Fassung (trotz Art. 6 Abs. 3 nDSG) nicht mehr genügen, um den Transparenzvorgaben betreffend den Verarbeitungszweck zu genügen. Unbestritten dürfte sein, dass die Erkennbarkeit gemäss Art. 6 Abs. 3 nDSG in Bezug auf den Verarbeitungszweck durch Art. 19 Abs. 2 lit. b nDSG und die ebenda niedergelegte Informationspflicht übersteuert wird. Neu wird somit über den Verarbeitungszweck im Zeitpunkt der Beschaffung zu informieren sein.

598 Nach DSGVO erstreckt sich die aktive Informationspflicht auf alle im Zeitpunkt der Erhebung angestrebten Zwecke, wobei diese in hinreichender Granularität aufgeführt werden müssen. So formulieren die Art. 5 Abs. 1 lit. a DSGVO und Art. 12 ff. DSGVO, insofern insb. Art. 13 Abs. 2 und Art. 14 DSGVO weit- und tiefgreifende Informationspflichten.[866] Der resp. die Verarbeitungszwecke sind nicht nur in den Datenschutzerklärungen, sondern auch in allfällig erforderlichen

863 Meier, N 712.
864 Befürwortend Rosenthal, HK-DSG, Art. 4 N 37; ablehnend wohl Meier, N 712.
865 Meier, N 707.
866 DSGVO ErwG 39.

Einwilligungserklärungen, dem Verarbeitungsverzeichnis und den Datenschutz-Folgenabschätzungen aufzuführen.[867] Sodann bildet der Verarbeitungszweck den Inhalt der Antwort auf ein Auskunftsbegehren gemäss Art. 15 Abs. 1 lit. a DSGVO; er ist einschlägig im Rahmen des Löschungsbegehrens, Art. 17 Abs. 1 lit. a DSGVO, sowie des Berichtigungsbegehrens, Art. 16 DSGVO.[868] Damit lässt sich festhalten, dass im Zuge der jüngsten rechtlichen Entwicklungen und namentlich der DSGVO die Transparenzmachung, die Dokumentations- und Rechenschaftspflicht auch in Bezug auf den Verarbeitungszweck eine beachtliche Aufwertung erfahren haben. Zum einen muss das Datensubjekt in hinreichender Differenziertheit über die Verarbeitungszwecke informiert werden. Zum anderen werden die Definierung und Festlegung des Verarbeitungszweckes im Rahmen von Verarbeitungsverzeichnissen, Datenschutz-Folgenabschätzungen, aber auch von Löschungskonzepten usf. zu einem eigentlichen Instrument der Rechenschaft: Datenverarbeitende haben sich stets den einmal festgelegten Verarbeitungszweck vor Augen zu halten und sind entsprechend in ihren Verarbeitungsmöglichkeiten an diesen gebunden. Die Transparentmachung des Verarbeitungszweckes im Verarbeitungsverzeichnis dient dazu, die Rechtmässigkeit der Personendatenverarbeitung zu überprüfen.

4.2.2.2. Transparenz betreffend unmittelbare und mittelbare Verarbeitungszwecke

599 Eine Kernherausforderung der *Zwecktransparenz* – ungeachtet ihrer Ausgestaltung als Erkennbarkeitsforderung oder einer Informationspflicht – liegt in den pluralen Verarbeitungszwecken. Verarbeitungszwecke sind regelmässig nicht «monistisch», stattdessen facettenreich. Es geht hier nicht darum, die rechtsgenügliche Informierung resp. Transparenz in Bezug auf mehrere, nebeneinanderstehende Verarbeitungszwecke und die Umsetzung in der Praxis präziser zu beleuchten.

600 Vielmehr interessiert der Befund, wonach Verarbeitungshandlungen in der Regel nicht nur einem *unmittelbaren, sondern darüber hinaus einem mittelbaren Zweck dienen*, namentlich ökonomischen Interessen der datenverarbeitenden Unternehmen. Der Logistep-Entscheid illustrierte den Befund: Die Beklagte machte geltend, dass der Zweck der Datenerhebung und -bearbeitung die Aufdeckung von Urheberrechtsverletzungen sei; das private Unternehmen, das mit der Verarbeitung beauftragt worden war und die notwendige Software anbot, handelte aus rein wirtschaftlichem Interesse.[869]

867 DSGVO ErwG 32 und ErwG 42.
868 DSGVO ErwG 65.
869 BGE 136 II 508.

Längst sind Wendungen wie «Ihre Daten sind Gold wert» oder «Kommerzialisierung der Persönlichkeit resp. von Personendaten» zum Topos des allgemeinen resp. juristischen Jargons geworden. Sie artikulieren, dass ein Endzweck von Datenverarbeitungen oft die Generierung von Geld für die verarbeitenden Unternehmen ist. Für die *Datensubjekte* allerdings sind Zusammenhänge zwischen Personendatenverarbeitungen und deren mittel- wie unmittelbaren Zwecken oftmals undurchsichtig. Was ist damit gemeint: 601

Mark Zuckerberg von Facebook hat stets betont, dass er die Welt verbessern wolle, indem er die Menschen vernetze, diesen eine Plattform biete, damit sie ihre Beziehungen pflegen könnten.[870] Die *Nutzung des Dienstes, der sozialen Plattform*, kostet kein Geld. Dennoch erfolgt sie nicht unentgeltlich: Personendaten sind die Währung.[871] Die Tatsache, dass Personendatenverarbeitungen in aller Regel für die Verarbeitenden neben einem unmittelbaren Zweck einen mittelbaren Zweck erfüllen, und zwar die Generierung von wirtschaftlichen Gewinnen, ist für die Datensubjekte bei den im *Internet* angebotenen und genutzten Diensten bis heute nicht offensichtlich. 602

Auch im Bereich des Marketings finden sich mit Blick auf die datenschutzrechtliche Zwecktransparenz kritische Praktiken,[872] wobei sich diese für die Schweiz anhand der weit verbreiteten und wohl bekannten Supercard von Coop resp. Cumulus-Karte der Migros illustrieren lassen. Zu letzterer war auf der Homepage der Migros viele Jahre – mittlerweile allerdings angepasst – zu lesen: 603

> «Cumulus ist das kostenlose Bonusprogramm der Migros. Das Cumulus-Bonusprogramm – unsere Art, uns für Ihre Treue zu bedanken».

Eine dergestaltige Formulierung erweckt *erstens* den Eindruck, dass ein «Bonus» für die *Treue* entrichtet wird, und *zweitens*, dass dieser «Bonus» ein Geschenk (eine Zuwendung resp. Leistung ohne Gegenleistung) ist. Die elektronische Erfassung des Einkaufsverhaltens wird präsentiert, als ob sie zum Zwecke der Evaluierung der «Treue» erfolge, also primär darauf ausgerichtet sei, das *Einkaufsvolumen* zu ermitteln. Dies ist in doppelter Hinsicht missverständlich: Denn mit der Cumulus-Karte wird keineswegs primär oder gar ausschliesslich Kundentreue belohnt. Das lässt sich dadurch belegen, dass sowohl Coop wie Migros klassische Treueprogramme wie *papierne Markensysteme* kennen. Die elektronische Kundenkarte hingegen ist gerade auch darauf ausgerichtet, personen- 604

870 NZZ am Sonntag, Die Naivität Zuckerbergs ist eine Gefahr für die Demokratie, November 2017, <https://nzzas.nzz.ch/notizen/naivitaet-zuckerbergs-ist-eine-gefahr-fuer-demokratie-ld.1326328> (zuletzt besucht am 30. April 2021).

871 Zu Daten als Entgelt statt vieler Weber/Henseler, SZW 2019, 335 ff.

872 Hierzu Buchner, 147 ff.; vertiefend zu Marketing, Datenschutz und Internet Sachs, *passim*.

bezogene Daten zu generieren und damit u. a. Direktmarketing zu betreiben.[873] Das Cumulus-Kundenprogramm ist somit keineswegs «kostenlos», weshalb eine entsprechende Formulierung auf der Eingangsseite aus datenschutzrechtlicher Perspektive problematisch ist.[874] Seit September 2016 findet man unter einem der zahlreichen Links zum Programm jeweils eine aktuelle, ausführliche Datenschutzerklärung.[875] Um die Zustimmung zu diesem mehrseitigen Dokument bittet die Migros ausdrücklich. Sie wählt damit den Weg, aus Vorsicht und Respekt «vor der Selbstbestimmung» systematisch die Einwilligung einzuholen, selbst wenn diese nicht verlangt wäre von Gesetzes wegen.[876]

605 Das Illustrationsexempel fördert mehrere Herausforderungen zu Tage: Vorab wurde auf der Eingangsseite ein falscher Eindruck erweckt hinsichtlich der Ziele resp. Zwecke sowie Entgeltlichkeit des «Treueprogramms»; die Erhebung von Personendaten erfolgt, wie erwähnt, keineswegs primär und exklusiv zum Zweck, die Treue der Kundschaft zu bewerten und zu verdanken. Sodann erscheint der Weg, Datenbearbeitungen über die Einwilligung zu legitimieren, zumindest theoretisch nachvollziehbar. Er kann in einer Gesellschaft, welche die Selbstbestimmung akzentuiert, als Erfüllung einer sozialen Erwartung qualifiziert werden. In der Realität jedoch laufen solche Einwilligungserklärungen gewissermassen ins Leere: Kaum jemand studiert so detaillierte Dokumente; tut man es doch, so verliert man in aller Regel den Überblick, wer welche Personendaten zu welchem Zweck verarbeitet. Es erstaunt damit auch nicht, dass das Instrument der informierten Einwilligung gerade im Bereich des Online-Tracking und Advertising als illusorisch resp. Fiktion bezeichnet wird.[877] Zudem konterkarieren solche Einwilligungserklärungen m. E. das datenschutzrechtliche Transparenzgebot: Dort, wo Datenschutzeinwilligungen eingeholt werden, obschon gesetzlich nicht verlangt, wird dem Datensubjekt gegenüber eine Rechtsposition suggeriert, die es de facto/ex lege nicht hat. Es wird Intransparenz geschaffen.

873 Vertiefend zu Daten als Leistung, um im Austausch gegen Personendaten Rabatte, Boni usf. zu erlangen, rechtsvergleichend und auch mit Blick auf die Strukturen des Deutschen, Österreichischen und Schweizer Datenschutzrechts Langhanke, 26 ff.

874 In eine solche Richtung auch Buchner, 148.

875 Vgl. Migros, Cumulus Datenschutz, Zürich 2021, <https://www.migros.ch/de/cumulus/ueber-cumulus/datenschutz.html> (zuletzt besucht am 30. April 2021).

876 Vgl. zu diesem Thema Meier, N 714.

877 Vgl. die Beiträge von Barocas/Nissenbaum; kritisch auch Radlanski, 16; m. w. H. Heuberger, N 285 ff.; die Problematik wird im Rahmen der Darstellung der Wirksamkeit datenschutzrechtlicher Regulierungen genauer beleuchtet, vgl. hierzu dritter Teil, VIII. Kapitel, B.2.2.; vgl. zum Firefox-Browser das Add-on «TrackMeNot», das privacy bei Internetsuchen gewährleisten will, Howe/Nissenbaum, in: Kerr/Steeves/Lucock (Hrsg.), 417 ff., 417; kritisch zur faktischen Effektivität des «consent» im Datenschutzrecht Schermer/Custers/van der Hof, Ethics Inf. Technol., 117 ff.; früh auf die Untauglichkeit der Zustimmung sowie die Unredlichkeit, sich hinter der Freiwilligkeit einer Informationserteilung zu verschanzen, hingewiesen hat Simitis, in: Schlemmer (Hrsg.), 67 ff., 77.

4.2.3. Die Zweckbindung im engeren Sinne

606 Mit der Zweckbindung im engeren Sinne ist die Vorgabe angesprochen, wonach *Personendatenverarbeitungen nur zu jenem Zweck verarbeitet werden dürfen, wie er vorab fixiert und transparent gemacht wurde.* Anders gewendet: Die zu einem bestimmten Zweck erhobenen Personendaten sollen nicht «zweckentfremdet» werden.[878] Die Zweckbindung i. e. S. wird in Art. 4 Abs. 3 DSG resp. Art. 6 Abs. 3 nDSG, letzter Satz niedergelegt («sie dürfen nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist»).

607 Die Kommentarliteratur zur DSGVO umschreibt den Inhalt des Zweckbindungsgrundsatzes, wie er in Art. 5 Abs. 1 lit. b DSGVO niedergelegt ist, als «Perpetuierung» des ursprünglich festgelegten und legitimen Verarbeitungszweckes. Allerdings gilt nicht jede Verarbeitung zu einem anderen Zweck als Verstoss gegen das entsprechende Gebot von Art. 5 lit. b DSGVO. Vielmehr soll nur die Weiterverarbeitung zu einem anderen Zweck, der mit dem ursprünglichen Zweck nicht kompatibel ist, verboten sein. Wie indes die Grenzlinie der «Vereinbarkeit» resp. «Unvereinbarkeit» eines ursprünglichen Verarbeitungszweckes mit einem neuen Verarbeitungszweck zu definieren ist, bleibt unklar.[879] Der Verarbeitungsgrundsatz der Zweckbindung soll die Zweckbindung auf je konkrete Konstellationen beziehen.[880]

608 Zentrales Thema im Rahmen der Zweckbindung ist somit die sog. *Zweckänderung*. Sie gilt als Verstoss gegen den Zweckbindungsgrundsatz gemäss Art. 4 Abs. 3 DSG.[881] Nach Art. 13 Abs. 3 DSGVO muss der Verantwortliche bei einer Zweckänderung eine *Nachinformation* vornehmen und, sofern geboten, eine entsprechende Einwilligung einholen. Auch nach DSG gilt, dass eine Modifikation der Bearbeitungszwecke transparent zu machen ist und ggf. eine Nachinformation zu erfolgen hat resp. eine Einwilligung hierfür einzuholen ist.[882]

609 Zudem werden aus dem Zweckbindungsgebot, wie erwähnt, *Löschungspflichten* abgeleitet: So sind beispielsweise Aufnahmen von Videokameras in öffentlichen Räumen zu löschen, sobald ihnen keine Aktualität mehr hinsichtlich Aufklärung und Verhinderung von Störungen des öffentlichen Friedens oder von Straftaten zukommt.

878 Vgl. Epiney/Nüesch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.81 f.
879 Hierzu Reimer, NomosKomm-DSGVO, Art. 5 N 24 f.
880 Vgl. Herbst, BeckKomm-DSGVO, Art. 5 N 22.
881 Rampini, BSK-DSG, Art. 12 N 9.
882 Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 14 mit zahlreichen Beispielen für Persönlichkeitsverletzungen durch Zweckänderungen; zur Einwilligung als Rechtfertigungsgrund: Rampini, BSK-DSG, Art. 13 DSG N 3 ff.

610 Die DSGVO flankiert das Zweckbindungsgebot mit weiteren Bestimmungen, namentlich dem Grundsatz der Datenminimierung und Speicherbegrenzung, Art. 5 Abs. 1 lit. c und lit. e DSGVO. Hieran anknüpfend verlangt Art. 5 Abs. 1 lit. e DSGVO, dass Personendaten, sobald sie zur Erfüllung des vordefinierten Verarbeitungszweckes nicht mehr erforderlich sind (und kein anderweitiger Legitimationsgrund für die weitere Verarbeitung vorliegt, wie beispielsweise gesetzliche Aufbewahrungspflichten, aber auch die Weiterverarbeitung zu sog. sekundären Zwecken wie Archiv-, Forschungs- und Statistikzwecken), endgültig *gelöscht* oder *anonymisiert* werden müssen.[883] Mit der Totalrevision werden entsprechende Pflichten explizit in Art. 6 Abs. 4 nDSG normiert. Löschungs- und Anonymisierungspflichten dienen folglich der Umsetzung des Zweckbindungsgrundsatzes sowie des Verhältnismässigkeitsprinzips. Sichtbar wird an dieser Stelle die Korrelation zwischen datenschutzrechtlichem Verhältnismässigkeitsprinzip und Zweckbindungsgrundsatz.

611 Besagte Grundsätze resp. Vorgaben werden ihrerseits durch zusätzliche Instrumente abgesichert und implementiert, namentlich durch «privacy by design», vgl. Art. 25 Abs. 1 DSGVO und für die Schweiz nach Totalrevision Art. 7 Abs. 3 nDSG. Löschungskonzepte sowie Retentions- sowie Lösch-Policies, welche Fristen wie auch Verfahren definieren, sind geboten. Mit der Totalrevision baut die Schweiz die Anforderungen zur Gewährleistung der Zweckbindung aus, wobei viele der geplanten Bestimmungen als Parallelbestimmungen zur DSGVO bezeichnet werden können.

612 Auch der Zweckbindungsgrundsatz im engeren Sinne lässt sich auf das in dieser Studie als erstes Strukturmerkmal bezeichnete Merkmal des Monismus resp. Dualismus für den öffentlichen resp. privaten Bereich beziehen: In einem Regime des prinzipiellen Verarbeitungsverbotes, wie es die DSGVO vorsieht, weisen die gesetzlich vorgesehenen Erlaubnistatbestände eine zweckbasierte Orientierung auf. Der Gesetzgeber definiert zulässige Verarbeitungsziele und -zwecke resp. -grundlagen, die das prinzipielle Verarbeitungsverbot durchbrechen.[884] Auf diesem Weg werden vom Gesetz beispielsweise die «Wahrung lebenswichtiger Interessen» in Art. 6 Abs. 1 lit. d DSGVO oder die «Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen» in Art. 6 Abs. 1 lit. c DSGVO auf der allgemein-abstrakten Ebene als Verarbeitungszwecke anerkannt, die einen Erlaubnistatbestand für eine Personendatenverarbeitung liefern können. Im Sinne einer Anknüpfung an das konkrete Gebot gemäss Art. 5 Abs. 1 lit. b DSGVO ist auf

883 Vgl. Art. 6 Abs. 4 nDSG; kritisch zum Instrument der Anonymisierung, das gewissermassen verspricht, den «Personenbezug» zu kappen, allerdings nicht geeignet ist, die Adressierung bestimmter Personen, wenn auch nicht identifizierbar, zu erreichen Barocas/Nissenbaum, 1 ff., 4; vgl. im Zusammenhang mit Personendaten von Bankkundinnen und -kunden Hirsch/Jacot-Guillarmod, RSDA 2020, 151 ff., 159 ff.

884 Vgl. insb. Art. 6 DSGVO.

Art. 6 Abs. 4 DSGVO hinzuweisen, der sich mit dem Verhältnis eines ursprünglich fixierten Verarbeitungszweckes, des Primärzweckes, zu einem Sekundärzweck befasst. In Bezug auf die Bestimmung ist umstritten, ob sich ihre Funktion auf einen Kompatibilitätstest beschränkt oder ob sie als Erlaubnistatbestand für Zweckänderungen figuriert.[885]

613 Ebendiese Zweckorientierung findet sich ebenso im DSG, allerdings auf einer nachgeschalteten Stufe. Im DSG, wo sowohl vor als auch nach Totalrevision für den privaten Bereich die prinzipielle Verarbeitungsfreiheit mit Schranken verankert wird, fliessen entsprechende Zweckerwägungen über die gesetzlich vorstrukturierten Rechtfertigungsgründe, namentlich das überwiegende Interesse ein, vgl. Art. 13 Abs. 2 DSG und Art. 31 Abs. 2 nDSG. Hier formuliert das Gesetz einen Katalog von potentiell anerkannten Interessen, die eine persönlichkeitsverletzende Verarbeitungshandlung zum Schutz der Erreichung gewisser Zwecke legitimieren können.

4.3. Von der Zweckbindung zum Schutzzweck des Datenschutzes

614 Mit der dargelegten «Trias» der Zweckvorgaben – interne Zweckbestimmung, externe Transparenzmachung dieses Verarbeitungszweckes sowie Zweckbindung – wird vorab Rechenschaft vonseiten des Verarbeitenden hinsichtlich seiner Verarbeitungshandlungen abgelegt. Sodann werden die Verarbeitungsaktivitäten eingeschränkt. Der Zweckbindungsgrundsatz gilt mit den umrissenen Elementen in der Kommentarliteratur als «Kernbestandteil» des Datenschutzrechts.[886]

615 Seine datenschutzrechtliche Relevanz erschöpft sich – so die These an dieser Stelle – keineswegs darin. Vielmehr wirft der Zweckbindungsgrundsatz eindringlich die Frage nach dem *Schutzzweck des Datenschutzes selbst* auf.[887] Es ist ebenso dieser Konnex zum Schutzzweck des Datenschutzrechts selbst, der die hervorragende Bedeutung des Zweckbindungsgrundsatzes für das Datenschutzrecht verstärkt. Die nachfolgenden Ausführungen wenden sich der Frage nach dem *Schutzzweck oder den Schutzzwecken resp. -zielen des Datenschutzrechts* zu.

616 In Bezug auf die Frage nach dem *Zweck der Datenschutzgesetzgebung* selbst – die Wissenschaftlerinnen und Wissenschaftler wie keine andere Frage herausfordert – ist auf Art. 1 DSG einzugehen. Unter dem Titel «Zweck» sagt Art. 1 DSG:

885 Vgl. Buchner/Petri, BeckKomm-DSGVO, Art. 6 N 181.
886 Herbst, BeckKomm-DSGVO, Art. 5 N 21.
887 Auch im Rahmen der 12. Tagung zum Datenschutz – Jüngste Entwicklungen am 5. Februar 2019, organisiert vom Europa Institut, wurde in verschiedenen Referaten der Schutz der Persönlichkeit, Grundrechte und Würde der Person als Schutzzweck des Datenschutzrechts betont; vgl. statt vieler entsprechend dem Gesetzeswortlaut Peter, 33; vertiefend zu Zielfunktionen des Datenschutzes grundlegend und früh Mallmann, 16 ff.

> «Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.»

617 Mit der Totalrevision wurde eine Änderung vorgenommen, wonach nur «natürliche Personen» entsprechenden Schutz finden. Neu wird das DSG in Bezug auf Personendatenverarbeitungen von juristischen Personen keine Anwendung mehr finden.

618 In der Schweiz wird der *Zweck des Datenschutzgesetzes* ebenso unter dem Begriff des *Schutzobjektes* abgehandelt. Insofern allerdings findet sich ein Sammelsurium an weiteren Begriffen, vom Privatsphärenschutz über den Schutz der informationellen Selbstbestimmung bis hin zum Schutz des Missbrauches von Personendaten sowie Schutz der informationellen Privatheit.[888] Das DSG beschränkt sich darauf zu statuieren, dass es den Schutz der *Persönlichkeit* (resp. der Grundrechte) bezweckt. Anknüpfungspunkt des zivilrechtlichen Teils des Datenschutzgesetzes ist Art. 28 ZGB.[889] Nach der Auffassung der schweizerischen Datenschutzgesetzgebung geht es damit um den Schutz eines subjektiven Rechts des Individuums.

619 Anders das Konzept in der DSGVO: Die DSGVO stellt ihren ersten Artikel unter den Titel «Gegenstand und Ziel», wobei es die natürlichen Personen (indes ohne konkretisierte Anknüpfung an ein spezifisches subjektives Recht) sowie der freie Verkehr von Personendaten sind, denen die Vorschriften der DSGVO dienen sollen. Zugleich wird auf die Bedeutung des Datenschutzes für die Prosperität sowie den wirtschaftlichen wie sozialen Fortschritt hingewiesen.[890]

620 Die Frage *nach Schutzzweck und Schutzobjekt der Datenschutzregulierung* bleibt bis heute Kernthematik, -problematik und -herausforderung.[891] Die nachfolgenden Ausführungen arbeiten mit der folgenden *Hypothese:* Die herausragende Bedeutung der Vorgaben zum Verarbeitungszweck liegt auch darin begründet, dass aus ihnen *neue Perspektiven für den Schutzzweck des Datenschutzrechts* selbst abgeleitet werden können. Eine Beschäftigung mit dem Zweckbindungsgrundsatz legt eine *hinter resp. unter der individualrechtlichen, insb. der persönlichkeitsrechtlichen Schutzausrichtung angelegte systemische Schutzdimension des Datenschutzrechts frei.* Anders gewendet: Der Schutzzweck und Schutzauftrag der Datenschutzregulierung erschöpft sich nicht im Individualrechtsschutz resp. Persönlichkeitsschutz. Die hier formulierte Hypothese wird anhand einer eingehenden Auseinandersetzung mit dem mittlerweile in die Jahre gekommenen

888 Hierzu vertiefend zweiter Teil, VI. Kapitel.
889 Vgl. BBl 1988 II 414 ff., 414.
890 Vgl. DSGVO ErwG 2 ff.
891 Zur Diversifizierung der Schutzzwecke insb. qua DSGVO vgl. dritter Teil, VIII. Kapitel, A.2.2.

Volkszählungsurteil des deutschen Bundesverfassungsgerichts herausgearbeitet und erhärtet.[892]

Das Urteil wurde als «Magna Carta»[893] resp. «Bergpredigt»[894] des Datenschutzrechts bezeichnet. Eine vertiefte Auseinandersetzung mit den Zweckerwägungen und namentlich der Zweckbindung in dieser Entscheidung erstaunt prima vista: Seit dem Urteil sind Jahrzehnte rasanten technischen Fortschrittes ins Land gegangen. Zudem schrieb das Volkszählungsurteil wegen seiner *Anerkennung des Rechts auf informationelle Selbstbestimmung* Rechtsgeschichte. Allerdings ist das Volkszählungsurteil nicht nur wegen seinem vielzitierten Recht auf informationelle Selbstbestimmung aufschlussreich. Vielmehr ist es ebenso richtungsweisend hinsichtlich seiner *Zweckerwägungen*. Unter Rückgriff auf diese zweckorientierten Erwägungen des Bundesverfassungsgerichts lassen sich Lösungsansätze zwecks Weiterentwicklung des Datenschutzrechts der Zukunft ableiten – eines Datenschutzrechts, das seine Schutzaufträge und -zwecke effizient gewährleisten wird, selbst im Zeitalter der Digitalisierung.[895] 621

Im Folgenden geht es um die Darstellung eines Zusammenspiels zwischen mehreren Aspekten – zweckbezogene Verarbeitungsgrundsätze, Schutz des subjektiven Rechts der informationellen Selbstbestimmung und Schutzzweck des Datenschutzrechts. Die Argumentation des Bundesverfassungsgerichts im Volkszählungsurteil lässt sichtbar werden, dass das *Individuum datenschutzrechtlich nicht einzig mittels subjektiver Rechte hinreichend geschützt werden kann*. Stattdessen führt eine Analyse der Erwägungen zu der Schlussfolgerung, dass nur ein *systemischer Ansatz*, welcher namentlich den diversen und facettenreichen Verarbeitungszusammenhängen und damit gesellschaftlichen Bereichen Rechnung trägt, angemessene Antworten auf die Herausforderungen der Personendatenverarbeitungen liefert. Schlüsselelement bildet hierbei der *Verarbeitungszweck und -zusammenhang*. Im Volkszählungsurteil ging es insofern um Personendatenverarbeitungen durch den deutschen Staat *zwecks Zensus*. 622

Der erste Satz des Volkszählungsurteils und seiner Leitsätze lautet wie folgt: 623

> «Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.»[896]

892 BVerfG 65, 1 – Mikrozensus, Urteil vom 16. Juni 1969.
893 So Hoffmann-Riem, AöR 1998, 513 ff., 515.
894 Meister, DuD 1986, 173 ff., 175.
895 Auf die Bedeutung des Verwendungszusammenhanges und der Zweckbindung weist namentlich Simitis, NJW 1984, 394 ff., 402 ff. hin.
896 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 1.

624 Das Bundesverfassungsgericht macht den Schutz des Menschen mit seiner Persönlichkeit zum Ausgangspunkt des Rechtsschutzes im Kontext der Personendatenverarbeitung. Aufschlussreich insofern eine weitere Passage aus den verfassungsgerichtlichen Erwägungen, die nichts an Aktualität eingebüsst hat:

> «Die Möglichkeiten der modernen Datenverarbeitung sind weiterhin nur noch für Fachleute durchschaubar und können beim Staatsbürger die Furcht vor einer unkontrollierbaren Persönlichkeitserfassung […] auslösen […].»[897]

625 Zum Schutzbereich, der auch im Lichte von Art. 2. Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz beurteilt wurde, sowie zu den datenschutzrechtlichen Herausforderungen heisst es weiter:

> «1.a. Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt […]. Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschliessend. Es umfasst […] auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. […] Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermassen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiss. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.»[898]

626 Im letzten Satz dieses Zitates findet sich ein Befund, der mit dem jüngsten Facebook-Skandal aus dem Jahre 2018 erneut eine beispiellose Virulenz erfahren hat: Personenbezogene Angaben aus Facebook-Kommunikationsbeziehungen waren durch eine Drittgesellschaft analysiert worden. Mutmasslicherweise wurde in der Folge versucht, das *Wahlverhalten bestimmter Personen* gezielt zu beeinflussen.[899] Das Ansinnen, über die Nutzung von Personendaten, die das Individuum in

897 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 8.
898 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 172.
899 Vgl. Rosenberg/Confessore/Cadwalladry, NYT vom 17. März 2018, abrufbar unter: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> (zuletzt besucht am 30. April 2021).

persönlichen Kommunikationsbeziehungen über Facebook teilte, einzelne Individuen politisch zu manipulieren, beeinträchtigt *nicht* nur die konkret betroffenen Individuen. Ein solches Vorgehen weist eine kollektive Dimension auf, weil über die Manipulation der stimm- und wahlberechtigten Bürgerinnen und Bürger *die Integrität des demokratischen Systems an sich erodiert* wird.

627 Das Bundesverfassungsgericht hatte mit besagtem, zuletzt zitiertem Satz die *systemische Dimension datenschutzrechtlicher Regulierung adressiert*. Gleichwohl fährt es, an diesen heute als zukunftsweisend zu bezeichnenden Passus anknüpfend, mit einem subjektivrechtlichen Fokus fort:

> «Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art, 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insofern die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.»[900]

628 Es ist diese Erwägung zum Recht auf informationelle Selbstbestimmung, die unter dem Stichwort «Volkszählungsurteil» in die Gedächtnisse, Schriften und das Internet eingegangen ist. Mit der Passage werden das Subjekt, die Person und ihre Persönlichkeit sowie die Selbstbestimmung als Schutzzweck des Datenschutzes in das Zentrum der Aufmerksamkeit gerückt. Eine solche individualrechtliche, persönlichkeitsrechtliche Anknüpfung ist und bleibt ebenso für das Schweizer Datenschutzrecht prägend, Art. 1 (n)DSG.[901]

629 Dessen ungeachtet steht gemäss den Ausführungen des Bundesverfassungsgerichts der Schutz der informationellen Selbstbestimmung nicht allein da. Seine Gewährleistung ist zugleich *Garant für mehrere Grundrechte*. Zudem ist das Recht Grundlage für ein demokratisches und freiheitliches Gemeinwesen. Der *individualrechtliche Schutz ist von weiteren Schutzdimensionen nicht nur unterlagert, sondern in diese eingebettet*. Wird hingegen eine Datenverarbeitung isoliert für ein konkretes Datensubjekt als individualrechtliche Problemstellung fokussiert, werden kontextuelle Herausforderungen des Datenschutzes übersehen.[902] Folglich scheint es zu kurz gegriffen, ein wie auch immer geartetes subjektives Recht zu definieren, dieses aber nicht in seine gesellschaftlichen Bezüge einzubetten. Es ist das Bundesverfassungsgericht, das neben der Anerkennung eines Rechts auf informationelle Selbstbestimmung eine solche *Bezugnahme anhand seiner Erwägungen zum Verarbeitungszweck und namentlich zur Zweckbindung* vornimmt.

900 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 173.
901 Vgl. zur persönlichkeitsrechtlichen Anknüpfung als drittes Leitprinzip des DSG zweiter Teil, VI. Kapitel.
902 Vgl. insofern Teubner, KritV 2000, 388 ff., 388 und 404; Ders., in: Brüggemeier (Hrsg.), 303 ff.; Hensel/Teubner, KritJ 2014, 150 ff.

630 Unbestritten steht ein subjektives Recht, das Recht auf informationelle Selbstbestimmung resp. das Persönlichkeitsrecht als «Schutzzweck» datenschutzrechtlicher Regelung, in den Urteilserwägungen im Vordergrund. In diesem Zusammenhang aktualisiert sich auch die traditionsreiche Unterscheidung zwischen «gewöhnlichen» und «sensiblen» Personendaten. Das Bundesverfassungsgericht erteilte der datenschutzrechtlichen Tragfähigkeit einer zweigeteilten Welt indes eine punktuelle Absage:[903]

> «Die Verfassungsbeschwerden geben keinen Anlass zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses Datum" mehr.»[904]

631 Der Hinweis, wonach eine Anknüpfung des Datenschutzes an die Kategorisierung von personenbezogenen Daten als sensibel resp. nicht-sensibel im Zeitalter der neuen Datenverarbeitungstechnologien zu kurz greife, steht nicht isoliert da.[905] Von entscheidender Bedeutung in Bezug auf die Ausgestaltung der datenschutzrechtlichen Vorgaben kann nicht die «Natur» einer bestimmten Personenangabe sein; eine Personenangabe ist nicht per se besonders schutzwürdig. Vielmehr ist der *Verwendungszusammenhang* das einschlägige Kriterium, wie das Bundesverfassungsgericht wie folgt attestiert:

> «Wieweit Informationen sensibel sind, kann hiernach nicht alleine davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhanges: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.»[906]

903 Nissenbaum, 232, schlägt vor, beide dichotomen Konzepte – «privat»-«öffentlich», «gewöhnliche Personendaten»-«besonders schutzwürdige Personendaten» – für das Private ruhen zu lassen.

904 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 176.

905 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 176.

906 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 177; zu den «sensitiven Daten» als festem Bestandteil der Datenschutzgesetzgebung mit einer Kritik Simitis, in: Brem/Druey/Kramer/Schwander (Hrsg.), 469 ff.; die Untauglichkeit einer gesetzlichen Einteilung von Personendaten in gewöhnliche und besonders schutzwürdige Angaben als Orientierungskriterium für die Datenschutzregulierung wurde auch wissenschaftlich kritisch diskutiert, namentlich durch Simitis, Nomos-Komm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 20 ff. und N 34 ff., wobei der Datenschutzexperte zur Veranschaulichung der Untauglichkeit folgendes Beispiel nennt: Den Namen als belangloses Datum zu taxieren, greife offensichtlich zu kurz. Denn sobald es darum geht, dass dieser

Das Bundesverfassungsgericht hinterfragt somit den tradierten Differenzierungsmechanismus einer bezugslosen Taxierung von Personendaten als besonders schutzwürdig und damit einschlägiges Anknüpfungskriterium für erhöhte Schutzpflichten. Stattdessen betont es die Bedeutung des konkreten Verwendungszusammenhangs.[907] Es weist damit implizit auf die datenschutzrechtliche Notwendigkeit einer *differenzierten Sichtweise in Bezug auf die Verwendungszusammenhänge* hin. Verfassungsgerichtlich wird die hohe Bedeutung betont, wonach der Bearbeitungszweck bereichsspezifisch und präzise bestimmt und die gesammelten Angaben für diesen Zweck geeignet und erforderlich zu sein haben.[908] 632

Zugleich verdeutlicht das Gericht, dass der sog. öffentliche Bereich kein einheitlicher ist. Vielmehr sind staatliche Datenverarbeitungen facettenreich und jeweils an spezifische Stellen, Verwaltungseinheiten usf. angebunden. Den Verarbeitungszweck im öffentlichen Bereich mit einer allgemein umschriebenen «öffentlichen Aufgabe» abbilden zu wollen greift damit zu kurz. Betreffend den Verwaltungsvollzug sind stets die konkreten Aufgaben zu beachten. Dieser notwendigen Differenzierung trägt man im «öffentlichen Bereich» gerade auch über das Legalitätsprinzip Rechnung. Sowohl das deutsche als auch das schweizerische Datenschutzgesetz verlangen für den *öffentlichen Sektor*, dass die Umschreibung des *Zwecks der Datenbearbeitung* Inhalt einer *Rechtsnorm* ist (Prinzip der Spezialermächtigung). 633

In Deutschland waren es bis zum Inkrafttreten der revidierten Fassung mit ihren Anpassungen infolge der DSGVO die §§ 13 ff. BDSG, die als «Einfallstor»[909] für eine Vielzahl zulässiger Bearbeitungszwecke beschrieben wurden. § 13 Abs. 1 BDSG lautete: 634

> «Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist.»[910]

Name auf die Liste der Mafia komme, werde offensichtlich, dass der Name nicht per se als nicht besonders schutzwürdige Angabe qualifiziert werden könne; Nissenbaum, 232.

907 Hierzu auch Simitis, in: Brem/Druey/Kramer/Schwander (Hrsg.), 469 ff., insb. 485 ff.; im DSG bildet die Einteilung zwischen «gewöhnlichen» und «besonders schutzwürdigen» Personendaten, vgl. insofern Art. 3 lit. c DSG und Art. 5 lit. c nDSG, bis heute ein zentrales Strukturierungselement. In dieser dualistischen Konzeptionierung bildet sich eine Vorstellung ab, wonach bestimmte Personendaten per se «gewöhnlich», andere per se «besonders schutzwürdig» sind – und zwar ungeachtet ihres konkreten Verarbeitungszusammenhanges. Weiterhin korreliert die Schwere eines Eingriffes resp. die Höhe der Schutzvorgaben mit einer abstrakten Qualifizierung der Daten. Dreh- und Angelpunkt ist die quasi abstrakte Definition von Personenangaben als besonders schutzwürdig resp. sensibel.

908 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 179.

909 So Buchner, 38.

910 § 13 Abs. 1 BDSG war mithin keine Ausnahmebestimmung zu § 4 BDSG; es handelte sich nicht um eine Legitimationsgrundlage, personenbezogene Daten dann erheben zu dürfen (ungeachtet einer spezifischen Grundlage), sofern dies zur Erfüllung der «übergeordneten» öffentlichen Aufgabe diente. Vielmehr verlangte das Datenschutzgesetz selbst, dass eine rechtliche Grundlage den Zweck der Datenbearbeitung mit der öffentlichen Aufgabe korrelierte, in einem Sachzusammenhang stand. § 13

635 Der deutsche Gesetzgeber beschränkte sich damit nicht darauf, für eine Datenbearbeitung eine gesetzliche Grundlage, die sich zum öffentlichen Interesse sowie dem Zweck der Datenbearbeitung äussert (und zwar hinreichend konkret), zu fordern. Vielmehr musste der *Zweck der Datenbearbeitung mit der Erfüllung von Aufgaben des jeweiligen Aufgaben- und Kompetenzbereichs der verantwortlichen Stelle korrelieren*. Der Zweck und die Zweckbindung werden im Rahmen der Datenerhebung an die *Organisations- resp. Verwaltungseinheit sowie deren spezifische Aufgaben* gekoppelt.

636 Einen solch engen Koppelungsmechanismus zwischen Verarbeitungszweck und Organisationseinheit mit ihrem Aufgabenbereich kennt die Schweiz in ihrem DSG nicht. Zwar gilt nach DSG das Erfordernis, wonach der *Zweck der Datenbearbeitung* selbst in einer spezifischen gesetzlichen Grundlage zu definieren ist, gemäss Art. 17 i. V. m. Art. 4 Abs. 3 und 4 DSG resp. Art. 6 Abs. 1 und Art. 34 nDSG. Gleichwohl plädierte der Bundesrat bereits im Zuge des Erlasses des DSG dafür, keine allzu hohen Anforderungen an die «gesetzliche Grundlage» hinsichtlich der Formulierung von Verarbeitungszwecken zu stellen; es solle genügen, dass eine Datenbearbeitung in einem «einsichtigen sachlichen Zusammenhang» mit der Aufgabe des betreffenden Bundesorgans stehe.[911] Ist die öffentliche Aufgabe selbst hinreichend rechtlich legitimiert, dann gelten Personendatenverarbeitungen zwecks Erfüllung dieser Aufgaben als darin inkludiert.

637 Zurück zum Volkszählungsurteil: Dem zur Beurteilung vorliegenden Verarbeitungszusammenhang, der Personendatenerhebung für einen Zensus, werden Besonderheiten zugemessen, die in ein Dilemma hinsichtlich der Zweckbindung münden: Der Staat in seinem «heutigen» Zuschnitt bedarf der Datensammlung und Datenspeicherung auf Vorrat hin, um seinen Aufgaben nicht unvorbereitet gegenüberzustehen.[912] Eine Datenerhebung für statistische Zwecke kann somit gerade nicht an eine strikte Zweckbindung gekoppelt werden, ohne damit zugleich des Erreichens ihres eigentlichen Zieles verlustig zu gehen. Die Volkszählung solle eine «gesicherte Datenbasis für weitere statistische Untersuchungen» liefern sowie die politische Planung ermöglichen. Beide seien auf verlässliche Feststellungen über Zahl wie Struktur der Bevölkerung angewiesen.[913]

Abs. 1 BDSG stellte eine eigentlich verschärfende Konkretisierung mit Blick auf den Verarbeitungszweck dar.

911 BBl 1988 II 414 ff., 467; vgl. zu den erhöhten Anforderungen an die gesetzliche Grundlage, wenn es um besonders schutzwürdige Personendaten geht, Epiney/Fasnacht, Jusletter vom 24. Februar 2014, N 20 ff., spezifisch bezogen auf das Klienten-Informationssystem für Sozialarbeit. Der Beitrag zeigte indes, dass in erster Linie das kantonale Datenschutzrecht für besagtes System einschlägig ist.

912 Vgl. insofern auch Buchner, 72 ff., der darauf hinweist, dass dem Staat relativ viel Vertrauen entgegengebracht wird, nicht dagegen den Privaten als Datenbearbeitenden. Spezifisch problematisiert er Zugriffsbegehrlichkeiten des Staates auf private Datenbestände; vgl. hierzu auch Prieur, AJP 2015, 1644 ff., 1646.

913 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 184.

Mehrzweckverarbeitungen seien in einem solchen Sinne im Rahmen statistischer Erhebungen zuzulassen.[914] Eine strikte Zweckbindung könne demnach im Zusammenhang statistischer Erhebungen ebenso wenig Geltung beanspruchen wie das Verbot der Vorratsdatenspeicherung.

638 Gerade wegen dieser Spezialitäten zweckorientierter Vorgaben im Rahmen statistischer Erhebungen verlangte das Bundesverfassungsgericht *flankierende und kompensierende Vorkehrungen*. Gefordert wurde die Implementierung eines Mechanismus der *Abschottung der Statistik,* und zwar durch *Anonymisierung resp. durch Geheimhaltung* für den Fall (und die entsprechende Zeitdauer), wonach Angaben noch einen Personenbezug aufweisen. Im Ergebnis heisst das nichts anderes, als dass Angaben, die personenbezogen und zu statistischen Zwecken erhoben wurden, zwar zu anderen Zwecken verarbeitet und weitergegeben werden dürfen, allerdings grundsätzlich erst, wenn eine Anonymisierung stattgefunden hat.[915] Damit bleibt gewissermassen der ursprüngliche statistische Zweck rechtlich wirksam:

> «Eine Weitergabe der für statistische Zwecke erhobenen, nicht anonymisierten oder statistisch aufbereiteten Daten für Zwecke des Verwaltungsvollzugs kann hingegen in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung eingreifen».[916]

639 Das Bundesverfassungsgericht macht auch insofern die *zwei- resp. mehrdimensionale Schutzwirkung* seiner zweckorientierten Erwägungen auch unter diesem Aspekt deutlich: Die *Gewährleistung des Statistikgeheimnisses* schütze nicht (nur) das Individuum, sondern auch die *Integrität und Funktionstüchtigkeit statistischer Erhebungen* und damit letztlich den Staat mit seinen gegenwärtigen Aufgaben und Strukturen. Denn:

> «Für die Funktionsfähigkeit der amtlichen Statistik ist ein möglichst hoher Grad an Genauigkeit und Wahrheitsgehalt der erhobenen Daten notwendig. Dieses Ziel kann nur erreicht werden, wenn bei dem auskunftspflichtigen Bürger das notwendige Vertrauen in die Abschottung seiner für statistische Zwecke erhobenen Daten geschaffen wird, ohne welches seine Bereitschaft, wahrheitsgemässe Angaben zu machen, nicht herzustellen ist. Eine Staatspraxis, die sich nicht um die Bildung dieses Vertrauens durch Offenlegung des Verarbeitungsprozesses und strikte Abschottung bemühte, würde auf längere Sicht zu schwindender Kooperationsbereitschaft führen, weil Misstrauen entstünde. Da staatlicher Zwang nur begrenzt wirksam werden kann, wird ein die Interessen der Bürger überspielendes staatliches Handeln allenfalls kurzfristig vorteilhaft erscheinen; auf Dauer gesehen wird es zu einer Verringerung des Umfangs und der Genauigkeit der Informationen führen […]. Kann damit nur durch eine Abschottung der Statistik die Staatsaufgabe „Planung" gewährleistet werden, ist das Prinzip der Geheimhaltung und möglichst früh-

914 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 173.
915 Vgl. entsprechende Forderungen aufgreifend Art. 31 Abs. 2 lit. e nDSG.
916 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 191; die Anonymisierungspflicht ist, wie erwähnt, eine mit der DSGVO sowie der Totalrevision des DSG nunmehr konkretisiert vorgesehene Pflicht zur Umsetzung des Zweckbindungsgebotes.

> zeitigen Anonymisierung der Daten nicht nur zum Schutz des Rechts auf informationelle Selbstbestimmung des Einzelnen vom Grundgesetz gefordert, sondern auch für die Statistik selbst konstitutiv.»[917]

640 Auch wenn das Bundesverfassungsgericht auf Relativierungen strikter Zweckbindung und folgend kompensatorischer Vorkehrungen im Rahmen statistischer Erhebungen einging, blieb die Idee des Verbotes der Zweckänderung zentral für seine Ausführungen:

> «Würden hingegen personenbezogene, nicht anonymisierte Daten, die zu statistischen Zwecken erhoben wurden und nach der gesetzlichen Regelung dafür bestimmt sind, für Zwecke des Verwaltungsvollzuges weitergegeben (Zweckentfremdung), würde in unzulässiger Weise in das Recht auf informationelle Selbstbestimmung eingegriffen.»[918]

641 Das Bundesverfassungsgericht markierte damit Notwendigkeit und Grundsatz der *Trennung von Statistik und Vollzug*.[919] Folglich bringt es zum Ausdruck, dass der öffentliche resp. staatliche Bereich kein monolithischer, sondern ein hoch ausdifferenzierter Bereich ist, innerhalb dessen zahlreiche Verarbeitungszwecke verfolgt werden.[920] *Datenschutzrechtliche Vorgaben dienen hierbei auch dem Schutz der Integrität des jeweiligen Bereichs*.

642 Das Volkszählungsurteil, obschon dieses primär und untrennbar mit dem Grundrecht auf informationelle Selbstbestimmung assoziiert wird, lädt somit zu einem *Perspektivenwechsel* resp. einer Ergänzung des Blickes um eine grundlegende, dahinterstehende Schutzdimension des Datenschutzrechts ein: Die Lektüre des Urteils führt zu der Erkenntnis, dass der *«Zweck» des Datenschutzrechts* – über ein Recht auf informationelle Selbstbestimmung hinausgehend – in der Gewährleistung *mehrdimensionaler Schutzrichtungen liegt*. Zwar wird dem individualrechtlichen Schutz (bis heute) eine prioritäre Rolle zugewiesen, indem das Datenschutzrecht am Schutz des Menschen, der Person, dem Datensubjekt und an den Individualrechten der Persönlichkeit oder der Selbstbestimmung anknüpft.[921]

643 Die Kontextrelevanz wird in der verfassungsgerichtlichen Problematisierung des *Transfers von Personenangaben, die zum Zweck der Statistik erhoben werden sollten, in weitere und andere Kontexte des Verwaltungsvollzuges* deutlich. Insofern kam das Gericht zu dem Schluss, dass eine Zuführung von Personenangaben, die im Zuge der statistischen Erhebung erhoben wurden, in diverse andere Verwaltungskontexte sowohl die *Integrität der Statistik als auch allgemein staatliche Aufgaben* beeinträchtigen würde. Einzig die Abschottung der statistischen Erhebung durch das Statistikgeheimnis resp. die spätere Anonymisierung der Per-

917 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 188.
918 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 223.
919 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 223.
920 Der Bearbeitungszweck wird von Glass, 125 ff. als Instrument zur Beschreibung des rechtmässigen Kontextraums beschrieben.
921 Vertiefend für das DSG im privaten Bereich zweiter Teil, VI. Kapitel.

sonenangaben liefere eine hinreichend wirksame Garantie, dass die Bürgerinnen und Bürger die im Rahmen des Zensus gestellten Fragen wahrheitsgetreu und vollständig beantworten würden. Müssten sie dagegen fürchten, dass ihre Angaben später in anderen Feldern des Verwaltungsvollzuges «gegen sie verwendet würden», würde dies das Aussageverhalten negativ beeinträchtigen.[922]

644 Die Bedeutung, die das *Bundesverfassungsgericht datenschutzrechtlich dem Schutz der Integrität der statistischen Erhebung zuweist*, untermauert es argumentativ mit der beschränkten Wirksamkeit von Zwangsmassnahmen. Vollstreckende Zwangsmassnahmen, die der Staat bekanntermassen durchaus zur Hand hat, griffen zu kurz, um dem Missbrauch der statistischen Erhebung entgegenzuwirken.[923] Nur wenn die Bürgerinnen und Bürger das notwendige *Vertrauen* haben, dass ihre personenbezogenen Daten einzig zu statistischen Zwecken verarbeitet und nicht weiterreichend zum Verwaltungsvollzug genutzt werden, sei davon auszugehen, dass die erfragten Angaben vollständig und wahrheitsgetreu erteilt würden. Müsse dagegen basierend auf einer Volkszählung mit einer «plötzlichen» Steuernachforderung oder einer Ausweisungsverfügung gerechnet werden, dürfe aller Voraussicht nach weder mit wahrheitsgetreuen noch vollständigen Antworten gerechnet werden. Die Integrität der Statistik und deren Funktionsfähigkeit würden damit über den Zweckbindungsgrundsatz und das Vertrauen der «Hauptpersonen» abgesichert, also quasi *intrinsisch* gewährleistet. Die Möglichkeit, die statistisch erhobenen Daten für den weiteren Verwaltungsvollzug zu nutzen, mag verführerisch erscheinen – auch aus staatlichen «Effizienzerwägungen», denen die Statistik ja gerade verpflichtet ist. Der Preis indes wäre, so das Bundesverfassungsgericht, zu hoch.

645 Das Volkszählungsurteil anerkennt mit diesen Ausführungen, dass der *öffentliche Bereich im Sinne des staatlichen Bereiches* kein einheitlicher Bereich ist. Er konstituiert sich aus facettenreichen Unterbereichen mit entsprechenden Aufgaben. Diese sind ihrerseits relevant für den Datenschutz, der sich als *relational oder akzessorisch zu den jeweils dahinterliegenden Verarbeitungszusammenhängen, Zielen und Zwecken* der einschlägigen staatlichen Bereiche bestätigt. Die Pluralität der Verarbeitungszusammenhänge anzuerkennen und voneinander abzugrenzen, erfolgt *nicht nur zum Schutz des Individuums*. Es dient *ebenso und gerade zum Schutz der Integrität der diversen Bereiche*.

646 Der Zweckbindungsgrundsatz präsentiert sich damit als Barriere-Mechanismus für Personendatenflüsse. Personendaten, die zu einem bestimmten Zweck erhoben und in einen zugehörigen Kreislauf eingespeist wurden, dürfen nicht unbe-

922 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 188.
923 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 178 und E 188.

schränkt in weitere, andere Kreisläufe eingespeist und dort anderen Verarbeitungszwecken zugeführt werden.

647 Mit diesen Ausführungen werden die bereits anhand der Geheimworte und Geheimhaltungspflichten herausdestillierten *dynamischen sowie akzessorischen Dimensionen* datenschutzrechtlicher Themen bestätigt.[924] Datenschutzrechtliche Herausforderungen sind folglich besser zu bewältigen, wenn als *Ausgangslage das Bild von Personendatenflüssen* gewählt wird. Diese sind eingebettet in verschiedene Verarbeitungszusammenhänge resp. Kontexte, was durch die Metapher der Landschaft symbolisiert werden könnte. In der Folge sind insb. die Grenzübertritte zwischen verschiedenen Bereichen sowie die Gestaltung von Personendatenflüssen vonseiten des Rechts zu adressieren.[925] Eine solche Herangehens- und Betrachtungsweise der datenschutzrechtlichen Ausgangslage konterkariert die traditionsreiche Anknüpfung an das dualistische Regime mit Datensubjekt resp. Person und Personendaten als Quasi-Objekten.

648 Der Zweck datenschutzrechtlicher Regulierung beschränkt sich damit, wie die vorangehenden Reflexionen zum Volkszählungsurteil freigelegt haben, nicht auf den Schutz des Individuums, also des Datensubjektes. Vielmehr kommt dem Datenschutzrecht eine Garantenstellung zum Schutz der Integrität verschiedener gesellschaftlicher Systeme, Institutionen oder Bereiche zu.

649 Die Zweckerwägungen destillieren eine richtungsweisende Facette des Zwecks des Datenschutzrechts selbst heraus: Aussagekräftige Statistiken seien, so das Bundesverfassungsgericht, für den Staat zeitgenössischen Zuschnittes unverzichtbar, um seine mannigfachen Aufgaben angemessen planen und bewältigen zu können. Wenn allerdings die Bürgerinnen und Bürger damit rechnen müssen, dass die personenbezogenen Angaben, die sie im Rahmen der Statistikerhebung offenbaren, Konsequenzen in anderen Bereichen – vonseiten der Einwohnerbehörde, des Steueramtes, der «Vormundschaftsbehörde» usf. – nach sich zögen, würde der *statistische Zweck selbst gefährdet*. Statistische Erhebungen können nur dann erfolgreich sein, wenn die zur Auskunft verpflichteten Bürgerinnen und Bürger nicht dazu «verleitet» werden, Angaben zu verweigern oder zu verfälschen. Dazu sind sie allerdings gerade dann veranlasst, wenn sie fürchten müssen, dass ihre Angaben Auswirkungen in anderen Zusammenhängen haben könnten. Die zweckorientierten Erwägungen und kompensatorischen Mechanismen zur Abschottung der Statistik präsentieren sich damit nicht nur als Schutzinstrument der Bürgerinnen und Bürger, sondern quasi als staatliches Selbstschutz-

924 Vgl. insb. erster Teil, I. Kapitel, A.

925 Vgl. zu den Data Flows zwischen Ländern, aber auch Gesellschaftsbereichen Birnhack, CLSR 2008, 508 ff., 512 f.; dazu, dass es bei der privacy um den Fluss von Personendaten gehe, Kang/Buchner, Harv. J.L. & Tech. 2004, 229 ff., 231 f., wobei ihr interessanter Beitrag in Dialogen strukturiert wird; der erste Dialog ist der Market-Talk, der zweite Talk ist der Dignity-Talk.

instrument: Mit ihrer Gewährleistung schützt der Staat sich selbst, seine Funktionstüchtigkeit und die Funktionstüchtigkeit seiner Instrumente und Bereiche, im Volkszählungsentscheid die Statistik und die sog. *Integrität der Statistik*. Die datenschutzrechtlichen Vorgaben haben sich ebenso dem Schutz der Integrität dieser anerkannten gesellschaftlichen «Institution» zu widmen. Mit einem solchen *systemischen Schutz* wird das Datensubjekt inkludierend geschützt.

650 Neben dem *individualrechtlichen* und *systemisch-institutionellen Gesicht* wurde anhand dieser Ausführungen zur Zweckbindung erneut das *dynamisch-relationale (oder auch dynamisch-akzessorische) Gesicht* der Thematik sichtbar. Der Zweckbindungsgrundsatz fixiert *personenbezogene Daten in einem bestimmten Informationskreislauf*. Er schreibt vor, dass zu einem bestimmten Zweck erhobene personenbezogene Daten nicht zu einem anderen Zweck bearbeitet werden dürfen. Kurz: *Eine Zweckentfremdung ist verboten, die Überleitung von zweckgebundenen Daten zur Erfüllung anderer Zwecke ist unzulässig.* Diese dynamische Dimension des Datenschutzrechts richtet den Fokus auf eine Vorstellung, nach welcher personenbezogene Daten aufgrund des definierten Zweckes in einem bestimmten Verarbeitungszusammenhang dienen – in einem bestimmten Flussbett fliessen. Unter welchen Voraussetzungen personenbezogene Daten aus diesem Flussbett abgeleitet und in einen anderen Datenflusslauf, in einen anderen Verarbeitungszusammenhang eingespeist werden dürfen, ist die zentrale Frage. Es geht damit – unter Beibehaltung der geografischen Sprache – um die Flussmündungen und Grenzübertritte («Schnittstellen»[926], «Schaltstellen», «Knotenpunkte»[927]). Das Datenschutzrecht befasst sich, wie es die zweckorientierten Leitvorstellungen zeigen, mit *Datenflüssen zwischen und in unterschiedlichen Systemen, mit Datenverarbeitungen zu unterschiedlichen Zwecken, in diversen Verarbeitungszusammenhängen.* Bei einer solchen Konzeptionierung steht die Frage nach den sog. *Transmissionsprinzipien im Vordergrund*.[928] Im Laufe dieser Arbeit wurden bislang insofern bereits nebst dem Geheimnis und der Einwilligung auch das Instrument der Anonymisierung vorgestellt.

651 Eine *kontextuelle Betrachtung* kommt zur Vervollständigung des Bildes nicht umhin, eine einbettende Klarstellung vorzunehmen: Es war ein Entscheid zum Datenschutzrecht des öffentlichen i. S. des staatlichen Bereiches, anhand dessen zweckorientierten Erwägungen und namentlich der Zweckbestimmung sowie -bindung sich *drei datenschutzrechtliche Herausforderungen, Schutzziele, Aspekte sowie Dimensionen* herausarbeiten liessen. Kontextuell betrachtet wird inso-

926 Vgl. zum Begriff im Zusammenhang mit Verarbeitungsprozessen von Personendaten durch Spitäler Gogniat, Jusletter vom 20. Juni 2016, N 2.

927 So Ladeur, Vortrag Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021).

928 Hierzu Nissenbaum, 145 ff., 192 f., 201 ff., 217 ff.; vertiefend dritter Teil, IX. Kapitel.

fern seit jeher und bis heute die Problematik des staatlichen Zugriffes vonseiten des Staates auf Datenbestände privater Akteure thematisiert.[929] Damit fragt sich sogleich weiter: Lässt sich die systemisch-institutionelle sowie dynamisch-akzessorische Bedeutung des Datenschutzes, der bis heute nicht die gebotene Aufmerksamkeit geschenkt wurde, auch für den *sog. privaten Bereich im Sinne der (Zivil-)Gesellschaft* nachzeichnen?

652 Hinweise in diese Richtung finden sich im bereits zitierten Logistep-Urteil des Bundesgerichts. Zwar legte das Gericht den Schwerpunkt auf den Befund, wonach das Vorgehen der Logistep AG und hierbei auch der *Zweck* ihrer Datenerhebungen *nicht erkennbar* waren. Gleichwohl enthalten auch die bundesgerichtlichen Ausführungen Hinweise zur Einschlägigkeit *pluraler Verarbeitungskontexte*. Im Logistep-Entscheid verortete das Bundesgericht den *Zweck* der Datenbearbeitung in der *Aufklärung von Urheberrechtsverletzungen*. Das *Interesse* der die Bearbeitungsgrundsätze verletzenden Partei allerdings war, wie geschildert, ein *wirtschaftliches*:

> «Die Beschwerdegegnerin selbst verfolgt ein wirtschaftliches Interesse. Sie strebt eine Vergütung für ihre Tätigkeit an. Diese Tätigkeit besteht darin, mit Hilfe einer eigens dafür entwickelten Software in P2P-Netzwerken nach urheberrechtlich geschützten Werken zu suchen und von deren Anbietern Daten zu speichern.»[930]

653 Für die Einhaltung der Grundsätze gemäss Art. 4 Abs. 3 und Abs. 4 DSG genügt es, dass der unmittelbare Datenbearbeitungszweck einer konkreten Datenverarbeitungshandlung als Massstab dient. Entscheidend war für das Bundesgericht, dass der relevante unmittelbare Zweck der Datenerhebung für die Datensubjekte im Dunkeln blieb, was gegen Art. 4 Abs. 3 und Abs. 4 DSG verstosse.[931] Es ergänzte indes sogleich, dass dieser Verstoss – entgegen dem zu engen Wortlaut von Art. 12 Abs. 2 lit. a DSG – gerechtfertigt werden könne. Allerdings würde im vorliegenden Fall kein überwiegendes privates oder öffentliches Interesse den Verstoss gegen die Bearbeitungsgrundsätze von Art. 4 Abs. 3 und Abs. 4 DSG rechtfertigen, selbst wenn man über das wirtschaftliche Interesse der bearbeitenden Partei dasjenige der Auftraggeberin an der Aufklärung von Urheberrechtsverletzungen in die Erwägungen integriere. Die Annahme überwiegender Interessen dürfe von vornherein nur mit Zurückhaltung angenommen werden.[932]

---

929 So jüngst Lobsiger, Verschärfung der Datenschutzaufsicht über die Polizei, Vortrag vom 7. Februar 2019, Zürcher Juristenverein; Buchner, 72 ff.; die Problematik ist akzentuiert, wenn die datenschutzrechtlichen Vorgaben, wie im schweizerischen DSG, für den öffentlichen Bereich strikter sind als für den privaten Bereich. Eine Lösung hierfür liegt in einem monistischen Ansatz mit identischem Regime für die beiden Sektoren, wie ihn nunmehr die DSGVO implementiert.

930 BGE 136 II 508, E 6.3.3.

931 BGE 136 II 508, E 4.

932 BGE 136 II 508, E 6.3.3. und E 6.4.; für einen umfassenderen Überblick über die Praxis des EDÖB, die Verwaltungsgerichtspraxis und die Bundesgerichtspraxis vgl. die einschlägigen Datenschutzkommentare.

Im vorliegenden Fall wurde eine Rechtfertigung verneint, wobei in diesem Entscheid für «den privaten Bereich» die *systemisch-institutionelle Dimension* des Datenschutzes und seiner Herausforderungen angelegt ist. Es ist der Kontext der Ökonomie, der mit dem privaten Lebensbereich kollidiert, wobei zugleich ein privater Akteur eine Aufgabe, die der staatlichen Strafbehörde zugewiesen wird, an sich zieht.[933] 654

Das dieser Studie den Titel verleihende Recht auf informationellen Systemschutz wird im dritten Teil, IX. Kapitel elaboriert. Es ist Konsequenz eines im Zuge dieser Schrift an diversen Stellen freigelegten systemrelativen Elements, wie es im zeitgenössischen Datenschutzrecht angelegt ist. Für die Herleitung des Rechts auf informationellen Systemschutz wird eine vergleichbare Konstellation gewählt werden, wie sie sich im Logistep-Entscheid findet. In beiden Fällen finden verdeckte Ermittlungen zwecks Aufdeckung mutmasslich unrechtmässiger Handlungen statt. Bei der im letzten Kapitel dieser Studie gewählten Konstellation geht es um die Versicherungsobservation zur vermeintlichen Betrugsaufdeckung. Auch hier kollidieren infolge von Personendatenverarbeitungen gesellschaftliche Kontexte miteinander, womit die *Integrität der gesellschaftlichen Bereiche* selbst aufs Spiel gesetzt wird.[934] 655

933 Interessant die historische Annäherung an den nur vermeintlich klaren Begriff der Ökonomie durch die Beiträge in Dejung/Dommann/Speich (Hrsg.).

934 Vgl. hierzu dritter Teil, IX. Kapitel; aufschlussreich sodann der jüngste Entscheid des Bundesverwaltungsgerichts, in dessen Argumentation zum Zweckbindungsgrundsatz ebenso die systemrelative Bedeutung aufscheint: Bearbeite die Beklagte im Rahmen des Helsana+-Programmes Personendaten, die bei einer anderen Versicherungsgesellschaft der Helsana-Gruppe im Zusammenhang mit der obligatorischen Krankenkasse gespeichert worden seien, stehe dies im Konflikt mit der Zweckbindung, Art. 4 Abs. 3 DSG, BGer A-3548/2018 vom 19. März 2019, E 3 ff. Mit Blick auf die Zweckbindung nimmt man in erster Linie das Unternehmen in den Blick, welches zu einem bestimmten und erkennbar gemachten Zweck Personendaten verarbeitet – an diesen Zweck ist das Unternehmen alsdann gebunden. In casu ist es in erster Linie die Krankenversicherungsgesellschaft, welche Personendaten zwecks Abwicklung der Grundversicherung verarbeitet, die gegen den Zweckbindungsgrundsatz verstösst, wenn sie zu diesem Zweck gesammelte Personendaten weitergibt. Doch nach bundesverwaltungsgerichtlichem Entscheid verletzte ebenso die Zusatzversicherung das Zweckbindungsgebot, indem sie auf Personenangaben einer anderen Versicherungsgesellschaft zugriff, die durch die Grundversicherung in ebendiesem Kontext und zu ebendiesem Zweck erhoben und gespeichert worden waren. Eine solche weite Auslegung zum Zweckbindungsgrundsatz schottet offensichtlich verschiedene Bereiche voneinander ab – die Grundversicherung gegenüber der Zusatzversicherung. Der Fluss von Personendaten zwischen diesen beiden Bereichen wird verhindert, indem selbst das «Drittunternehmen» an den Verarbeitungszweck des «Erstunternehmens» gebunden ist; die konsequenteste Weise, die Einschlägigkeit des Verwendungszusammenhanges datenschutzrechtlich zum zentralen Ansatzpunkt und Lösungsansatz zu machen, findet sich in einer sektoriellen Datenschutzgesetzgebung. Namentlich die USA kennt für den privaten Bereich kein datenschutzrechtliches Querschnittsgesetz. Auch in Europa finden sich bereichsspezifische Datenschutznormierungen, ohne dass auf eine Querschnittsgesetzgebung verzichtet wird.

4.4. Resümee

656 Die vorangehenden Ausführungen haben die zentrale Bedeutung der *Zweckvorgaben* im und für das Datenschutzrecht analysiert. Gezeigt wurde, dass die verschiedenen Regelungsinhalte verschiedene Stossrichtungen verfolgen. Das Verhältnismässigkeitsprinzip wird an den Verarbeitungszweck angebunden, indem Verarbeitungshandlungen zur Erreichung eines definierten Zweckes geeignet, erforderlich und verhältnismässig im engeren Sinne zu sein haben. Mit diesen Vorgaben werden Verarbeitungsmöglichkeiten von Anfang an vordefiniert und damit zurückgebunden. Zudem greifen in Bezug auf den Verarbeitungszweck Transparenzvorgaben, wobei mit der Totalrevision des DSG neu eine Informationspflicht verankert wird.

657 Spezifisch unter dem Grundsatz der Zweckbindung (im weiteren Sinne) lassen sich die Vorgaben an die vorgängige Zweckfixierung resp. -definierung, die Transparenzvorgaben hinsichtlich des Verarbeitungszweckes sowie die Zweckbindung im engeren Sinne unterscheiden. Der faktischen Einhaltung der Zweckvorgaben dienen Instrumente wie das Verarbeitungsverzeichnis, Löschungs- und Anonymisierungsvorgaben, die Datenschutz-Folgenabschätzung, aber auch die Anforderungen an die hinreichend konkrete sowie granulare Transparenzmachung von Verarbeitungszwecken im Rahmen von Datenschutz- und Einwilligungserklärungen.

658 Nachdem der Inhalt der Gebote auch in ihren Entwicklungslinien nachgezeichnet wurde, gelangte die Arbeit zu einer *Grundsatzfrage: zur Frage nach dem Zweck der Datenschutzgesetzgebung*. Im Zentrum stand eine vertiefte Beschäftigung mit den Ausführungen des Bundesverfassungsgerichts in seinem Volkszählungsurteil. Hierbei wurde gezeigt, dass das Urteil, das für «sein» Recht auf informationelle Selbstbestimmung berühmt wurde, den Schutzzweck des Datenschutzes zwar durchaus stark individual- und persönlichkeitsrechtlich anknüpft. Allerdings wurde auch manifest, dass das Bundesverfassungsgericht anhand seiner Erwägungen zu den Zweckgrundsätzen eine *systemische resp. institutionelle* Schutzdimension des Datenschutzes betont. Das Bundesverfassungsgericht machte deutlich, dass innerhalb des «öffentlichen Bereiches» plurale Verarbeitungszusammenhänge und -zwecke zu differenzieren seien und es nicht angehe, zu statistischen Zwecken erhobene Angaben beliebig den unzähligen und facettenreichen Bereichen des Verwaltungsvollzuges zugänglich zu machen. Der öffentliche Bereich und die öffentliche Verwaltung ist folglich aus datenschutzrechtlicher Perspektive gerade kein einheitlicher Bereich. Vielmehr konstituiert er sich aus zahlreichen Einheiten, Institutionen, Aufgabenfeldern mit jeweils «eigenen» Datenverarbeitungszwecken.

Zweckbindungsvorgaben, die eine Schlüsselrolle in der Argumentation des Bundesverfassungsgerichts einnahmen, zielen entsprechend nicht nur auf den *Subjektschutz*, sondern namentlich auch auf den *Systemschutz* ab. Der Datenschutz dient damit nicht nur dem Schutz des einzelnen Individuums, sondern ebenso dem *Schutz der Integrität verschiedener Bereiche resp. Systeme*. Die datenschutzrechtlichen Vorgaben sind also auch darauf auszurichten, die Funktionstüchtigkeit und Integrität der jeweils auf dem Spiel stehenden Kontexte, Institutionen und Bereiche zu gewährleisten.[935] Angemessene und befriedigende Antworten vonseiten des Datenschutzrechts, das beide Schutzdimensionen und -zwecke seiner selbst anerkennt, können nur durch eine systemrelative Betrachtung gefunden werden. 659

Die im Volkszählungsurteil thematisierte systemische Dimension und Relevanz des Datenschutzes wird viele Jahrzehnte später durch den jüngsten Facebook-Skandal bestätigt: Personendaten, die aus persönlichen Kommunikationsbeziehungen über Facebook generiert wurden, gelangten an ein Drittunternehmen zur Analyse (es ist anzunehmen, dass diese verkauft wurden), woraufhin man Nutzerinnen und Nutzer in ihrer Rolle als Wählerinnen und Wähler im US-Wahlkampf zu beeinflussen versuchte. Personendaten wurden losgelöst von ihrem ursprünglichen Verarbeitungskontext, losgelöst von persönlichen Kommunikationsbeziehungen, in intransparenter Weise und vermutlich auch aus wirtschaftlichen Interessen ausgewertet, um damit die politische Willensbildung zu beeinflussen. Damit wurde nicht nur die Integrität des Lebensbereiches persönlicher Beziehungen, sondern auch die Integrität des politischen Kontextes, des demokratischen Systems korrumpiert. Eine Betrachtung, die einzig und isoliert die Manipulation des einzelnen Datensubjektes problematisiert, vermag der systemischen Herausforderung nicht gerecht zu werden. 660

Mit der Freilegung der *subjektrechtlichen und systemischen Schutzdimension* anhand des Blickes auf die Zweckbindungsvorgaben wurde auch die *dynamisch-akzessorische Dimension* der Datenschutzthematik herausgearbeitet. Sie hängt aufs Engste mit der systemischen Schutzdimension zusammen: Mit der Zweckbindung werden Personendaten in einem bestimmten Informationsflussbett oder Verarbeitungskontext gehalten, ein Übertritt in einen anderen Informationskreislauf oder einen anderen Verarbeitungskontext soll verhindert werden. Der bis spätestens 661

935 Zu diesem Ansatz Nissenbaum, *passim*; wie das Bundesverfassungsgericht prägnant ausführte: Keine obrigkeitliche Vollstreckungsmassnahme vermag zu gewährleisten, dass die Bürgerinnen und Bürger korrekt und vollständig an dem für «den Staat» so wichtigen Zensus teilnehmen. Müssten diese fürchten, dass ihre Angaben in weiteren Feldern des Verwaltungsvollzuges ausgewertet würden, bestünde das Risiko, dass die Bürgerinnen und Bürger im Rahmen der statistischen Erhebungen keine korrekten und vollständigen Informationen gäben, womit Ziel und Zweck der statistischen Erhebung aufs Spiel gesetzt würden. Lediglich das Statistikgeheimnis (neben weiteren konkreten Massnahmen) könne das notwendige Vertrauen bei den Bürgerinnen und Bürgern generieren und damit ihre unverzichtbare Kooperation sicherstellen.

zum Zeitpunkt der Erhebung festgelegte Verarbeitungszweck, der transparent gemacht werden muss, bindet die hierfür erhobenen Personendaten in dem Bereich, für dessen Zwecke sie erhoben werden.

662 Die vorangehenden Ausführungen beantworten die Frage nach dem Schutzzweck des Datenschutzrechts wie folgt: Anhand des Zweckbindungsgrundsatzes lassen sich *drei Facetten* des Datenschutzes, des Zwecks des Datenschutzrechts und einer Schutzkonzeptionierung beschreiben: die *subjektivistische*, die *systemische* und die *dynamische* Dimension. Die erste Dimension steht bis heute im Vordergrund, die letzteren beiden dagegen bleiben, obschon im geltenden Datenschutzrecht angelegt, im Hintergrund. Inwiefern die systemisch-institutionelle sowie dynamisch-akzessorische Sichtweise zur Fortentwicklung des Datenschutzrechts fruchtbar gemacht werden können, ja müssen, wird im letzten Kapitel dieser Arbeit erörtert.[936]

663 Nunmehr ist in Kürze auf die beiden Grundsätze der Datenrichtigkeit und -sicherheit einzugehen, um den Katalog der gemeinsamen und allgemeinen Verarbeitungsgrundsätze abzurunden.[937]

5. Die Vorgaben an die Richtigkeit von Personendaten

5.1. Gesetzliche Entwicklungen und Inhalte

664 Mit der Datenrichtigkeit befasst sich explizit Art. 5 DSG, dessen Abs. 1 verschiedene Pflichten gegenüber den Verarbeitenden formuliert und dessen Abs. 2 DSG einen Berichtigungsanspruch des Datensubjektes verbürgt. Der Inhalt des Richtigkeitsgebotes gemäss Art. 5 Abs. 1 DSG in seiner qua Novelle von 2006 verankerten Fassung ist in *vielerlei Hinsicht unklar.* Der vormaligen Version «Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern», wurde ein zweiter Satz angefügt:

> «Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.»

665 Der vergleichende Blick auf die Divergenz zwischen dem Normtext gemäss Art. 5 Abs. 1 DSG und der DSGVO macht eine erste Unklarheit der Bestimmung des DSG sichtbar: Während Art. 5 Abs. 1 lit. d DSGVO verlangt, dass Personendaten bezüglich des verfolgten Zwecks richtig und erforderlichenfalls aktuell sein müssen, stipuliert das DSG in seinem Art. 5 Abs. 1 vorab eine *Pflicht zur Vergewisse-*

936 Beachte nach Totalrevision zu den Befugnissen des EDÖB Art. 49 ff. nDSG, wobei er im Rahmen von Empfehlungen und Leitfäden zur guten Praxis erarbeitet und hierbei die «Besonderheiten des jeweiligen Anwendungsbereichs» berücksichtigt.

937 Hierzu sei auf die einschlägige Kommentar- und Spezialliteratur verwiesen.

rung bezüglich der Richtigkeit von Personendaten, nicht aber ein allgemeines Gebot, wonach nur richtige Personendaten verarbeitet werden dürfen. Beide Normtexte sprechen sodann von «angemessenen Massnahmen», um die Richtigkeit resp. Vollständigkeit der Personendaten sicherzustellen. Eine «Prüfungspflicht» in Bezug auf die Datenrichtigkeit und Vollständigkeit sowie die Verpflichtung, angemessene Massnahmen zur Sicherstellung der faktischen Richtigkeit sowie Vollständigkeit zu ergreifen, ist zumindest dem Wortlaut nach nicht dasselbe wie eine Pflicht, die Richtigkeit der Personendaten selbst sicherzustellen. Die Aspekte können damit auch auf einem Zeitstrahl, der den «Lebenszyklus» von Personendaten und ihrer Verarbeitung in den Blick nimmt, reflektiert werden.

666 Die Totalrevision inkludiert die Vorgaben in Bezug auf die Datenrichtigkeit systematisch überzeugend neu in den Katalog der allgemeinen Verarbeitungsgrundsätze, niedergelegt in Art. 6 Abs. 5 DSG. Die Bestimmung lautet:

> «[5] Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern. Sie oder er muss alle angemessenen Massnahmen treffen, damit die Daten berichtigt, gelöscht oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind. Die Angemessenheit der Massnahmen hängt namentlich ab von der Art und dem Umfang der Bearbeitung sowie vom Risiko, das die Bearbeitung für die Persönlichkeit oder Grundrechte der betroffenen Personen mit sich bringt.»

667 Das Gebot der Richtigkeit wird damit etwas detaillierter normiert, wobei weiterhin die «Pflicht zur Vergewisserung» statuiert wird. Auf die explizite Verankerung eines Aktualisierungsgebotes wird verzichtet. Der Berichtigungsanspruch resp. -vermerk des Datensubjektes wird nach Totalrevision neu mit Art. 32 Abs. 1 und Abs. 3 nDSG verbürgt. In Anbetracht der Totalrevision soll punktuell insoweit auf die Herausforderungen des noch geltenden Art. 5 Abs. 1 DSG eingegangen werden, als daraus ein Erkenntnisgewinn auch für die datenschutzrechtlichen Entwicklungen gezogen werden kann.

668 Die Richtigkeit von Personendaten kann nicht isoliert beurteilt werden. Vielmehr bedarf sie der *Kontextualisierung*. Entsprechend wird sie auch als «relativ» beschrieben und von Gesetzes wegen in einen Bezug zum *Verarbeitungszweck* gesetzt.[938] Als verletzt gilt der Verarbeitungsgrundsatz gemäss Art. 5 Abs. 1 DSG sodann, wenn es der Verarbeitende unterlassen hat, die Richtigkeit von Personendaten zu überprüfen *und* die Personendaten tatsächlich nicht richtig sind.

669 Die Anforderungen an den Prüfungsmassstab hinsichtlich des «Sich-Vergewisserns» betreffend die Datenrichtigkeit dürften höher sein, wenn verarbeitende Stellen Personendaten nicht unmittelbar beim Betroffenen erheben. «Vergewis-

938 Illustrativ das Beispiel Rosenthal, HK-DSG, Art. 5 N 2.

sern» verlange die hinreichende Aufmerksamkeit und Sorgfalt, um in angemessener Weise sicherzustellen, dass die erhobenen Daten richtig sind.[939] Art. 5 Abs. 1 DSG stipuliere eine *Vergewisserungspflicht*, was – so die Kommentarliteratur – gerade nicht mit einem Gebot, nur richtige Personendaten zu verarbeiten, gleichzusetzen sei.[940] Letzteres ergäbe sich aus anderen und weiteren Datenverarbeitungsgrundsätzen.[941] Als «richtig» i. S. v. Art. 5 Abs. 1 DSG beurteilt werden Personendaten, wenn sie Tatsachen in Bezug auf die betroffene Person sachgerecht sowie aktuell wiedergeben und ein vollständiges, wahrheitsgetreues (objektives) Bild liefern.[942]

670 Umstritten ist das Verhältnis der Richtigkeitsvorgaben in Bezug auf eine anfängliche gegenüber einer sukzessiv zu wiederholenden Prüfungs- resp. Verifizierungspflicht mit kontinuierlich andauernden Pflichten zur Berichtigung, Vervollständigung, Aktualisierung.[943] Damit ist die Frage nach der Relation zwischen dem ersten Satz und dem zweiten, 2006 eingeführten Satz sowie dessen Haupt- und Relativsatz aufgeworfen. Die Interpretationen divergieren:

671 Wermelinger/Schweri konstatieren, dass sich der «neue» Regelungstext (eingefügt 2006) auf den ersten Blick wie eine Verschärfung des Rechts ausnähme. Doch bei Lichte betrachtet handle es sich um das Gegenteil, «eine Relativierung der Nachführungspflicht». Mit der sog. Nachführungspflicht sei weniger der Charakter der Dauerpflicht und wiederholenden Prüfungspflicht gemeint als vielmehr die Pflicht zur inhaltlichen Bereinigung unrichtiger, veralteter oder unvollständiger Angaben. Der Datenbearbeiter müsse nunmehr angemessene Massnahmen zur Sicherstellung der Richtigkeit nur bezüglich derjenigen Daten treffen, die im Hinblick auf ihren Zweck und ihre Bearbeitung diese Nachführung voraussetzen.[944] Anders die Interpretation von Rosenthal: Seiner Ansicht nach stelle der Satz 2 die Tragweite von Satz 1 klar und zwar relativierend: Eine allgemeine und in zeitlicher Hinsicht regelmässige Nachführungspflicht werde nicht verankert; vielmehr bestünde diese lediglich dort, wo das Risiko einer Persönlichkeitsverletzung vorliege für den Fall, dass unrichtige (resp. unvollständige oder veraltete) Personendaten verarbeitet würden.[945] Nach Maurer-Lambrou/

939 Zur Vergewisserungspflicht, deren Angemessenheit für den Einzelfall zu prüfen ist, Rampini, BSK-DSG, Art. 12 N 11 ff.; Rosenthal, HK-DSG, Art. 5 N 5.

940 So Rosenthal, HK-DSG, Art. 5 N 4; ebenso Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 11.

941 Vgl. BGer 1A.6/2001, E 2.a.; zu Art. 5 Abs. 1 DSG beachte auch BVGer A-7588/2015.

942 Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 4; Schweizer, digma 2007, 64 ff.; Meier, N 745.

943 Ungeachtet eines vom Datensubjekt geltend gemachten Berichtigungsanspruchs, vgl. Art. 5 Abs. 2 DSG und Art. 32 Abs. 1 nDSG.

944 Wermelinger/Schweri, Jusletter vom 3. März 2008, N 14; so auch Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 13.

945 Rosenthal, HK-DSG, Art. 5 N 9; wann dies der Fall ist, wird nicht präzisiert. Der Autor vertritt zugleich, dass sich eine Pflicht, nur richtige Personendaten zu verarbeiten, zwar nicht aus Art. 5

Schönbächler ist eine prinzipiell «regelmässige Fortschreibung» geboten.[946] Epiney/Nüsch differenzieren konsequent zwischen der Verifizierungspflicht und der Berichtigungs- resp. Löschungspflicht und reflektieren diese jeweils auf der Zeitachse. Hierbei vertreten sie, dass es sich bei der Vergewisserungspflicht nicht nur um eine einmalige, initiale Pflicht handle und stattdessen die periodische Überprüfung angezeigt sei. Sodann seien angemessene Massnahmen zu ergreifen, um die als unrichtig eruierten Angaben zu berichtigen oder zu vernichten.[947]

672 Eine vergleichbare Systematisierung des sog. Richtigkeitsgebots findet sich namentlich bei Meier, der zwischen der *materiellen und der temporellen Komponente* unterscheidet.[948] Meier vertritt die Ansicht, dass mit der Revision von 2006 sowohl die Verpflichtung zur Vergewisserung betreffend die Richtigkeit der Daten (an sich und namentlich bereits mit der Erhebung) als auch die Pflicht zur rollenden Aktualisierung aufgrund der Einfügung des zweiten Satzes nicht mehr absolut gelte. Den Verarbeitenden träfe keine allgemeine proaktive Berichtigungspflicht. Vielmehr sei eine Relativierung des Grundsatzes für sich sowie der Pflichten des Bearbeiters vorgenommen worden.[949] Der Autor weist allerdings auf einen einschlägigen Punkt im Rahmen des damaligen Gesetzgebungsprozesses hin: Die Relativierung durch den 2. Satz von Art. 5 Abs. 1 DSG sei auf eine Fehlannahme im Parlament zurückzuführen:[950] Dort ging man mit Blick auf das Regelungsregime im privaten Bereich davon aus, dass gemäss geplanter Neufassung von Art. 12 Abs. 2 lit. a DSG *keine* Rechtfertigungsgründe für einen Verstoss gegen den «Grundsatz der Datenrichtigkeit» möglich seien. Allerdings wurde eine derartige Interpretationsweise des Art. 12 Abs. 2 lit. a DSG bald schon verworfen: Heute ist anerkannt, dass eine Rechtfertigung selbst hier, wenn auch zurückhaltend, möglich sein soll.[951] Verhältnismässigkeitserwägungen würden damit über die Rechtfertigungsgründe einfliessen; eine Relativierung durch die Einfügung eines zweiten Satzes mit besagtem Inhalt wäre unnötig.

673 Vor dem Hintergrund der jüngsten Rechtsentwicklungen ist m. E. hinsichtlich die *Richtigkeitsvorgaben* von Folgendem auszugehen: Die Vergewisserungspflicht ist eine eigenständige Pflicht, deren Missachtung eine Persönlichkeitsverletzung begründet. Eine Vergewisserungspflicht betreffend die Richtigkeit weist zweierlei Ingredienzen auf, eine objektive und eine subjektive.

Abs. 1 DSG, doch aber aus den allgemeinen Bearbeitungsgrundsätzen ergäbe, vgl. N 4; früh verwies Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 29, auf die Problematik von Entscheidungen, die auf unrichtigen, unvollständigen oder veralteten Informationen basieren.

946 Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 13.

947 Epiney/Nüsch, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.94 ff.

948 Meier, N 745.

949 Ders., N 750.

950 Ders., N 751.

951 Vgl. BGE 136 II 508, E 5.2.4.

674 Der Formulierung, wonach man sich über die Richtigkeit von Personendaten zu *vergewissern* hat, liegt eine Basisannahme zugrunde, wonach die Personendaten auch *faktisch* richtig sind – man *vergewissert* sich ihrer Richtigkeit. Gleichwohl scheint der Gesetzgeber keinen ergebnisorientierten, objektiven Fokus einzunehmen. Vielmehr wird die gebotene Sorgfalt, «Anstrengung», die Prüfungspflicht hervorgehoben. Zudem werden die angemessenen Massnahmen zum Kernkriterium gemacht. Damit werden die Richtigkeitsvorgaben an die Zweckvorgaben gekoppelt. Die parlamentarischen Erwägungen dokumentieren, dass der Gesetzgeber dem Richtigkeitsgebot keinen absoluten Geltungsanspruch zuweisen wollte. Es sollte an das Verhältnismässigkeitsgebot gebunden werden.

675 Vorgeschlagen wird an dieser Stelle zudem, die Erwägungen des Google-Street-View-Urteils sinngemäss wie folgt zu integrieren: Auch im Zusammenhang mit der Richtigkeit von Personendaten ist anzuerkennen, dass eine *Nullfehlertoleranz nicht verlangt werden kann*.[952] In dem Entscheid wurde im Rahmen des Verpixelns von Gesichtern usf. eine Fehlertoleranz von einem Prozent akzeptiert, was analog leitend sein könnte.[953] Entsprechend ist im Geiste der schon für die Physik anerkannten «Fehlerrechnung» ein («angemessener») Fehlerquotient im Rahmen der Richtigkeitsvorgaben anzuerkennen.[954] Massnahmen, welche die Richtigkeit von Personendaten – gemessen am Verarbeitungszweck – gleichwohl nicht innerhalb dieser oder einer im Vorfeld definierten «Fehlermarge» gewährleisten können, sollen ihrerseits dem Grundsatz nach nicht als angemessen qualifiziert werden. Mit anderen Worten sollen sich Verarbeitende nicht hinter das Argumentarium zurückziehen können, «sich vergewissert» und «angemessene Massnahmen» ergriffen zu haben, wenn hieraus nicht auch als Resultat – gemessen am Zweck – ein *Mindestquotient an Richtigkeit, Vollständigkeit und Aktualität* resultiert. Die Vergewisserungspflicht sowie die angemessenen Massnahmen sind somit *objektiv und ergebnisorientiert* zu interpretieren. Sie haben als Resultat ein bestimmtes Niveau der Richtigkeit zu erreichen.

676 Eine Relativierung ist gleichwohl angezeigt: Sofern eine Unrichtigkeit *keinen Einfluss auf die Zweckerfüllung hat*, kann sie unter Umständen toleriert werden.[955] Sodann gibt es Personendaten, deren Speicherung gerade in der nicht aktuellen resp. aktualisierten Weise geboten ist. Exemplarisch sind die Angaben zu einer Person zum jeweiligen Untersuchungszeitpunkt durch eine Ärztin (Gewicht, Hör-

952 BGE 138 II 346, Regeste und E 10.6.2.

953 So Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.29 ff. mit Hinweis auf BGE 138 II 346, E 10.7.

954 Vgl. allerdings zum Ausmass der Fehlerhaftigkeit im Rahmen von Kreditauskünften vertiefend unter dem Vollzugsdefizit dritter Teil, VII. Kapitel, B.2.; zur Problematik der Fehlerhaftigkeit auch im Zusammenhang mit Auskunfteien, insb. auch Kreditauskunfteien bereits Forstmoser, SJZ 1974, 217 ff., 218 f.

955 Vgl. hierzu sogleich vertiefend.

und Sehvermögen, Blutdruck, Puls usf.).[956] In diesem Zusammenhang ist zu beachten, dass archivierte Daten keiner Aktualisierung bedürfen.[957] Wird mit geschätzten und ca.-Angaben gearbeitet, ist für den Fall, dass ebendies angegeben wird, ebenso von einer Richtigkeit auszugehen, sofern die Personendaten (in zutreffender Weise) innerhalb der angegebenen Marge liegen.

677 Im Übrigen ist dem Grundsatz nach anzunehmen, dass sich eine verarbeitende Stelle nicht mit Erfolg auf «unzumutbare Massnahmen» berufen können soll, die nicht dazu führen, ein mit einem Fehlertoleranzquotienten versehenes Richtigkeitsniveau der Personendaten zu erreichen, sofern die Zweckerreichung untergraben wird. In diesem Fall ist der Verarbeitungsprozess aus datenschutzrechtlicher Perspektive nicht nur im Lichte der Richtigkeitsvorgaben an sich als ungenügend zu bezeichnen.

678 Der Grundsatz der Datenrichtigkeit erstreckt sich über den *gesamten Zyklus* von Datenverarbeitungsprozessen. Die Vorgaben für die Datenrichtigkeit sind wiederholt und regelmässig zu beachten, wobei im gerade beschriebenen Sinne Korrekturen, Aktualisierungen resp. Löschungen vorzunehmen sind. Es handelt sich damit um Dauerpflichten – unter dem Vorbehalt von Personendaten, die ihrerseits als «historische Daten» gelten.[958] Eine über einen bestimmten Fehlerquotienten hinausgehende Unrichtigkeit ist als Verletzung des Richtigkeitsgebotes zu qualifizieren, sofern damit die Erreichung des Zweckes torpediert wird, wobei Rechtfertigungsgründe hierfür zumindest theoretisch (wenn auch mit Zurückhaltung) nicht ausgeschlossen sind.

679 Für die präsentierte Auslegung von Art. 5 DSG ist auch das der Logik entspringende methodenrechtliche Argument in Erinnerung zu rufen, wonach ein Abweichen von einem Gesetzeswortlaut bei krass stossenden Ergebnissen resp. bei einem offenkundigen Irrtum des Gesetzgebers selbst *contra verba legis* zulässig ist.[959] Logische Folgerung aus diesem Argument ist, dass eine Auslegung, die im Rahmen des Wortlautes eines Gesetzestextes liegt, bei irrtümlicher Annahme des Gesetzgebers *a fortiori* zulässig sein muss.

680 Zur Untermauerung der hier vertretenen erhöhten Anforderungen an die Gewährleistung der Richtigkeitsvorgaben seien sodann die folgenden systematischen Erwägungen ins Feld geführt: Die Pflichten im Zusammenhang mit der Richtigkeit von Personendaten hängen untrennbar mit weiteren *generalklauselartigen Verarbeitungsgrundsätzen* zusammen, vorab mit den aus dem *Verhältnismässigkeitsgrundsatz* abgeleiteten Vorgaben. Damit sind sie zugleich eng mit den

956 Vgl. Herbst, BeckKomm-DSGVO, Art. 5 N 61.
957 Vgl. Ders., a. a. O.
958 Hierzu Rosenthal, HK-DSG, Art. 5 N 2.
959 Vgl. BGE 128 I 34, E 3.

Zweckvorgaben verzahnt.[960] Die Verarbeitung von unzutreffenden Personendaten kann regelmässig nicht geeignet sein, den damit verfolgten Verarbeitungszweck zu erfüllen, weshalb die Verarbeitung zugleich regelmässig unverhältnismässig sein dürfte.[961] Auch das Aktualitäts- resp. Aktualisierungsgebot kann entsprechend als Ausdruck des Verhältnismässigkeitsgebots gelesen werden. Die endlose Speicherung von Personendaten, die ihre Richtigkeit und Aktualität längst verloren haben, ist folglich (unter dem Vorbehalt namentlich von Archivierungsvorgaben) prinzipiell unzulässig.

681 Die hier vertretene Auslegung, wonach die Richtigkeit von Personendaten nicht nur im Zeitpunkt der Erhebung zu prüfen und unter Berücksichtigung eines Fehlerquotienten umzusetzen ist, wobei nach geltendem DSG eine rollende Überprüfungspflicht und daran anschliessend eine Berichtigungs- resp. Löschungspflicht einzuhalten sind, wird somit innergesetzlich von einer *systematischen Auslegung* getragen. Die objektivierte und ergebnisorientierte Rückkoppelung der Gebote des Richtigkeitsgrundsatzes nimmt eine Garantenstellung für die Einhaltung weiterer Verarbeitungsgrundsätze ein: So gewährleistet eine regelmässige Überprüfung der Richtigkeit, Aktualität und Vollständigkeit von Personendaten (gemessen am Verarbeitungszweck) und darauf basierend das Ergreifen von Folgemassnahmen, dass dem Grundsatz der Verhältnismässigkeit und der Zweckbindung effizient und nachhaltig Nachachtung verliehen wird.

682 Eine systemische Auslegung berücksichtig internationale resp. supranationale Normtexte. Hierbei ist namentlich Art. 5 Abs. 4 lit. d der am 8. Mai 2018 verabschiedeten Modernisierung der Datenschutzkonvention 108 des Europarates zu erwähnen.[962] Der Bestimmung gemäss müssen Personendaten «accurate, and, where necessary, kept up to date» sein.[963] Personendaten haben richtig zu sein, womit das Ergebnis zum Kriterium erhoben wird und nicht eine Vergewisserungspflicht oder «angemessene Massnahmen». Die Konjunktion «and» verdeutlicht zudem, dass es sich bei der Berichtigung und Aktualisierung um zwei eigenständige Pflichten handelt, wobei die Aktualisierungspflicht nicht absolut gilt.[964]

683 Ähnlich lautete Art. 6 Abs. 1 lit. d der EU-Richtlinie 95/46, nach der die Mitgliedstaaten sicherzustellen hatten, dass personenbezogene Daten richtig sind

960 Vgl. Meier, N 752.

961 Zur Alimentierung «wirtschaftlicher» Begehrlichkeiten, der hohen Fehlerhaftigkeit namentlich von Score-Werten im Zusammenhang mit Kreditauskünften und der über die Verletzung des datenschutzrechtlichen Richtigkeitsgebotes hinausgehenden Dimension der Problematik vertiefend dritter Teil, VII. Kapitel, B.2.

962 Der Schweizerische Bundesrat verabschiedete das Änderungsprotokoll im Herbst 2019 <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-76861.html> (zuletzt besucht am 30. April 2021).

963 Daten:recht, Europaratskonvention 108 verabschiedet, Zürich 2018, <http://datenrecht.ch/europaratskonvention-108-verabschiedet> (zuletzt besucht am 30. April 2021).

964 Das naheliegende Illustrationsbeispiel sind Archive, die personenbezogene Angaben enthalten.

und, sofern erforderlich, aktualisiert werden.[965] Die Richtlinie wurde ersetzt durch die DSGVO. Art. 5 Abs. 1 lit. d DSGVO verlangt, dass die Personendaten sachlich richtig sind. Es handelt sich damit um ein objektives Kriterium.[966] Verlangt wird die Übereinstimmung von Personendaten mit der Realität.[967] Darüber hinaus müssen Personendaten (erforderlichenfalls) auf dem neusten Stand sein; es sind angemessene Massnahmen zu treffen, damit Personendaten, die für den Verarbeitungszweck unrichtig sind, unverzüglich aktualisiert resp. gelöscht werden. Es greifen drei Grundsatzpflichten: Das Verbot der Erhebung und Speicherung unrichtiger Personendaten, das Gebot der Aktualisierung unrichtig gewordener Personendaten sowie dasjenige der Löschung resp. Berichtigung gespeicherter unrichtiger Personendaten.[968]

Besagte Vorgaben gelten gleichwohl nicht absolut. Die DSGVO verlangt unter Ausrichtung am Verarbeitungszweck «angemessene Massnahmen». Indem nach DSGVO allerdings an den Richtigkeitsgrundsatz ein objektiver Massstab angelegt wird (und keine Vergewisserungspflicht), dürfte unter Sichtung der Kommentarliteratur das Folgende gelten: Personendaten haben gemessen am Verarbeitungszweck richtig und aktuell zu sein, unrichtige resp. veraltete Personendaten sind zu berichtigen resp. zu löschen. Eine Berufung auf die Angemessenheit der Massnahmen, die kein Mindestmass an Richtigkeit im Ergebnis zu erreichen vermögen, dürfte ausgeschlossen sein. Zugleich bringt Art. 5 Abs. 1 lit. d DSGVO unmissverständlich zum Ausdruck, dass es sich bei der Sicherstellung der Datenrichtigkeit *und* der Aktualität um einen Prozess handelt, der kontinuierlich resp. wiederholend durchzuführen ist. Die DSGVO räumt zudem individualrechtliche Ansprüche der Datensubjekte ein, die auf die Gewährleistung der Richtigkeits- und Aktualitätsvorgaben abzielen, vgl. zum Berichtigungsanspruch des Datensubjektes Art. 16 DSGVO und zum Löschungsbegehren Art. 17 sowie Art. 21 Abs. 1 und Abs. 2 DSGVO. 684

Entsprechende Ansprüche finden sich auch im DSG mit dem Berichtigungsanspruch im Sinne eines Betroffenenrechts, vgl. Art. 5 Abs. 2 DSG resp. Art. 32 Abs. 1 nDSG (in engem Zusammenhang damit stehen auch Löschungsansprüche).[969] Die Berichtigung ist kosten- und formlos möglich.[970] Während ein Teil 685

965 Die Richtlinie wurde von Birnhack, CLSR 2008, 508 ff., 515 als das erfolgreichste internationale Instrument zur Globalisierung des Datenschutzrechts beschrieben; der Autor weist zudem darauf hin, dass die Richtlinie von amerikanischen Wissenschaftlern als aggressiv beschrieben wurde, 519; zur Bedeutung, das Datenschutzrecht «international» zu adressieren, Cottier, SRIEL 2016, 255 ff.

966 Vgl. Herbst, BeckKomm-DSGVO, Art. 5 N 60.

967 Ders., a. a. O., Art. 5 N 60.

968 Hierzu Reimer, NomosKomm-DSGVO, Art. 5 N 34 ff.

969 Im Einzelnen zu diesem Recht, das unentgeltlich und formlos geltend gemacht werden kann, Rosenthal, HK-DSG, Art. 5 N 12 ff.; Meier, N 761 ff.; vgl. sodann den Anspruch gemäss Art. 15 Abs. 3 DSG.

970 Mit Hinweis auf das Musterformular des EDÖB Rosenthal, HK-DSG, Art. 5 N 15.

der Lehre dieses Individualrecht in Abhängigkeit von Ziel, Funktion oder Typ der Bearbeitung einschränken will, vertritt Meier mit Referenz auf ein Recht auf informationelle Selbstbestimmung, dass das Berichtigungsrecht uneingeschränkt gelten müsse.[971] Auch Widmer tritt in zutreffender Weise dafür ein, dass selbst geringfügige Fehler dem Berichtigungsanspruch zugänglich seien.[972] Der Anspruch auf Berichtigung lässt sich als Element des sog. Selbstdatenschutzes bezeichnen.[973] Nachweis und Beweis der Unrichtigkeit von Personendaten obliegen dann der betroffenen Person. Misslingt der betroffenen Person der Unrichtigkeitsbeweis, wird sie auf die Möglichkeit eines Bestreitungsvermerks gemäss Art. 15 Abs. 2 DSG und Art. 32 Abs. 3 nDSG verwiesen. Im Lichte der datenschutzrechtlichen Realitäten greift allerdings das individualrechtliche Instrumentarium über weite Strecken ins Leere.[974] Die Betroffenen werden nur ausnahmsweise von Verstössen gegen die Verarbeitungsvorgaben Kenntnis erlangen.[975]

686 Nach diesen Auslegungserwägungen zum Regelungsinhalt im Zusammenhang mit der Datenrichtigkeit ist bezüglich der Gewährleistung des Grundsatzes mit seinen Unteraspekten auf die Herausforderungen und insb. die Interessenlagen einzugehen.

5.2. Herausforderungen

687 Die Verarbeitung falscher, veralteter und unvollständiger Angaben bleibt aus Datenschutzperspektive ein Kernproblem. Der Grundsatz wird als häufig verletzt beschrieben. Verarbeitende stossen hinsichtlich der Umsetzung allfälliger Löschungsvorgaben auf technische Hürden. Das Richtigkeitsgebot und die Problematik der (Un-)Richtigkeit wird im Rahmen der Bedeutung des sog. Vollzugsdefizites im dritten Teil dieser Arbeit anhand der Kreditauskünfte vertieft thematisiert. Hier wird sich zeigen, weshalb *nur* eine *ergebnisorientierte Interpretation* der Richtigkeitsvorgaben den Zielen und Zwecken des Datenschutzrechts Rechnung zu tragen vermag.[976]

688 Die Bedeutung der datenschutzrechtlichen *Richtigkeitsvorgaben* hängt damit von einer Auseinandersetzung mit den *Interessenlagen sowie Schutzmotivationen* ab:

971 Meier, N 768.
972 Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5 N 5.55.
973 Vgl. zum Selbstdatenschutz Pärli, digma 2011, 66 ff., 67; zu den verschiedenen Betroffenenrechten Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5; spezifisch zum Löschungsanspruch gemäss DSGVO als Selbstdatenschutz Gesmann-Nuissl, InTeR 2018, 201 ff., 208.
974 Spezifisch zur seltenen Geltendmachung des Berichtigungsanspruches Rosenthal, HK-DSG, Art. 5 N 17.
975 Ein Szenario, in welchem das Datensubjekt von der Unrichtigkeit von Personendaten Kenntnis erlangt, ist im Rahmen der Bonitätsauskünfte dann gegeben, wenn einer Person, die stets ihre Rechnungen fristgerecht bezahlt hat, dennoch beispielsweise ein Kreditkauf aufgrund eines «vermeintlich» schlechten Score-Wertes verweigert wird.
976 Vgl. hierzu dritter Teil, VII. Kapitel, B.2.

Das *Richtigkeitsgebot* dient – knüpft man am individualrechtlichen Ansatz des Datenschutzrechts an – zunächst dem *Schutz und den Interessen der Betroffenen*. Persönlichkeitsverletzungen durch die Bearbeitung unrichtiger Daten sollen verhindert werden, vgl. für den privaten Bereich auch Art. 12 Abs. 2 lit. a i. V. m. Art. 5 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 Abs. 5 nDSG. Wie gezeigt, verbürgen sowohl das DSG als auch die DSGVO subjektive Rechte resp. Betroffenenrechte der Datensubjekte, um die Richtigkeitsvorgaben durchzusetzen. Solche Rechtsbehelfe stehen in der Tradition der Anknüpfung des Datenschutzrechts im Schutz der Person und einer individualgüterrechtlichen Rechtsposition.

689 Allerdings wurde gezeigt, dass gerade mit der jüngsten datenschutzrechtlichen Weiterentwicklungswelle eine neue Facette in die Rechte integriert wird. Sie stellt sich neben die individualrechtliche Abstützung: Integriert wird eine prozessorientierte Sichtweise, welche die proaktive Dauerpflicht der Verarbeitenden anerkennt und die Etablierung entsprechender organisatorischer und prozeduraler Massnahmen gebietet, um das Richtigkeitsgebot zu erfüllen. Damit zeigt das Datenschutzrecht sowohl in der EU mit der DSGVO als auch in der Schweiz mit der Totalrevision eine markante Abkehr resp. Weiterentwicklung eines ursprünglich ganz im defensivrechtlichen Individualgüterrechtsschutz verankerten Datenschutzrechts. Gleichwohl bleibt dieser Ansatz nicht nur im DSG, sondern auch in der DSGVO erhalten.

690 Das Richtigkeitsgebot wird durch weitere Aspekte faktisch auf den Prüfstand gestellt: Es gilt zwar als im rechtlich geschützten Interesse des Individuums. Die Verarbeitenden haben dieses neu durch die Etablierung und den Einsatz angemessener technischer, organisatorischer und prozeduraler Instrumente sowie Massnahmen zu gewährleisten. Allerdings korrelieren die Interessen an der Einhaltung und Erfüllung der Richtigkeitsvorgaben nur teilweise mit dahinterliegenden *geschäftlichen Interessen der Bearbeitenden*.

691 Eine Korrelation lässt sich wie folgt beschreiben: Für die Bearbeitenden haben in erster Linie richtige, aktuelle und vollständige Daten einen (Aussage-)Wert, womit die Einhaltung der datenschutzgesetzlichen Vorgaben durch dahinterliegende Geschäftsinteressen motivational abgesichert wird. Die Einhaltung der Richtigkeitsgebote ist insofern durchaus im Geschäftsinteresse der Verarbeitenden. Unrichtige Personendaten können für personendatenverarbeitende Stellen nutzlose Aufwendungen verursachen.[977] Marketingstrategien und -massnahmen beispielsweise, die auf personenbezogener Werbung durch Zustellung von Katalogen basieren, generieren Fehl- und Mehraufwand, sofern sie auf Falschinformationen beruhen. Bei Data-Mining und Warehousing können bereits die ins

977 Vgl. Meier, N 743.

Data Warehouse integrierten Rohdaten unrichtig oder veraltet sein.[978] Werden an sich richtige Daten ungleicher Präzision und Herkunft – vom Anmeldeformular, von Scannerkassen oder Drittanbietern – aus ihrem ursprünglichen Kontext extrahiert und in verkürzter Form in ein Informationssystem eingespeist, kann dies zudem aufgrund des Bezugsverlustes ein verzerrtes Gesamtbild ergeben und zu falscher Kundenbewertung führen.[979] Gerade bei automatisierten personenbezogenen Analyseinstrumenten wird davon ausgegangen, dass mehrere Faktoren zu einem hohen Fehlerpotential beitragen können.[980] Verarbeitungen von unrichtigen Personendaten sind hier *sowohl für die Datensubjekte als auch für die verarbeitenden Unternehmen kritisch* – und zwar nicht nur aus datenschutzrechtlicher Perspektive, sondern auch aus Effizienzerwägungen mit Blick auf Geschäftsaktivitäten. In entsprechenden Szenarien herrscht *Kongruenz* dergestalt, dass sowohl die Interessen der Betroffenen als auch die der Bearbeitenden auf die Richtigkeit der Daten gerichtet sind. Die Verantwortlichen dürften damit eine mehrfache Motivation haben, den datenschutzrechtlichen Grundsatz der Richtigkeit einzuhalten: die Einhaltung der Datenschutzgesetzgebung an sich, damit einhergehend der Schutz der Individuen (als Datensubjekte, aber auch z. B. als Konsumentinnen und Konsumenten) sowie die Effizienz der eigenen Geschäftsaktivitäten, denen Personendatenverarbeitungshandlungen dienen.

692 Anders scheint die Einhaltung der weiteren datenschutzrechtlichen Verarbeitungsgrundsätze (für den Fall, dass man die Gültigkeit eines Gesetzes resp. des Datenschutzgesetzes und das Handeln im Einklang mit diesem Gesetz nicht als hinreichenden Anreiz für ein rechtskonformes Handeln beurteilt) keinen vergleichbaren direkten Vorteil für die Verarbeitenden zu generieren. Vielmehr handelt es sich um einen Vorteil, der erst in jüngerer Zeit mit der Aufwertung der Bedeutung des Datenschutzrechts, aber auch der Medienlandschaft verbunden ist: die Vertrauenswürdigkeit in das Geschäftsgebaren der Handelnden und die Integrität des Markts.

693 Die vorangehenden Befunde sind vor dem Hintergrund, wonach Verstösse gegen das DSG bislang nur ganz selten Konsequenzen nach sich zogen – was gleichzeitig Ausdruck und Mitursache für das im dritten Teil zu vertiefende Vollzugsdefizit des Datenschutzrechts ist – von besonderem Interesse für diese Studie.

694 Dafür, dass das Richtigkeitsgebot nur ungenügend umgesetzt wird, gibt es verschiedene Ursachen. Dazu gehören die Techniken wie der Aufwand und damit

978 Hierzu und zu weiteren datenschutzrechtlichen Herausforderungen von Data Mining und Data Warehousing Burkert, in: Jung/Winter (Hrsg.), 117 ff., 119 f.

979 M. w. H. Peter,136 f.; Maurer-Lambrou/Schönbächler, BSK-DSG, Art. 5 N 6 ff.; Rampini, BSK-DSG, Art. 12 N 9; hier zeigt sich übrigens die Rückkoppelung des Richtigkeits- an das Zweckbindungsgebot.

980 Schweizer, digma 2007, 64 ff.

auch die Interessen der verschiedenen involvierten Parteien an der (Nicht-)Einhaltung des Grundsatzes. Sodann ist zu attestierten, dass es Praktiken gibt, in denen die Datenbearbeitenden gerade kein *Interesse* haben, dem Richtigkeitsgebot Nachachtung zu verschaffen: Weder das Datenschutzrecht an sich noch die geschäftliche Motivationslage veranlassen in diesen Fällen die Verarbeitenden dazu, die Richtigkeitsgebote der Datenschutzerlasse einzuhalten. Angesprochen ist an erster Stelle die Praxis der Kreditauskunfteien.[981] Falsche, inakkurate, vorurteilsbehaftete oder aufgrund einer unvollständigen Datenlage unzutreffende Bonitätsauskünfte führen hier zur wirtschaftlichen Alimentierung sowohl der Kreditauskunfteien als eigenständiger Branche als auch der krediteinräumenden Institutionen.[982] Der Bereich der Bonitätsauskünfte gilt aus datenschutzrechtlicher Perspektive seit jeher als neuralgisch.[983] Hier zeigen sich empfindliche Schwachstellen, nicht nur bezogen auf die Transparenz der Verarbeitungsprozesse, sondern auch bezüglich der Richtigkeits- und Vollständigkeitsvorgaben. Letztere bezeichnet Buchner als unverzichtbares Korrelat zulässiger Datenverarbeitung, wobei insofern gravierende Defizite und Devianzen nachgewiesen wurden.

695 In den USA dokumentierten mehrere Studien eine hohe Fehlerquote von Kreditauskünften. Eine Untersuchung geht davon aus, dass rund ein Fünftel aller amerikanischen Verbraucher dem Risiko ausgesetzt ist, aufgrund fehlerhafter Credit Scores in eine *höhere* Risikoklasse eingeordnet zu werden und infolgedessen beträchtliche finanzielle Einbussen zu erleiden. Für den amerikanischen Hypothekarmarkt wird die Mehrbelastung mit bis zu USD 124'000.00 beziffert für den Fall, dass eine Schuldnerin aufgrund einer fehlerhaften Datenverarbeitung zu Unrecht einer höheren Risikoklasse zugewiesen wird.[984]

696 Für die Fehlerhaftigkeit kann es verschiedene Ursachen geben – Identifikationsfehler und -verwechslungen, Falschauskünfte, unvollständige oder widersprüchliche Akten, im Rahmen von automatisierten Entscheidungen auch «vorprogrammierte» Vorurteile.[985] Die Wohnlage kann, muss aber keineswegs einen richtigen Schluss auf die Kreditwürdigkeit und Liquidität einer Person zulassen. Die Konsequenzen von dergestalt unrichtigen Personenangaben tragen alsdann in erster Linie die Individuen, wobei diese – in Zahlen gefasst – schwer wiegen. Für die in-

981 Vertiefend hierzu dritter Teil, VII. Kapitel, B.2.; zu den jüngsten technischen und faktischen Möglichkeiten vgl. Radlanski, 26; vertiefend zum Kreditscoring Helfrich, *passim*; kritisch zu diesem vor dem Hintergrund des BDSG bereits Möller/Florax, NJW 2003, 2724 ff.; kritisch auch Mallmann, 80 ff., zu den Handels- und damit Kreditauskunfteien.

982 Letztere können basierend auf unter Umständen zu Unrecht schlechten Score-Werten höhere Zinsfüsse veranschlagen.

983 Buchner, 119 ff.; Möller/Florax, NJW 2003, 2724 ff.

984 M. w. H. Buchner, 124 f.

985 Der Name beispielsweise ist kein zuverlässiger Identifikator, was auch ein Grund für Überlegungen ist, einheitliche Personen-Identifikatoren wie die AHV-Nummer zu implementieren; vgl. insb. zur Richtigkeit und Vollständigkeit im Kontext von Kreditauskunfteien Mallmann, 89 ff.

volvierten Unternehmen erweist sich diese «Unrichtigkeit» der Datenverarbeitungen umgekehrt als lukrativ. Der Sektor alimentiert sich selbst anhand fehlerhafter Auskunfteien, die den Anschein erwecken, besonders rational-analytisch, mathematisch und «zuverlässig» zu sein. Die Praktiken sind aus datenschutzrechtlicher Perspektive problematisch. Dies gilt nicht nur hinsichtlich des Richtigkeitsgebots, sondern auch mit Blick auf weitere Verarbeitungsgrundsätze, insb. die Vorgaben in Bezug auf die Transparenz und Einwilligung, zudem das Verhältnismässigkeitsgebot.[986] Die Verarbeitung von und der Umgang mit «unrichtigen resp. nicht akkuraten» Personenangaben ermöglicht einen *wirtschaftlichen Profit zulasten der Betroffenen*. Allerdings ist dies wohl bloss kurzfristig vorteilhaft für die profitierenden Unternehmen. Denn eine solche Praxis verletzt nicht nur die datenschutzrechtlichen Verarbeitungsgrundsätze, allem voran das Richtigkeitsgebot. Sie beschädigt das Vertrauen in den Finanzsektor selbst, was dessen Produktivität untergräbt.[987]

697 Genau diesen Aspekt greift der *Fair Credit Reporting Act* mit seinem *Amending Act*, dem *Fair and Accurate Credit Transactions Act* von 2003 auf: § 1681 hält fest, dass der Banksektor von einem «fair and accurate credit reporting» abhängig sei. Unfaire und inakkurate Kreditauskünfte dagegen erodieren das Vertrauen der Allgemeinheit – ein Vertrauen, auf das ein effizienter Banksektor angewiesen sei. Damit ist erneut eine *kontextuelle Dimension des Datenschutzes* anerkannt.

698 Über die Richtigkeitsvorgaben wurde die kontextuelle Ingredienz des Datenschutzrechts sichtbar: explizit für das US-amerikanische Recht über den *Fair Credit Reporting Act*, der bereichsspezifisch und folglich bereichsschützend reguliert. Die Richtigkeit und Akkuratheit der Personendaten sind von entscheidender Bedeutung. Indirekt fliesst diese kontextuelle Schutzdimension ebenso in die allgemeine Datenschutzgesetzgebung der Schweiz und der EU ein, und zwar über das Richtigkeitsgebot.

699 An dieser Stelle bestätigt sich somit ein Befund, wie ihn auch die Analyse des Volkszählungsurteils zu Tage förderte: Die kontextuelle Relevanz der Richtigkeit und Vollständigkeit von Personenangaben wurde in besagtem Entscheid bereits vom Bundesverfassungsgericht festgestellt. Mit der Gewährleistung entsprechender Richtigkeits- und Vollständigkeitsvorgaben sollten nicht nur individuelle,

986 Dass gerade der Bereich des Profiling und automatisierter Analyseverfahren und Einzelfallentscheidungen den Datenschutz herausfordert, artikulieren die DSGVO, aber auch die Totalrevision des DSG. Sie widmen diesen Prozessen neu spezifische datenschutzrechtliche Bestimmungen. Insofern ist auf die Vorgaben im Zusammenhang mit der automatisierten Einzelfallentscheidung und dem Profiling hinzuweisen, welche die Gewährleistung nachvollziehbarer Ergebnisse beispielsweise von Scoring-Praktiken erreichen wollen, vgl. Art. 2 lit. f, Art. 13 Art. 15 Abs. 1 lit. h, Art. 22 DSGVO und Art. 5 lit. f und g, Art. 18, Art. 25 Abs. 2 lit. f, Art. 35 nDSG. Im Zusammenhang mit automatisierten Entscheiden setzen die Erlasse primär auf Transparenzvorgaben und Betroffenenrechte.

987 Vertiefend dritter Teil, VII. Kapitel.

sondern ebenso institutionelle Schutzziele erreicht werden – in besagtem Fall die Wahrung der Integrität der statistischen Erhebung.[988]

Im Rahmen der Auseinandersetzung mit den Richtigkeitsvorgaben bestätigt sich, dass eine Sichtweise, die den dynamischen Aspekt der Datenverarbeitungsprozesse sowie der datenschutzrechtlichen Herausforderungen einnimmt, produktiv ist.[989] Beschrieben wurde die primäre und fortwährende Verantwortlichkeit der Verarbeitenden zur Gewährleistung der Vorgaben. Mit der Statuierung einer kontinuierlichen Prüfungs- und Berichtigungs-, Aktualisierungs- resp. Löschungspflicht lässt sich ebenso unter dem Richtigkeitsgebot eine neue Konzeptionierung feststellen. Das Datenschutzrecht hat eine systemrelative sowie eine an kontinuierlichen Datenflüssen orientierte dynamische Dimension. Damit bahnt sich ein Paradigmenwechsel oder zumindest eine Ergänzung des ursprünglichen Ansatzes eines statisch-defensivrechtlichen und isoliert persönlichkeitsrechtlich gedachten Datenschutzrechts den Weg.[990] 700

6. Der Grundsatz der Datensicherheit

Unter dem Stichwort «Datensicherheit» eröffnet sich heute ein weites Feld. Ursprünglich primär mit der Verhinderung von Datendiebstahl oder Hacking assoziiert, könnte man «Datensicherheit» namentlich im Zuge der jüngsten datenschutzrechtlichen Novellierungen als *Schirmbegriff für ein elaboriertes Gefüge* von Vorgaben umschreiben, der sich nicht auf technische und organisatorische Massnahmen beschränkt. Unter dem Tatbestandselement des unbefugten Bearbeitens werden als Bedrohungssituationen insb. die unautorisierte Vernichtung oder Löschung genannt, sodann der unbeabsichtigte Wegfall der Verfügbarkeit, der Diebstahl, die Fälschung, Änderung oder das Kopieren durch Unberechtigte.[991] 701

Nachfolgend wird zunächst der Grundsatz der Datensicherheit gemäss noch geltendem Recht und Art. 7 DSG erörtert. Es folgt ein Abriss über die jüngsten Entwicklungen im Zusammenhang mit der Datensicherheit, wie sie insb. die DSGVO und Totalrevision des DSG bringen.[992] Auch hier verdichten sich die 702

988 Hierzu oben zweiter Teil, V. Kapitel, B.4.2.; zur Gewährleistung von Richtigkeit und Vollständigkeit als Zielfunktion des Datenschutzes allgemeiner bereits Mallmann, 70 ff.

989 Vgl. zum Betrachtungsgegenstand des Datenflusses im Rahmen der Studie zum Kreditscoring der SCHUFA auch Helfrich, 29.

990 Hierzu vertiefend zweiter Teil, VI. Kapitel.

991 Lehmann/Sauter, in: Schweizer (Hrsg.), 135 ff., 142.

992 Vgl. zum Begriff der Verletzung der Datensicherheit Art. 5 lit. h nDSG und zum Grundsatz der Datensicherheit Art. 8 nDSG, zudem zur Meldepflicht bei Verletzungen der Datensicherheit Art. 24 nDSG; sodann relevant sind die Massnahmen gemäss Art. 7 und Art. 22 nDSG; eine gute Übersicht zur Datensicherheit findet sich bei Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 94 ff.; sodann zu Vorgaben zur Datensicherung ausserhalb des DSG, insb. aber nach DSG vgl. Lehmann/Sauter, in: Schweizer (Hrsg.), 135 ff.; zu den Themen Datenschutz und IT-Sicherheit sodann Tinne-

neuen Akzente zu einem *Perspektivenwechsel in der Datenschutzregulierung*, wonach die systematische und konsequente Forderung nach Vorkehrungen zum Datenschutz *und* zur Gewährleistung der Datensicherheit primär von den Verantwortlichen zu implementieren ist. Dabei werden risikobasiert verschiedene Umsetzungsinstrumente vorgesehen. Anhand der Weiterentwicklungen im Zusammenhang mit der Datensicherheit fliesst wiederum eine im Vergleich zu einem einzelfallorientierten, deliktsrechtlich gedachten Verletzungsfall des Datensubjektes, gegen welchen in erster Linie über eine persönlichkeitsrechtliche Klage durch das Individuum vorgegangen werden soll, neue Konzeptionierung ein.[993] Auch hier sind es die datenverarbeitenden Stellen, die früher und an erster Stelle konsequent und nachhaltig in die Pflicht sowie Eigenverantwortung genommen werden, die datenschutzrechtlichen Vorgaben mittels Datenschutzvorkehrungen zu implementieren und eine Strategie resp. ein Programm zur Datensicherheit zu entwickeln, umzusetzen und zu überprüfen.[994]

703 Bei der Datensicherheit handelt es sich um kein starres Konzept. Die Anforderungen lassen sich nicht abstrakt bestimmen. Im Sinne des Grundsatzes aus der Homöopathie «Gleiches mit Gleichem zu heilen» kommt den Technologien und ihrer Fortentwicklung bei der Gewährleistung der datenschutzrechtlichen Datensicherheit besondere Bedeutung zu. Damit verändert sich das, was zur Gewährleistung einer angemessenen Datensicherheit geboten ist, sukzessive. Zudem können Veränderungen in den Geschäftsmodellen Anpassungen der Datensicherheitsmassnahmen bedingen. Die zu treffenden, angemessenen Massnahmen zur Sicherstellung der Datensicherheit hängen stets von den *korrelierenden Risiken* der jeweiligen Verarbeitungshandlungen ab.[995]

704 Art. 7 Abs. 1 DSG fordert angemessene technische und organisatorische Massnahmen, um *unbefugtes Verarbeiten* zu verhindern. Die gemäss Art. 7 Abs. 2 DSG verlangten konkretisierenden Bestimmungen finden sich, den Dualismus des DSG rezipierend, differenziert für den privaten Bereich in Art. 8 ff. VDSG und für den öffentlichen Bereich des Bundes in Art. 20 ff. VDSG (beachte allerdings die im Zuge der Totalrevision des DSG ebenso revidierte Verordnung). Im privaten Bereich sind Verarbeitende zur Gewährleistung der Datensicherheit nicht nur

---

FELD/BUCHNER/PETRI, 413 ff.; einschlägige Bestimmungen finden sich zudem in der ausführenden Verordnung, die mit der Totalrevision des DSG revidiert wird, wobei entsprechende Anpassungen hier nicht integriert werden können.

993 Vgl. zum Persönlichkeitsschutz als drittem Strukturmerkmal zweiter Teil, VI. Kapitel. Ebenda wird der Fokus auf den privaten Bereich verengt.

994 Vgl. Botschaft 2017–1084, 1 ff., 30 und 34.

995 Vgl. STAMM-PFISTER, BK-DSG, Art. 7 N 9 ff.; dazu, dass die Sensitivität der Personendaten einen Einfluss auf die Beurteilung der Angemessenheit der Massnahmen hat LEHMANN/SAUTER, in: SCHWEIZER (Hrsg.), 135 ff., 139; vgl. zu den Sicherheitsmassnahmen zwecks Gewährleistung der Informationssicherheit in Netzwerken im Zusammenhang mit haftungsrechtlichen Fragen der Internet-Provider nach Schweizer Recht ROHN, 41 ff., aber auch 263 ff.

datenschutzrechtlich, sondern ebenso basierend auf Handels- oder Geschäftsgeheimnissen verpflichtet.[996]

705 Mit den Massnahmen zur Gewährleistung der Datensicherheit werden primär solche des Schutzes vor *unberechtigten Zugriffen* durch Datendiebstahl, Phishing sowie vor Datenverlusten, Fälschungen oder widerrechtlichen Verwendungen aufgeführt. Die Sicherung von Personendaten vor dem *Zugriff durch Unbefugte* gilt als Kernelement der Schutzvorgaben; die Konsequenzen unbefugter Zugriffe infolge unzureichender Sicherungsvorkehrungen haben meist weitreichende Auswirkungen, nicht zuletzt, weil grosse Datenmengen mit unter Umständen sensiblen resp. besonders schutzwürdigen Personendaten in den Einflussbereich Unberechtigter gelangen können.[997] Die Verarbeitungshandlungen sind in der Folge kaum mehr kontrollierbar – *a fortiori* nicht durch die Datensubjekte selbst.

706 Allerdings wird vertreten, dass sich die Tragweite von Art. 7 Abs. 1 DSG nicht darin erschöpft, den Zugriff durch Unbefugte zu verhindern. Vielmehr leite der Grundsatz dazu an, ganz allgemein die unbefugte Datenbearbeitung zu verhindern.[998] Art. 7 Abs. 1 DSG verlange generell *angemessene Massnahmen* zur Verhinderung auch unrechtmässiger, unverhältnismässiger oder zweckwidriger Datenbearbeitung i. S. v. Art. 4 Abs. 1–4 DSG. Zur Frage, ob sich Art. 7 DSG über einen eigenständigen Regelungsgehalt hinausgehend auch auf die Grundsätze von Art. 4 Abs. 1–4 DSG erstreckt, soll nicht detailliert erörtert werden, zumal die Debatte eher theoretischer Natur ist.[999]

707 Die Pflicht, angemessene technische und organisatorische Massnahmen zur Sicherstellung der Einhaltung der datenschutzrechtlichen Verarbeitungsgrundsätze zu treffen, wird *direkt und unmittelbar* aus diesen selbst abgeleitet.[1000] Es steht ausser Frage, dass diese grossen materiellen Grundsätze des Datenschutzrechts der Implementierung durch passende Massnahmen bedürfen.

708 Zudem darf angenommen werden, dass mit einem Verstoss gegen den Grundsatz der Datensicherheit oft zugleich weitere Grundsätze tangiert und verletzt werden. Meier konstatiert insofern, dass die Datensicherheit im weiteren Sinne – die ma-

996 Meier, N 781.
997 Vertiefend zweiter Teil, VI. Kapitel.
998 Rosenthal, HK-DSG, Art. 7 N 7.
999 So räumt Rosenthal, HK-DSG, Art. 7 N 7 ein, dass es sich eher um eine Frage von akademischem Interesse handelt. Eine etwas anders gelagerte, für personendatenverarbeitende Stellen indes besonders problematische Konstellation liegt vor, wenn im Rahmen eines Datensicherheitsvorfalles, beispielsweise eines Hacking-Angriffes, auf sog. sensible Personendaten zugegriffen wird, zu deren Haltung die betroffene Stelle, hätte sie die Verarbeitungsgrundsätze eingehalten, gar nicht mehr berechtigt wäre. Der Datensicherheitsvorfall und unter Umständen die Enthüllung eines Verstosses gegen die Vorgaben des Grundsatzes der Datensicherheit figurieren dann zugleich als Detektor für Verletzungen der materiellen Datenschutzgrundsätze gemäss Art. 4 DSG resp. Art. 6 nDSG.
1000 Vgl. umfassender zu den zu ergreifenden Massnahmen technischer, organisatorischer, baulicher und rechtlicher Natur zwecks Umsetzung der Datenschutz-Compliance Art. 24 DSGVO.

terielle Legitimität der Datenbearbeitung – ein Ziel des gesamten Datenschutzgesetzes sei.[1001] Dagegen verpflichte die Datensicherheit im engeren Sinne darauf, zu gewährleisten, dass keine unbefugten Personen Zugriff auf Daten und damit die Möglichkeit einer Bearbeitung haben.[1002]

709 Dass der Grundsatz der Datensicherheit i. e. S. eine eigenständige Bedeutung hat, dokumentieren die ausführenden Bestimmungen gemäss Art. 8–10 VDSG (vor Revision). Die Vorgaben an die Datensicherheit werden somit in der ausführenden Verordnung zum Datenschutzgesetz präzisiert.

710 Die Verabschiedung der Totalrevision des DSG im Parlament am 25. September 2020 bedingte auch die Anpassung der Ausführungsbestimmungen zum DSG. Die Revision der VDSG sowie VDZS (Datenschutzzertifizierung) wurden 2022 verabschiedet.[1003] Entsprechend findet sich nachfolgend eine Darstellung der Bestimmungen der VDSG nach noch nicht revidierter Fassung.

711 Art. 8 Abs. 1 VDSG umschreibt die Komponenten der Datensicherheit i. S. v. Art. 7 Abs. 1 DSG: Umzusetzen ist erstens die *Vertraulichkeit*, wonach Personendaten nur durch befugte Personen verarbeitet werden. Zweitens ist die *Verfügbarkeit* zu gewährleisten, wonach Personendaten disponibel zu sein haben, wenn sie gebraucht werden. Drittens wird die *Integrität* verlangt, nach welcher sicherzustellen ist, dass Personendaten nicht unbefugterweise verändert werden dürfen.[1004] Dem Schutz von Systemen vor den Risiken der Vernichtung, des Verlustes, technischer Fehler, Fälschungen, des Diebstahls oder widerrechtlicher Verwendung, des unbefugten Änderns, Kopierens, Zugriffs oder anderer unbefugter Bearbeitungen kommt spezifische Bedeutung zu.[1005]

712 Massnahmen zur Gewährleistung der Datensicherheit sind sowohl für technologisch unterstützte sowie digitale Systeme und Verarbeitungshandlungen (Stichworte «Cyber Security», «Cyber Defense») wie auch für manuelle Verarbeitungen zu ergreifen.[1006] Angezeigt sein können z. B. auch raumgestalterische Massnahmen (Sichtschutz) oder Weisungen, wonach bestimmte Akten «unter Verschluss» zu halten sind.

713 Ob die getroffenen Massnahmen zur Gewährleistung der Datensicherheit *angemessen* sind, bestimmt sich nach Zweck, Art und Umfang der Datenbearbeitung

1001 Meier, N 780.
1002 Vgl. Ders., N 785 ff.
1003 Vgl. <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> (zuletzt besucht am 3. Juni 2021).
1004 Vgl. zu den Umschreibungen Stamm-Pfister, BSK-DSG, Art. 7 N 7; Epiney/Civitella/Zbinden, 30 f.
1005 Vgl. Art. 7 Abs. 1 lit. a–d VDSG (vor Revision).
1006 Vgl. vertiefend allerdings zu spezifischen Bedeutungszusammenhängen von Cyber Security Hansen/Nissenbaum, Int. Stud. Q. 2009, 1155 ff.; zur Regulierung von Cyber Security sowie den Verantwortlichkeitsfragen Studer/de Werra, Expert Fokus 2017, 511 ff.

und Einschätzung potentieller Risiken für die Betroffenen sowie nach dem aktuellen Stand der Technik, Art. 8 Abs. 2 lit. a–d VDSG. Insofern werden in entsprechenden Korrelationen *vier verschiedene Schutzniveaus* unterschieden.[1007]

714 Die Vorgaben an die Datensicherheit implementieren *einen risikobasierten Ansatz*. Die Anforderungen zur Gewährleistung der Datensicherheit variieren je nach Risiken und hierbei auch Verarbeitungskonstellationen (Kategorie der Personendaten, Verarbeitungszusammenhang, Menge und Tiefe der bearbeiteten Personendaten usf.). Die Anforderungen an die Datensicherheit für den öffentlichen Bereich sind höher als für den privaten Bereich: Die Pflicht zum Erlass eines Bearbeitungsreglements geht für den privaten Sektor weniger weit als bei Bundesorganen.[1008] Allgemein anerkannt ist unter dem Grundsatz der Datensicherheit zudem, dass absolute Sicherheit nicht verlangt werden kann.[1009]

715 Obwohl die Einhaltung des Grundsatzes der Datensicherheit gemäss der expliziten Anknüpfung des Datenschutzrechts, vgl. Art. 1 DSG resp. Art. 1 nDSG, auf den Schutz der Datensubjekte abzielt, ist seine Einhaltung ebenso im *Interesse der Verarbeitenden*. Dies gilt *a fortiori*, sobald die Einhaltung des Datenschutzrechts und der Datensicherheit eine aufgewertete Bedeutung in Recht und Gesellschaft erfährt. Diese Aufwertung ist im Zuge der jüngsten datenschutzrechtlichen Neuerungswellen unübersehbar. Die Verarbeitenden sollten namentlich nicht die Folgen von medialen Reaktionen auf Datensicherheitsvorfälle und damit einhergehende Reputations- und Vertrauensverluste ausblenden.[1010] Verstösse gegen die Datensicherheit, Datenschutzpannen sowie daraus resultierende Reputationsverluste sind zudem in besonders empfindlicher Weise geeignet, einschneidende wirtschaftliche Konsequenzen für die Unternehmen nach sich zu ziehen.[1011] Es wird indes davon ausgegangen, dass zahlreiche Unternehmen die Vorgaben der Datensicherheit nicht eingehalten haben. In der Zeit vor dem Inkrafttreten der DSGVO und vor der Planung einer Totalrevision des DSG wurden indes allfällige rechtli-

1007 Meier, N 793.

1008 Vgl. Rosenthal, HK-DSG, Art. 7 N 21 f.

1009 Insofern ist die Situation vergleichbar mit den Reflexionen im Rahmen der Vorgaben zum Richtigkeitsgebot, wo ebenso wenig von einer Nullfehler-Vorgabe ausgegangen werden kann.

1010 Vertiefend zur Problematik des Vollzugsdefizites des (bisherigen) Datenschutzrechts dritter Teil, VII. Kapitel, A.

1011 Vgl. Aerotelegraph, Datenleck: Kriminelle erbeuten Passagierdaten von British Airways, Zürich 2018, <https://www.aerotelegraph.com/datenleck-bei-british-airways-kundendaten-gefaehrdet> (zuletzt besucht am 30. April 2021); Blick, Gescannte Führerausweise und Pässe waren einsehbar, Mega-Datenleck bei VW, Tesla und Co.!, Zürich 2018, <https://www.blick.ch/news/wirtschaft/automobilindustrie-bericht-datenleck-bei-autobauern-ueber-100-unternehmen-betroffen-id8640517.html> (zuletzt besucht am 30. April 2021); Blick, Datenleck beim Krankenversicherer CSS, Heikle Infos über Kundin landeten bei Fremdem, <https://www.blick.ch/news/wirtschaft/datenleck-beim-krankenversicherer-css-heikle-infos-ueber-kundin-landeten-bei-fremdem-id8549037.html> (zuletzt besucht am 30. April 2021); zum medialen Rauschen als Hauptwirkung des Datenschutzes Vesting, in Ladeur (Hrsg.), 155 ff., 182; Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f., 23.

che Konsequenzen bei einer Verletzung der Datensicherheitsvorgaben noch als bedeutungslos beurteilt.[1012]

716 Mittlerweile wurden im Anwendungsbereich der DSGVO entsprechende Sicherheitsvorfälle bereits mit einschneidenden Bussen belegt.[1013] Mit den aktuellen datenschutzrechtlichen Neuerungen gewinnt das Datenschutzrecht selbst deutlich an Wirkungskraft. Damit einhergehend haben die Vorgaben für die Datensicherheit *merkliche Stärkung* erfahren.[1014]

717 Die DSGVO verlangt unter dem Titel der Datensicherheit gemäss Art. 5 Abs. 1 lit. f. DSGVO, dass Personendaten nur in einer Weise verarbeitet werden dürfen, die eine angemessene Sicherheit gewährleistet, was mit den Begriffen «Integrität» und «Vertraulichkeit» bezeichnet wird.[1015] Entsprechend ergriffene Massnahmen haben auf sämtlichen Verarbeitungsstufen und während des *gesamten Lebenszyklus von Personendaten* und deren Verarbeitungen zu greifen. Sie zielen darauf ab, das Risiko ungewollter Datenverluste, Transfers, Zerstörungen oder Beschädigungen sowie, allgemeiner, unrechtmässiger Datenverarbeitungen zu reduzieren. Der Verarbeitungsgrundsatz wird insb. über Art. 32 ff. DSGVO, aber auch Art. 24 f. DSGVO konkretisiert.[1016] Mit Blick auf diese Bestimmungen bestehen teilweise Abgrenzungsschwierigkeiten.

718 Art. 32 DSGVO, der den Abschnitt 2 mit dem Titel «Sicherheit personenbezogener Daten» einleitet, steht seinerseits unter dem Titel der «Sicherheit der Verarbeitung». Sowohl von einem Verantwortlichen wie vom Auftragsverarbeiter wird verlangt, geeignete technische und organisatorische Massnahmen (TOM) zur Gewährleistung eines angemessenen Schutzes vor der Verletzung von Rechten und Freiheiten der Datensubjekte zu ergreifen.[1017] Art. 32 DSGVO befasst sich folglich auch, aber nicht nur mit dem technischen Datenschutz, indem er die Gewährleistung der «Daten- und Systemsicherheit» verlangt («Sicherheitsmassnahmen»).[1018] Im Kontext des Schutzes der Integrität von informationstechnischen Systemen sei spezifisch auch auf das Urteil des Bundesverfassungsgerichts verwie-

1012 Rosenthal, HK-DSG, Art. 7 N 21.
1013 Zum Bussgeld, das gegenüber British Airways im Jahr 2020 verhängt wurde, vgl. <https://www.bbc.com/news/technology-54568784> (zuletzt besucht am 3. Juni 2021).
1014 So auch Reimer, NomosKomm-DSGVO, Art. 5 N 45.
1015 Ders., a. a. O., Art. 5 N 45 ff.; Meier, N 786 ff.; Stamm-Pfister, BK-DSG, Art. 7 N 7 und N 24 ff.; vgl. zum Grundsatz auch Art. 8 nDSG.
1016 Vgl. auch Herbst, BeckKomm-DSGVO, Art. 5 N 76.
1017 Bei den sog. TOM handelt es sich um Massnahmen, die sowohl von einem Verantwortlichen als auch einem Auftragsverarbeiter zu ergreifen sind. Neben solchen «gemeinsamen» Vorgaben gibt es sodann solche, die nur vom Verantwortlichen zu beachten sind, und solche, die lediglich den Auftragsverarbeiter treffen. Eine entsprechende Rollendifferenzierung und daraus resultierende teilweise Differenzierungen der Vorgaben der DSGO sind Kernelemente des Regelungsregimes der DSGVO; zu den Rollen des Verantwortlichen und des Auftragsverarbeiters vgl. Art. 4 Nr. 7 resp. Nr. 8 DSGVO und Art. 26 DSGVO.
1018 Jandt, BeckKomm-DSGVO, Art. 32 N 1.

sen, das 2008 mit dem sog. Computer-Grundrecht eine spezielle Ausprägung des allgemeinen Persönlichkeitsrechts anerkannte.[1019]

719 Damit Massnahmen i. S. v. Art. 32 DSGVO als geeignet qualifiziert werden können, sind neben dem Stand der Technik die Eintrittswahrscheinlichkeit eines Vorfalles sowie die (materiellen und immateriellen) Folgen und die Schwere der Risiken zu ermitteln, wobei Art, Breite und Tiefe der Personendaten(bestände) ebenso einschlägig sind. Die zu treffenden technischen und organisatorischen Massnahmen zur «Datensicherheit» orientieren sich, wie erwähnt, an einem risikobasierten Ansatz, wobei insofern die sog. Datenschutz-Folgenabschätzung gemäss Art. 35 DSGVO vor Augen zu halten ist. Im Rahmen der Evaluation der Eignung der zu ergreifenden Sicherheitsmassnahmen können die Implementierungskosten in die Analyse miteinbezogen werden.

720 Hinsichtlich der angemessenen Massnahmen zur Datensicherheit ist weiter Art. 24 DSGVO in Betracht zu ziehen, wobei die Abgrenzung gegenüber Art. 25 DSGVO sowie Art. 32 DSGVO nicht gänzlich geklärt ist. Art. 24 DSGVO wird als Generalauftrag zur Gewährleistung der Datenschutz-Compliance sowie der Datensicherheit beschrieben.[1020] Die Bestimmung verpflichtet Verantwortliche und Auftragsverarbeitende, alle sachlich notwendigen Vorkehrungen zur Gewährleistung der Datenschutz-Compliance und -Sicherheit zu ergreifen.[1021] Mit «Datenschutzvorkehrungen» sind Compliance- und Sicherheitsmassnahmen gemeint, die erforderlich und verhältnismässig sind, um die Einhaltung der DSGVO zu gewährleisten. Dazu gehören betriebliche Massnahmen technischer, baulicher, rechtlicher und organisatorischer Natur.[1022] In Bezug auf die Gewährleistung der Datensicherheit sowie auf das Vorgehen bei Datensicherheitsvorfällen kommt der angemessenen Schulung und Instruktion der Mitarbeitenden Bedeutung zu.

721 Für die Implementierung angemessener Massnahmen der Datensicherheit ist, um das Bild zu vervollständigen, auf weitere *Umsetzungsinstrumente* hinzuweisen. Sie finden sich in der DSGVO. Die Totalrevision des DSG sieht vergleichbare Instrumente und Normen vor. Sie sollen nachfolgend in Kürze umrissen werden:

722 Der Erfüllung der Sicherheitsvorgaben dient zunächst das sog. *Verarbeitungsverzeichnis* als Basisinstrument, vgl. Art. 30 DSGVO und Art. 12 nDSG. Es bildet die Landschaft der Verarbeitungsprozesse, die Kategorie von Personendaten so-

1019 BVerfGE, Az. 1 BvR 270/07 – Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Urteil vom 27. Februar 2008; zu diesem sog. Computer-Grundrecht namentlich Karavas, Neue Zeitschrift für Sozialforschung 2010, 95 ff.; Gusy, DuD 2009, 33 ff.; Böckenförde, JZ 2008, 925 ff., 927 ff.; Drallé, 5 ff.

1020 Raschauer, NomosKomm-DSGVO, Art. 24 N 1.

1021 Ders., a. a. O., Art. 24 N 1 ff.

1022 Ders., a. a. O., Art. 24 N 10 f.

wie die Personendatenflüsse ab, womit sich die zu ergreifenden angemessenen Sicherheitsmassnahmen klarer bestimmen lassen.

723 Weiter leistet die erwähnte *Datenschutz-Folgenabschätzung* einen Beitrag zur «Sicherung der Datensicherheit», Art. 35 DSGVO und Art. 22 nDSG. Sie ist bei besonders «riskanten» Verarbeitungen vorzunehmen, wobei sich hieraus Rückschlüsse auf die zu treffenden angemessenen (Sicherheits-)Massnahmen ergeben.[1023] Das Instrument verlangt im Vorfeld die Evaluierung von Risiken sowie von angemessenen Mitigationsmassnahmen.

724 Zudem sind im Zusammenhang mit der Datensicherheit im Sinne eines «Vorfeldschutzes» die Bestimmungen und Vorgaben einschlägig, die unter dem Terminus des «*privacy by design*» (Gewährleistung von Datenschutz durch Technikgestaltung) resp. «*privacy by default*» (Gewährleistung von Datenschutz durch datenschutzfreundliche Voreinstellungen) figurieren, vgl. Art. 25 DSGVO und Art. 7 nDSG. Im Rahmen von «privacy by design» sind Aspekte des Datenschutzes und der Datensicherheit bereits im Zuge der Prozessentwicklung zu integrieren.

725 Die Datensicherheit wird sodann neuerdings über die *Meldepflichten* im Zusammenhang mit sog. *Datensicherheitsvorfällen* adressiert, Art. 33 f. DSGVO, sog. Data Breach Notification. Die Totalrevision sieht neu explizit entsprechende Pflichten vor, vgl. Art. 24 nDSG. Ein Datensicherheitsvorfall liegt bei einer Verletzung der Sicherheit von Personendaten vor. Angenommen wird eine solche für den Fall, in welchem ein Defizit bezüglich der Datensicherheit infolge ungenügender technischer oder organisatorischer Massnahmen zu einer objektiv unbeabsichtigten, unrechtmässigen oder unbefugten Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit von Personendaten führt.[1024] Nach DSGVO gilt eine Notifikationspflicht gegenüber den Aufsichtsbehörden mit einer Meldefrist von 72 Stunden, wobei die Etablierung entsprechender Prozesse die verarbeitenden Stellen in der Praxis vor Herausforderungen stellt. Zudem greift eine Meldepflicht gegenüber den Betroffenen für den Fall, dass die Verletzung der Datensicherheit ein hohes Risiko für diese darstellt.[1025]

726 Der Verantwortliche und ggf. der Auftragsverarbeiter sind gemäss Art. 33 Abs. 5 DSGVO verpflichtet, nicht nur die getroffenen Massnahmen zur Datensicherheit und eine Risikoeinschätzung, sondern auch Verletzungen mit sämtlichen einschlägigen Informationen zu *dokumentieren*.[1026] Auch gemäss Art. 24 Abs. 1 und

1023 Hierzu WP 248 (Entwurf); ISO 2913:2017; beachte sodann die Liste der Datenschutzstelle des Fürstentum Liechtensteins, abrufbar unter: <https://www.datenschutzstelle.li/application/files/6715/5127/0000/Liste_der_Verarbeitungstaetigkeiten.pdf> (zuletzt besucht am 30. April 2021).

1024 Vgl. auch Art. 4 Nr. 12 DSGVO zum sog. Eintritt einer Verletzung des Schutzes personenbezogener Daten Jandt, BeckKomm-DSGVO, Art. 32 N 7.

1025 Vgl. WP 29/248, Data Breach Notification, WP250rev.01, 20 ff., 30 ff.

1026 Vgl. DSGVO ErwG 85.

Art. 5 Abs. 2 DSGVO müssen die Verantwortlichen in der Lage sein, jederzeit Rechenschaft über die risikobasiert evaluierten und angemessenen Massnahmen ablegen zu können.[1027] Die Totalrevision des DSG sieht keine entsprechende explizite Dokumentationsvorgabe vor. Sie wird allerdings in der Praxis bereits heute als Element der datenschutzrechtlichen Governance beurteilt und umgesetzt.

727 Anhand der gerade im Zusammenhang mit der Datensicherheit beschriebenen Instrumente zeigen sich *zwei Aspekte*, die mit den datenschutzrechtlichen Neuerungen Akzentuierung finden: Erstens sollen die Verarbeitungsgrundsätze durch einen Katalog neuer Instrumente auch faktisch effizient umgesetzt werden. Zweitens wird anhand dieser Instrumente die zeitliche und prozesshafte Dimension des neueren Datenschutzrechts sichtbar. Die entsprechenden Massnahmen sichern die Vorgaben an die Datensicherheit über sämtliche Etappen der Verarbeitungszyklen ab.

728 Der Ausbau von Vorgaben an Massnahmen zwecks Einhaltung der Datensicherheit und hierbei insb. des technischen Datenschutzes reflektiert gewissermassen ein Prinzip des *vices rependere* (Gleiches mit Gleichem vergelten) und ebenso des *Verursacherprinzips* (polluter pays principle, namentlich für das Umweltrecht bekannt).[1028] Markiert wird damit ein Trend, das Augenmerk auf die faktische Verwirklichung und die Umsetzung des Rechts in der Realität zu lenken.[1029] Mit dem Trend, technische, aber auch organisatorische sowie prozedurale Massnahmen vorzusehen, um dem Datenschutzrecht mit dem Aspekt der Datensicherheit in der Realität Griffigkeit zu verleihen, steht das Datenschutzrecht nicht isoliert da – ebenso wenig mit der Korrelierung, die Zuständigkeit hierfür in erster Linie in die Hände des Verursachers resp. des «Geschäftsherren» («Verantwortlichen») zu legen.

729 Beschrieben wird diese Entwicklung, die durch diverse Prozesse konstituiert wird, auch als Integration des Datenschutzes und der Datensicherheit in die DNA der verarbeitenden Organisationen.[1030] Teilelemente sind insofern die Durchführung der Datenschutz-Folgenabschätzung, die Erstellung des Inventars, aber auch die Etablierung der Prozesse zwecks Erfüllung der Meldepflichten bei Datensicherheitsvorfällen.

1027 Sog. Accountability-Ansatz.

1028 Zum Verursacherbegriff im Umweltrecht Caluori, URP 2011, 541 ff.; zum Verursacherprinzip in diesem Kontext auch Rööseli, URP 2021, 117 ff., unter Darstellung des Instruments der Gesundheitsgefährdungsabschätzung, die als Parallele zur Risikofolgenabschätzung der neuen Datenschutzerlasse gesehen werden kann; zu Umwelt, Sicherheit sowie Information und damit zur Herausbildung eines Umwelt-, Sicherheits- und Informationsstaates Hassemer, in: Simon/Weiss (Hrsg.), 121 ff., 122 ff.

1029 Eine entsprechende Entwicklung lässt sich zudem für den Kontext des Familienrechts nachweisen.

1030 Vgl. hierzu Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f., 23.

730 Anhand der erwähnten Instrumente lässt sich unter dem Aspekt der Datensicherheit eindrücklich nachzeichnen, inwiefern der Datenschutz und das Datenschutzrecht im Begriff sind, einen *Systemwechsel zu vollziehen*: Die Existenz und Relevanz des Datenschutzrechts soll sich nicht erst im Falle einer «widerrechtlichen Persönlichkeitsverletzung» und einer resultierenden Klage manifestieren und aktualisieren. Mit den datenschutzrechtlichen Neuerungen findet eine Ergänzung und punktuell eine Abkehr von einer individualrechtlichen und defensivrechtlichen Anknüpfung des Datenschutzrechts statt. Neu wird die Einhaltung des Datenschutzrechts und damit auch der Datensicherheit zur *Governance- und Compliance-Aufgabe*, für die an erster Stelle die «Verantwortlichen» in die Pflicht genommen werden. Die entsprechenden Pflichten lassen sich nicht in einem einmaligen Akt erfüllen. Vielmehr bedarf es eines kontinuierlichen, risikobasierten Managements der diversen Prozesse, welche die Vorgaben des Datenschutzrechts und damit auch der Datensicherheit gewährleisten sollen. Gerade anhand des Grundsatzes der Datensicherheit wird hierbei der risikobasierte Ansatz der datenschutzrechtlichen Neuerungen deutlich.

731 Im Ergebnis wird damit der Datenschutz zu einem Element des Risikomanagements.[1031] Wenn die ergriffenen Massnahmen und deren Angemessenheit zur Gewährleistung der Datensicherheit gemäss dem Accountability-Ansatz zu dokumentieren sind und der Verarbeitende insofern in der Rechenschaftspflicht steht, wird ein weiterer Kontrapunkt gegenüber einem bisher persönlichkeitsrechtlich und damit deliktsrechtlich gedachten Datenschutzrecht gesetzt, der die primäre «Eigenverantwortung» der Verarbeitenden anerkennt.

732 Damit sind die Erkenntnisse *zu den generalklauselartigen Verarbeitungsgrundsätzen* als zweites Strukturmerkmal des DSG zu resümieren.

C. Ergebnisse

733 Die vorangehenden Ausführungen haben sich mit den gemeinsam für den öffentlichen und den privaten Bereich statuierten «allgemeinen» und über weite Strecken generalklauselartig formulierten Verarbeitungsgrundsätzen befasst, wie sie das eidgenössische Datenschutzgesetz in seiner noch in Kraft stehenden Fassung

1031 Zur Forderung eines Perspektivenwechsels im Datenschutzrecht weg vom «Schadensrecht» hin zum Risikorecht: Ladeur, Vortrag, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021); zur Bedeutung der Kategorien «Risiko» (und «Vertrauen») für das heutige Zusammenleben im Zusammenspiel mit dem Privaten als Schutzkonzept Hotter, 74 ff.; auf die Relevanz von risiko- und zweckbezogenen Erwägungen für eine ausdifferenzierte Gestaltung des Datenschutzrechts weist auch Rossnagel, digma 2011, 160 ff., 163 f. hin; zum Datenschutz als Risikorecht auch Donos, 179 ff.

in Art. 4 ff. DSG niederlegt.[1032] Nach der Totalrevision finden sich die allgemeinen Verarbeitungsgrundsätze in Art. 6 nDSG, der den Grundsatz der Datenrichtigkeit neu inkludiert. Die Vorgaben an die Datensicherheit normiert Art. 8 nDSG, wobei die ausführende Verordnung zum DSG in einer angepassten Fassung zu beachten ist.

734 Unter Reflexion der Lehre und Praxis wurde den grundsatzbasierten Verarbeitungsvorgaben Kontur verliehen, wobei ihre Inhalte und Funktionen konkretisiert wurden. Zur Erreichung des Ziels, die datenschutzgesetzlich generalklauselartigen oder offenen Bearbeitungsgrundsätze griffiger zu beschreiben, wurden zudem Erkenntnisse aus der allgemeinen Methodenlehre zu den unbestimmten Rechtsbegriffen sowie den Generalklauseln angewendet. Herausdestilliert wurden Kerninhalte, Akzente und Entwicklungslinien zu den einzelnen allgemeinen, weitgehend generalklauselartigen und damit abstrakten Verarbeitungsgrundsätzen.

735 Es wurden zugleich die Neuerungen berücksichtigt, wie sie mit der DSGVO, aber auch der Totalrevision des DSG vorgesehen werden. An den grossen und traditionsreichen materiellrechtlichen Verarbeitungsgrundsätzen wird weitgehend festgehalten. Für die Totalrevision des DSG stellt insb. der Ausbau der Transparenzvorgaben ein Kernelement dar, das sich seinerseits ebenso auf die Verarbeitungsgrundsätze bezieht. Eine wesentliche Neuerung im Zusammenhang mit den Verarbeitungsgrundsätzen bilden sodann die neuen Umsetzungsinstrumente. Weiter wurden die Stärkung der Eigenverantwortung, der risikobasierte Ansatz sowie der Accountability-Ansatz vorgestellt.

736 Zu den einzelnen allgemeinen generalklauselartigen Grundsätzen, die trotz dieser Trends als *zweites Strukturmerkmal* des noch geltenden, aber auch künftigen DSG benannt wurden, sind die folgenden Kernbefunde festzuhalten:

737 Das *Rechtmässigkeitsprinzip* wurde als *Koppelungsinstrument* qualifiziert. Als Metapher figurierte das «Drehkreuz», wobei über den Grundsatz – in verschiedene Richtungen gestellt – die *Gesamtlandschaft* datenschutzrechtlicher Vorgaben in Gestalt eines «Netzes» sichtbar wird. Vorab präsentiert es sich als Brücke für die *ausserhalb* des Datenschutzgesetzes befindlichen datenschutzrechtlichen Vorgaben. Von besonderer Bedeutung sind hierbei zahlreiche spezifische Informationsnormen, wie sie in Spezialgesetzen, weiter im OR oder im ZGB zu finden sind. Sie formulieren bereichs-, sektor- oder kontextspezifische datenschutzrechtliche Vorgaben.[1033] Die Koppelungsfunktion des Rechtmässigkeitsprinzips des DSG zeigt sich indes *nicht nur nach aussen*, sondern auch *nach innen unter Be-*

1032 Vgl. Art. 6 nDSG.
1033 Grundlegend zu Art. 328b OR und DSG sowie zum Datenaustausch zwischen Arbeitgeber und Versicherung, Pärli, insb. 123 ff.

zugnahme auf das duale Regime des DSG. Über das Rechtmässigkeitsprinzip erfolgt die Anknüpfung des gewählten *Ausgangspunktes*. Rechtmässigkeit bedeutet gemäss DSG mit Blick auf den Ausgangspunkt der Datenverarbeitung – Grundsatz des Verarbeitungsverbotes mit Erlaubnisvorbehalt für den öffentlichen Bereich resp. Grundsatz der Verarbeitungsfreiheit mit Schranken für den privaten Bereich – nicht dasselbe.[1034] Unrechtmässig sind im privaten Bereich, unter Anlehnung der Datenschutzgesetzgebung an Art. 28 ZGB, nur qualifizierte Personendatenverarbeitungen.[1035] Hierbei gelten namentlich Verstösse gegen die allgemeinen Verarbeitungsgrundsätze als Schranken der grundsätzlich freien Datenverarbeitung; ihre Verletzung begründet die unrechtmässige Personendatenverarbeitung und damit die Persönlichkeitsverletzung. Das Vorliegen von Rechtfertigungsgründen ist in einem zweiten Schritt zu prüfen. Anders dagegen bedarf die rechtmässige Personendatenverarbeitung im öffentlichen Recht prinzipiell eines Erlaubnistatbestandes basierend auf einer rechtlichen Grundlage. Das *Rechtmässigkeitsprinzip* im schweizerischen Datenschutzrecht ist folglich *kein einheitliches Prinzip*. Vielmehr inkorporiert es ein differenziertes Regime für die verschiedenen Bereiche, namentlich auch des traditionsreichen «Zweikammersystems» mit dem öffentlichen Bereich gegenüber dem privaten Bereich. Mit einer solchen Strukturierung implementiert man in der Schweiz über das Rechtmässigkeitsprinzip ein *nuanciertes und abgestuftes Datenschutzregime, das sich harmonisch in die gesamte Rechtsordnung mit ihren für die jeweiligen Bereiche etablierten Leitprinzipien einfügt*. Im DSG wird damit, obschon dieses als Querschnittsgesetz oftmals gewissermassen als Synonym für das Datenschutzrecht gelesen wird, in markanter Weise auch über das Rechtmässigkeitsprinzip die datenschutzrechtliche Einschlägigkeit *bereichsspezifischer Ausdifferenzierung* sichtbar. Dagegen geht die DSGVO zumindest dergestalt zu einem «bereichsindifferenten Modell» über, als dass diese dem Grundsatz nach identische Vorgaben für die rechtmässige Verarbeitung von Personendaten durch öffentliche Stellen wie Private formuliert. Anknüpfend an das Rechtmässigkeitsprinzip sowie die im zweiten Teil, IV. Kapitel herausgearbeitete *duale Struktur des DSG* sah man sich folglich wiederholt mit der Herausforderung konfrontiert, die «gemeinsamen, allgemeinen Verarbeitungsgrundsätze», die dem Datenschutzrecht für den öffentlichen und den privaten Bereich als «gemeinsamer Nenner» vorangestellt sind, sinnvoll mit den «beiden Bereichen» zu korrelieren und harmonisieren.

738 Zum Verarbeitungsgrundsatz von *Treu und Glauben* wurde vorab statuiert, dass im Rahmen des noch in Kraft stehenden DSG die Transparenzvorgaben für den öffentlichen und privaten Bereich differieren. Als Kernbefund für Treu und Glauben im Datenschutzrecht wurde seine richtungsweisende und akzentu-

1034 Vertiefend zum Dualismus als erstes Strukturmerkmal zweiter Teil, IV. Kapitel.
1035 Vertiefend hierzu zweiter Teil, VI. Kapitel.

ierte Bedeutung in Bezug auf das *Thema der Transparenz* herausdestilliert. Vom Grundsatz geht, so wurde es nachgewiesen, eine *dezidierte Anstosswirkung in Bezug auf den Ausbau von Transparenzvorgaben* aus. Weit weniger produktiv entfaltet sich Treu und Glauben in seinem Charakter als Verarbeitungsgrundsatz in seiner Funktion als Handlungsanweisung gegenüber den Verantwortlichen und damit in der Praxis. Vielmehr liegt seine Hauptleistung in den Impulsen, die er für die Datenschutzgesetzgebung geliefert hat, womit er als *Quellrecht* für den Ausbau und die Erhöhung der Transparenzvorgaben im Datenschutzrecht zu bezeichnen ist. Hervorgegangen ist ein Fächer mit diversen Instrumenten und variablen Stossrichtungen: Neben den aktiven Informationspflichten gegenüber den Datensubjekten und den Einwilligungsvorgaben schaffen neue oder ausgebaute Meldepflichten, Auskunftsrechte, Dokumentations- und Rechenschaftspflichten, die Pflicht zur Erstellung des Verarbeitungsverzeichnisses, aber auch Zertifizierungsverfahren erhöhte Transparenz in Bezug auf Prozesse der Personendatenverarbeitung sowie ihrer Übereinstimmung mit den datenschutzrechtlichen Vorgaben. Die umfassenden Rechenschafts- und Dokumentationspflichten bezüglich der zur Einhaltung des Datenschutzes implementierten Massnahmen bilden ein zentrales Instrument, um Verarbeitungsprozesse transparent und damit auch auf ihre Rechtskonformität hin überprüfbar zu machen. Freigelegt wurde somit ein *Trend*, über Treu und Glauben im Rahmen des Datenschutzes *Transparenzerfordernisse sowie Dokumentations- und Rechenschaftspflichten* in diversen Facetten auszubauen sowie die Verantwortlichkeiten für die Einhaltung der Datenschutzvorgaben nachhaltig und früher in den Zuständigkeitsbereich der Verarbeitenden zu legen. Mit diesen massgeblich über Treu und Glauben vollzogenen Entwicklungen wird die Bedeutung der *Kategorie des Vertrauens* im und für das Datenschutzrecht adressiert, was auch der Tatsache geschuldet ist, dass die Bewältigung informationeller Herausforderungen nicht in identischer Weise geleistet werden kann, wie sie beispielsweise im Umgang mit Sachgütern möglich ist. Damit verbunden ist eine Veränderung der Perspektive dergestalt, dass der *integre Umgang mit Personendaten* vorgeschaltet und nachdrücklich in den Verantwortungsbereich der Verarbeitenden gestellt wird, womit sich eine Ergänzung resp. Überwindung der defensiv- und deliktsrechtlichen Konzeption manifestiert, wie sie in der persönlichkeitsrechtlichen Anknüpfung des Datenschutzrechts angelegt ist. Nebst dem Aspekt der Transparenz wurde unter dem Grundsatz von Treu und Glauben im Datenschutzrecht zudem auf die Figur der «vernünftigen Erwartungen» resp. die US-amerikanische Doktrin der *«reasonable expectations of privacy»* eingegangen, die ansatzweise in Europa Rezeption findet, namentlich in der Rechtsprechung des EGMR.[1036] Hier wurde dargelegt, inwiefern der Ansatz der *«reasonable expectations of privacy»* – nicht individualisiert, sondern

1036 Hierzu dritter Teil, IX. Kapitel; Paefgen, 33 ff.

kontextualisiert verstanden – Impulse geben kann, um tradierte Konzepte des geltenden Datenschutzrechts fortzuentwickeln.

739 Bezüglich des *Verhältnismässigkeitsgrundsatzes* wurde festgestellt, dass dieser – trotz des Grundsatzentscheides des DSG für ein duales System – im privaten wie im öffentlichen Bereich in seinem «öffentlich-rechtlichen» Gehalt der Trias von Eignung, Erforderlichkeit und Verhältnismässigkeit i. e. S. Anerkennung findet. Für beide Bereiche müssen Personendatenverarbeitungen geeignet sowie erforderlich zur Erreichung des Zweckes sowie verhältnismässig im engeren Sinne sein. Das ist zugleich bemerkenswert wie reflexionswürdig. Indem das Verhältnismässigkeitsprinzip als Mittel-Zweck-Relation mit *seinem «engen» öffentlich-rechtlichen Inhalt Gültigkeit auch für den privaten Bereich* beansprucht, wird *ebenso für den privaten Bereich* eine *Machtasymmetrie* in der Beziehung von Datenverarbeitenden und Betroffenen anerkannt. Gleichwohl wird die datenschutzrechtliche Beziehung zwischen Privaten und die hier anerkannte Machtasymmetrie *nicht identisch* gedacht im Vergleich zu derjenigen im öffentlichen Bereich. Die Anerkennung der Differenzierung kommt im Dualismus des DSG aufgrund des entgegengesetzten Ausgangspunktes zum Ausdruck, wobei ein aus dem öffentlichen Bereich in den privaten Bereich importiertes Verhältnismässigkeitsgebot in seiner Trias eine gewisse Angleichung bringt. Anders der Ansatz in einem monistischen System, wie es die DSGVO implementiert, wo eine identische Behandlung stattfindet resp. die Differenzierungswürdigkeit zwischen Personendatenverarbeitungen durch öffentliche und private Stellen verworfen wird. Ein Verhältnismässigkeitsprinzip, das die Eignung, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne ebenso für den privaten Bereich verlangt, setzt einer prinzipiellen Verarbeitungsfreiheit, wie sie im DSG für den privaten Bereich verankert wird, *eine enge, griffige und markante Schranke*. Entsprechend kommt dem Verhältnismässigkeitsprinzip eine entscheidende Rolle zu, Personendatenverarbeitungen im privaten Bereich zu limitieren und damit eine gewisse Annäherung an das datenschutzrechtliche Schutzniveau zwischen der Normierung im privaten und derjenigen im öffentlichen Bereich zu erreichen. Darüber hinausgehend wurde dargelegt, inwiefern der Verhältnismässigkeitsgrundsatz und namentlich seine faktische Einhaltung im Rahmen der jüngsten Revisionswellen durch verschiedene konkretisierte Instrumente und Vorgaben abgesichert wird. In diesem Zusammenhang sind erneut namentlich das Verarbeitungsverzeichnis, aber auch Löschungs- und Anonymisierungsvorgaben zu nennen. Das Verhältnismässigkeitsprinzip steht, obschon bis heute im DSG gemeinsam mit Treu und Glauben verankert, seinerseits in untrennbarem Zusammenhang mit dem *Verarbeitungszweck*.

740 In Bezug auf den *Verarbeitungszweck* wurden mehrere konkrete Vorgaben resp. Teilgehalte differenziert durchleuchtet. Dazu gehören insb. die vorgängige

Zweckfixierung und -definierung, die Zwecktransparenzvorgaben sowie die Zweckbindung im engeren Sinne. Im Rahmen der Ausführungen zu den Zweckgrundsätzen durfte sodann eine datenschutzrechtliche Kernfrage nicht unbeachtet bleiben: diejenige nach dem Zweck des Datenschutzrechts. Sie wurde vertieft analysiert, obschon Art. 1 DSG resp. Art. 1 nDSG eine klare Antwort hierauf zu geben scheinen. Anlass dafür, den gesetzlichen Schutzzweck resp. das Schutzobjekt zu hinterfragen, gab nicht nur die Tatsache, dass um die Erfassung des Schirmbegriffs der «Privatheit», der seinerseits als Schutzzweck des Datenschutzrechts gilt, bis heute intensiv gerungen wird. Im Zentrum stand eine Auseinandersetzung mit der Argumentation des Bundesverfassungsgerichts im Volkszählungsurteil zum Zweckbindungsgrundsatz. Im Zuge einer Analyse des Volkszählungsurteils des Bundesverfassungsgerichts, das mit seinem Recht auf informationelle Selbstbestimmung Rechtsgeschichte schrieb, wurde anhand eines bislang wenig rezipierten Aspekts des Urteils die *systemische sowie dynamische Dimension* des Datenschutzes sowie des Datenschutzrechts herausgeschält. Dieser Aspekt findet sich in den Ausführungen zu den Zweckgrundsätzen. Dreh- und Angelpunkt auch der verfassungsgerichtlichen Erwägungen war die *Anerkennung der Einschlägigkeit pluraler Verarbeitungszusammenhänge und Verarbeitungszwecke sowie die Erforderlichkeit, diese voneinander abzuschotten*: Die im Rahmen einer Volkszählung erhobenen Personendaten dürfen – trotz der Besonderheiten einer solchen Datenerhebung zur Erfüllung staatlicher Aufgaben – nicht beliebig für weitere Ziele und Zwecke der vielgestaltigen weiteren Aufgaben des Verwaltungsvollzuges (beispielsweise im Kontext der Steuererhebung, der Strafverfolgung oder Migration) genutzt werden. Der *öffentliche Bereich* wurde vom Bundesverfassungsgericht nicht als einheitlicher und gewissermassen monolithischer, sondern stattdessen als *facettenreicher, diversifizierter und pluralistischer Bereich* mit unzähligen Organisationseinheiten, Zielen und Verarbeitungszusammenhängen präsentiert – was ebenso datenschutzrechtlich als bedeutsam herausgestellt wird. Ausgangspunkt der *systemischen Dimension* des Datenschutzrechts ist damit vorab die Anerkennung *pluraler Verarbeitungszusammenhänge*, wobei der Zweckbindungsgrundsatz insofern einschlägig wird, als er Personendatenverarbeitungen an einen im Vorfeld definierten Verarbeitungszweck ankoppelt und damit ihre «unbeschränkte Diversifizierung» verhindert. Geschützt wird damit namentlich das Datensubjekt und dessen «Recht auf informationelle Selbstbestimmung», was die individualrechtliche Position abbildet. Diese Schutzdimension allerdings steht nicht isoliert da. Vielmehr dienen die fraglichen Vorgaben darüber hinausgehend zugleich dazu, die *Funktionstüchtigkeit und Integrität verschiedener Bereiche mit ihren Zielen, Instrumenten und Verarbeitungszusammenhängen zu gewährleisten*. Spezifisch für das Instrument der statistischen Erfassung der Bürgerinnen und Bürger hält das Bundesverfassungsgericht fest, dass lediglich das *Statistikgeheimnis die Integrität der statistischen Erhebung* und die hierzu

notwendige Kooperationsbereitschaft sowie das Vertrauen der Bürgerinnen und Bürger garantieren könne. Zwangsmassnahmen vonseiten des Staates dagegen können ebendies gerade *nicht* leisten.[1037] Nur wenn die aussagende Person darauf vertrauen kann,[1038] dass die erteilten Personenangaben nicht zu anderen Massnahmen des Verwaltungsvollzuges «gegen sie» verwertet werden, wird sie vollständig und korrekt die in der Volkszählung gestellten Fragen beantworten. Datenschutzrechtliche Vorgaben schützen folglich – so ein Kernergebnis des Urteils, seiner Analyse und dieses Teils – neben dem *Datensubjekt namentlich die Integrität und damit das Funktionieren verschiedener Subsysteme*. Das Volkszählungsurteil öffnet indes nicht nur das Fenster für einen Blick auf die *systemische Dimension* des Datenschutzrechts, sondern gleichermassen für seine *dynamische Dimension*. Es geht um den Schutz «angemessener Datenflüsse», wobei der Zweckbindungsgrundsatz das Instrument ist, einmal zu einem bestimmten Zweck erhobene Personendaten in ebendiesem Flussbett innerhalb eines bestimmten Bereiches, in einem spezifizierten Verarbeitungszusammenhang zu fixieren und den beliebigen, unbeschränkten und freien Übertritt in andere (Bereiche, Felder,) Flussbette zu verhindern. Anhand des Zweckbindungsgrundsatzes wurde dargelegt, dass sich der *Zweck des Datenschutzes und des Datenschutzrechts* nicht auf den Schutz des Datensubjektes, den Persönlichkeitsschutz oder ein Recht auf informationelle Selbstbestimmung beschränkt. Vielmehr zeigen sich neben der – bis anhin oft ausschliesslich betonten – subjektiven Dimension die systemische wie die dynamische Dimension des Datenschutzrechts. Kein Vorfall könnte diese bislang vernachlässigten Aspekte des Datenschutzrechts deutlicher vor Augen führen und bestätigen als der jüngste Facebook-Skandal. Er dokumentiert die disruptiven Wirkungen von Datenflüssen und Verarbeitungsprozessen auf die Kontextintegrität: Aus dem Kontext persönlicher, freundschaftlicher und familiärer Kommunikationsbeziehungen wurden mutmasslich Personendaten abgeleitet, um in der Folge gezielt auf das Wahlverhalten einzuwirken. Im Ergebnis werden damit das *demokratische System*, aber auch der Bereich persönlicher Lebensführung erodiert. Die Problematik des Vorfalles erschöpft sich nicht in der Manipulation eines einzelnen Subjektes; vielmehr werden die Integrität des persönlichen Lebensbereiches wie des politischen Systems untergraben. Vor diesem Hintergrund hat das Volkszählungsurteil aus dem Jahr 1985 nicht bloss Rechtsgeschichte hinsichtlich einem Recht auf informationelle Selbstbestimmung geschrieben. Dem Entscheid lassen sich mit diesen Erkenntnissen weit über 2020

1037 Insofern tritt erneut die auch unter Treu und Glauben sichtbar gewordene «Spezifität» von Informationen und dem rechtlichen Umgang mit diesen zu Tage sowie die Relevanz von Vertrauen im Zusammenhang mit Informations- und Kommunikationsprozessen; vgl. zur Bedeutung von Vertrauen im Zusammenhang mit der Privatsphäre Hotter, 75 f. unter Referenz auf Luhmann.

1038 Zur Bedeutung des Vertrauens und damit auch von Treu und Glauben vorangehend zweiter Teil, V. Kapitel, B.2.

hinausgehende Richtungshinweise für die Entwicklung eines Datenschutzrechts, das seinen Schutzaufgaben gerecht zu werden vermag, gewinnen.

741 Den Abschluss dieses Kapitels zum zweiten Strukturmerkmal bildete der Blick auf die beiden Verarbeitungsgrundsätze der *Datenrichtigkeit und Datensicherheit*. Sie sind zwar konkreter resp. weniger generalklauselartiger Natur. Gleichwohl gehören sie zu den grossen gemeinsamen Verarbeitungsgrundsätzen und weisen entsprechend breite wie facettenreiche Inhalte auf. Zudem gilt auch ihre Verletzung als begründend für eine Persönlichkeitsverletzung im privaten Bereich.[1039]

742 Der exakte Regelungsinhalt, der unter dem Titel des *Richtigkeitsgebotes* eingefangen wird, ist umstritten. Die hier vertretene Ansicht schliesst sich einer Meinung an, wonach absolute Richtigkeit im Sinne einer Nullfehlertoleranz unter dem Grundsatz der Datenrichtigkeit nicht verlangt werden kann. Eine erfolgreiche Berufung auf eine rein subjektiv verstandene Prüfungspflicht («Vergewissern») sowie ergriffene «angemessene Massnahmen» soll indes nicht beliebig zugelassen werden: Als im Sinne des Grundsatzes nicht genügend zu qualifizieren sind Massnahmen, die zwar vielleicht als weit- sowie tiefgreifend und damit gewissermassen in dieser Richtung als «angemessen» beurteilt werden könnten, die indes nicht ergebnisorientiert ein um einen Fehlerquotienten im Vorfeld definiertes statistisches Mindestmass an Richtigkeit erreichen. Ebenso wenig reicht die «Vergewisserung», wenn im Anschluss an die Feststellung der ungenügenden Richtigkeit, die am Zweck zu messen ist, nicht die «angemessenen Massnahmen» ergriffen werden, die das «angemessene Richtigkeitsniveau» bewerkstelligen. Der ergänzende Berichtigungsanspruch des Datensubjektes ist Konsequenz des subjektivrechtlich angeknüpften Datenschutzgesetzes. Zugleich wurde eine systemische Dimension datenschutzrechtlicher Herausforderungen im Rahmen der Erörterungen zum Gebot der Datenrichtigkeit sichtbar gemacht. Einschlägig war insofern die Praxis des «Credit Reporting» mit seinen Fehlerquoten: *Prima vista* scheinen weder die Kreditauskunfteien noch die Kreditinstitute ein Interesse zu haben, datenschutzkonform zu handeln, zumal sich diese vielmehr durch falsche Score-Werte wirtschaftlich alimentieren und es einzig und allein die Betroffenen sind, die durch falsche Score-Werte und damit nachteilige Konditionen belastet werden. An diesem Defizit setzen die USA mit ihrem *Fair Credit Reporting Act* an, einem der sektorspezifischen Erlasse für den privaten Bereich. Er verlangt ein akkurates und faires Kreditauskunftswesen, wobei der Erlass dies nicht primär zum Schutz des Individuums fordert. Vielmehr führt der Act zu Beginn aus, dass der *Bankensektor*, um *effizient* zu sein, auf das *Vertrauen der Allgemeinheit* angewiesen ist; unfaire und inakkurate Kreditauskunftspraktiken

1039 Zur Einbettung der allgemeinen Verarbeitungsgrundsätze in das Regime des datenschutzrechtlichen Persönlichkeitsschutzes im privaten Bereich zweiter Teil, VI. Kapitel, A.–C.

untergraben dieses Vertrauen und im Ergebnis die *Effizienz des Bereichs* selbst. Für die Schweiz wurde unter Berücksichtigung dieser systemischen Schutzdimension – spezifisch in Bezug auf die Vorgaben zur Datenrichtigkeit – eine Auslegeordnung präsentiert, wonach die Richtigkeit von Personendaten initial und rollend sicherzustellen ist. Als angemessene Massnahmen insofern können nur solche gelten, welche – in Anlehnung an die Ausführungen des Bundesgerichts im Google-Street-View-Entscheid – die Richtigkeit unter Berücksichtigung eines Fehlertoleranzquotienten sicherstellen. Eine Berufung auf das Ergreifen von «angemessenen» Massnahmen, die indes nicht dazu führen, dass das geforderte Richtigkeitsniveau erreicht wird, hält vor dem datenschutzgesetzlichen Richtigkeitsgebot nicht stand. Ein Verstoss gegen die Vorgaben ist insofern immerhin theoretisch mit Zurückhaltung rechtfertigbar. Abrundend ist für die Pflichten zur Datenrichtigkeit zu resümieren, dass flankierende Instrumente ausgebaut und konkretisiert werden, wobei ein risikobasierter Ansatz wirksam wird.

743 Zum Grundsatz der *Datensicherheit* wurde festgehalten, dass auch insofern keine «absolute» Sicherheit gefordert werden kann. Zudem sind die zur Gewährleistung der Datensicherheit zu ergreifenden Massnahmen heterogen sowie namentlich unter Berücksichtigung der mit den Personendatenverarbeitungsprozessen einhergehenden Risiken relativ. In diesem Sinne gibt es «no such thing as data security». Darüber hinaus wurde beschrieben, inwiefern die Instrumente und Massnahmen, die den Aspekt der Datensicherheit bewerkstelligen sollen, stark ausgebaut wurden und Ausdifferenzierung erfahren haben. Ein bedeutsames Element bei der Gestaltung der Vorgaben im Rahmen der Datensicherheit ist die *zeitliche Dimension*, indem die Datensicherheit durch Massnahmen im Vorfeld, rollend, aber auch im Falle von Datensicherheitsvorfällen zu garantieren ist. Vorgaben zur Datensicherheit finden sich nicht nur im DSG, sondern auch in der DSGVO. Im Zuge der Totalrevision leisten mehrere Instrumente einen Beitrag, um die Datensicherheit zu effektuieren. Zu nennen sind namentlich die Datenschutz-Folgenabschätzung sowie die Notifikationspflichten bei Datensicherheitsvorfällen, aber auch «privacy by design» sowie die Dokumentationspflichten. Für Personendatenverarbeitungen, die durch informationstechnologische Anwendungen unterstützt werden, haben – analog zum homöopathischen Ansatz, «Gleiches mit Gleichem zu behandeln» – technikbasierte Lösungen spezifische Bedeutung für die Gewährleistung der Datensicherheit.

744 Sowohl im Rahmen des Grundsatzes der Datensicherheit als auch in demjenigen der Datenrichtigkeit wurde aufgezeigt, dass die jüngsten Revisionswellen darauf abzielen, die allgemeinen Verarbeitungsgrundsätze nicht mehr bloss in abstrakter Weise vorzuschreiben. Vielmehr sehen sie *konkrete Umsetzungsinstrumente* vor, um die allgemeinen Verarbeitungsgrundsätze faktisch griffig werden zu lassen. Damit wurde ein Transformationsprozess nachgezeichnet: Die datenschutzrecht-

liche Fixierung auf einen defensiv gedachten Subjektschutz wird aufgeweicht und ergänzt, teilweise sogar verdrängt durch ein Konzept, wonach der Datenschutz zur «Governance»-Aufgabe und Teil eines Risikomanagements wird. Die Verantwortlichen werden frühzeitig und nachhaltig in die Pflicht genommen, angemessene Massnahmen – auch technischer und organisatorischer Natur – zur Gewährleistung der Grundsätze zu ergreifen. Die Angemessenheit dieser Massnahmen orientiert sich neu konsequent an einem risikobasierten Ansatz, womit der individualrechtliche Ansatz, der sogleich vertieft wird, ergänzt wird.

745 Durch eine Analyse der *generalklauselartigen gemeinsamen Verarbeitungsgrundsätze des DSG* zieht sich wie ein roter Faden die Erkenntnis, dass die Einschlägigkeit differenzierter Kontexte und Bereiche für und im bereits geltenden Datenschutzrecht resp. DSG anerkannt wird. Dies ist im Lichte des Eingangstitels, wonach das Datenschutzgesetz die individuellen Rechte des Einzelnen schützt, erstaunlich. Die Kontextrelevanz mag zudem auf den ersten Blick paradox erscheinen, befasst man sich doch mit den gemeinsamen Verarbeitungsgrundsätzen eines «Querschnittsgesetzes». Anknüpfend an das erste Strukturmerkmal, den Dualismus (mit seiner Zweiteilung des Regelungsregimes für den öffentlichen und den privaten Bereich), wurden im Rahmen der «gemeinsamen generalklauselartigen Verarbeitungsgrundsätze» gleichwohl an mehreren Stellen *Differenzierungen* nachgezeichnet, welche sich an der gröbsten Form bereichsspezifischer Differenzierung, am *Dualismus* zwischen staatlichem und gesellschaftlichem Bereich orientieren (z. B. unterschiedliche Transparenzvorgaben unter noch geltendem DSG für den öffentlichen und den privaten Bereich). Zugleich wurden anhand der allgemeinen Verarbeitungsgrundsätze Nuancierungen beschrieben, die weitergehende Differenzierungen eröffnen und gewissermassen die Einschlägigkeit pluraler Verarbeitungszusammenhänge und Kontexte sichtbar machen (so namentlich das Rechtmässigkeitsprinzip sowie der Zweckbindungsgrundsatz).[1040] Umgekehrt wurden Mechanismen nachgewiesen, die eine Annäherung im Schutzniveau der Datenschutznormierung für den privaten und den öffentlichen Bereich vorsehen – so der Import des Verhältnismässigkeitsprinzips im öffentlich-rechtlichen Sinne in den Bereich der Personendatenverarbeitung durch Private im DSG, aber auch der Monismus der DSGVO.

746 Die Bedeutung *pluraler Verarbeitungskontexte* für die Datenschutzgesetzgebung – wie sie anhand des allgemeinen Verarbeitungsgrundsatzes der Zweckbindung besonders gut sichtbar wird – sowie die Relevanz des Schutzes pluraler Bereiche ist damit im schweizerischen Datenschutzrecht selbst in den gemeinsamen, allgemeinen Verarbeitungsgrundsätzen angelegt. Dem Zweckbindungsgrundsatz kommt sowohl *de lege lata* mit seinem individualrechtlichen Rahmen als auch

1040 Zum Ansatz der kontextuellen Relevanz der privacy richtungsweisend die Arbeiten von Nissenbaum.

mit Blick auf die Rekonzeptionalisierung eine entscheidende Rolle zu.[1041] Richtungsweisend für die Erkenntnis, wonach der Zweck der Datenschutzregulierung ebenso im Schutz von gesellschaftlichen Bereichen, Institutionen, Kontexten oder Systemen liegt, waren die Ausführungen des Bundesverfassungsgerichts, insb. zum Zweckbindungsgrundsatz. Die kontextuelle Schutzdimension datenschutzrechtlicher Regulierungen wurde folglich – auch aufgrund der Selbstverständlichkeit, mit der das DSG in einer dualistischen Struktur und in einer individualrechtlichen, persönlichkeitsrechtlichen Anknüpfung verankert ist – in ihrer theoretischen und konzeptionellen Tragweite bislang ungenügend adressiert. Der bis heute prägenden *persönlichkeitsrechtlichen Anknüpfung des DSG für den privaten Bereich* als drittem Strukturmerkmal widmet sich das anschliessende VI. Kapitel dieses zweiten Teils. Es folgt eine vertiefte Beschäftigung mit der Funktionsweise der datenschutzgesetzlichen Vorgaben für den privaten Sektor, womit die subjektiv-, abwehr- und deliktsrechtlichen Ingredienzen genauer umrissen werden.

1041 Die Bedeutung des Verarbeitungszweckes wird für die Schweiz insb. thematisiert von Cichocki, Jusletter IT vom 21. Mai 2015, N 23 ff.

VI. Kapitel: Drittes Strukturmerkmal – Persönlichkeitsschutz

«Nicht die Struktur des Persönlichkeitsrechts bestimmt die Aufgaben des Datenschutzrechts, sondern die Struktur der Gesellschaft.»
– sinngemäss nach Spiros Simitis[1042]

A. Zum Einstieg

Der Schutz des Einzelnen vor *Eingriffen* durch Dritte erfolgt im Privatrecht klassischerweise über das *Deliktsrecht*.[1043] Es geht darum, «die Interessen des Geschädigten am Erhalt seiner Rechtsgüter gegen die Handlungsfreiheit des Schädigers abzuwägen».[1044] Indem das DSG an den Persönlichkeitsschutz und damit an die widerrechtliche Persönlichkeitsverletzung anknüpft, ist das *datenschutzgesetzliche Regime in erster Linie dem zivilrechtlichen Deliktsrecht* zugeordnet. 747

An dieser Stelle wird der Fokus auf das Datenschutzgesetz im privaten Bereich verengt. Der «Zweck» des Datenschutzgesetzes ist gemäss Art. 1 DSG resp. Art. 1 nDSG – neben dem Schutz der Grundrechte – der *Schutz der Persönlichkeit*. Die entsprechende Anknüpfung wurde im Rahmen der erstmaligen Verabschiedung des DSG vorgenommen. Insofern wurde vertreten, dass *Art. 28 ff. ZGB* für die Bewältigung der Herausforderungen gerade im Zusammenhang mit der technologisch unterstützten Personendatenverarbeitung datenschutzrechtlich nicht mehr genüge.[1045] Nach langem Ringen setzte sich die Überzeugung durch, wonach sich eine allgemeine Datenschutzgesetzgebung ebenso auf den privaten Bereich erstrecken müsse.[1046] Damit präsentiert sich die Datenschutzgesetzgebung für den privatrechtlichen Bereich – auch nach Totalrevision, trotz der damit einhergehenden Integration eines Compliance-Ansatzes – als *Konkretisierung von Art. 28 ff. ZGB*.[1047] Die nachfolgenden Ausführungen widmen sich der Regelungsmechanik im Detail. Damit wird eine *akkurate Charakterisierung* des Regelungsregimes möglich werden: Das DSG implementiert für den privaten Bereich – so die Schlussfolgerung – in erster Linie einen *Integritätsschutz und gerade kein sog. Recht auf informationelle Selbstbestimmung*. 748

1042 Insofern Simitis im Interview, <https://www.datenschutzzentrum.de/artikel/940-Interview-mit-Prof.-Dr.-Dr.h.c.-Spiros-Simitis.html> (zuletzt besucht am 30. April 2021).
1043 Ohly, 86.
1044 Ders., a. a. O.
1045 BBl 1988 II 414 ff., 441; Danioth, AB 88.032, 126: «[…] der Rechtsschutz gilt der Persönlichkeit und der Menschenwürde bei der Bearbeitung und Verwendung von Daten über eine Person»; Schweizer, 45; dazu, dass mit der Anknüpfung der privacy resp. des Datenschutzes in der Menschenwürde die Anlehnung an die Grundrechte gemacht wird, Birnhack, CLSR 2008, 508 ff., 509.
1046 Hierzu vertiefend zweiter Teil, IV. Kapitel.
1047 Vgl. neben den Gesetzgebungsmaterialien auch BGE 138 II 364, Regeste und E 8.

749 Die *persönlichkeitsrechtliche Basierung des Datenschutzgesetzes für den privaten Bereich* wird keineswegs bloss im Zweckartikel statuiert, vgl. Art. 1 DSG und Art. 1 nDSG. Vielmehr orientieren sich Art. 12 f. DSG resp. Art. 30 f. nDSG weitgehend konsequent an der Regelungsstruktur von Art. 28 ZGB.[1048] Die persönlichkeitsrechtliche Anknüpfung des DSG für den privaten Bereich schlägt sich logisch folgend zudem im Instrumentarium des Rechtsschutzes nieder, zum einen im Rahmen der Gewährleistung von Betroffenenrechten der Datensubjekte, zum anderen durch die zivilrechtlichen Klagebehelfe der Betroffenen, Art. 15 und Art. 25 DSG resp. Art. 32 nDSG und Art. 25 nDSG.

750 Das DSG ist in seiner Version vor der Totalrevision materiellrechtlich wie prozedural betrachtet für den privaten Bereich konsequent dem Schutz der *Person und Persönlichkeit verpflichtet*. An ebendieser Grundlegung sowie der reflexiven Konzeptionierung der allgemeinen Datenschutzgesetzgebung für den privaten Bereich wird im Zuge der Totalrevision des DSG weitgehend festgehalten, vgl. Art. 1 nDSG und Art. 30 ff. i. V. m. Art. 6 nDSG. Einschneidende Neuerungen finden sich für den privaten Bereich allerdings im Ausbau der Durchsetzungsinstrumente, sowohl was die Kompetenzen des EDÖB als auch was die strafrechtlichen Sanktionen anbelangt. Zudem wird die persönlichkeitsrechtliche Konzeption zwar nicht aufgegeben, doch aber – wie bereits gezeigt – markant ergänzt. Die entsprechenden Entwicklungstrends (Integration eines Compliance-Ansatzes sowie risikobasierten Ansatzes sowie von Instrumenten zur faktischen Einhaltung der Vorgaben) sind massgeblich von der DSGVO angestossen.[1049]

751 Gleichwohl ist – und bleibt – das DSG für den Bereich der Verarbeitung durch Private im *zivilrechtlichen Persönlichkeitsschutz* verwurzelt, Art. 1 i. V. m. Art. 12 i. V. m. Art. 4 ff. DSG resp. Art. 1 i. V. m. Art. 30 f. i. V. m. Art. 6 nDSG. Nachfolgend werden der Regelungsinhalt und die Regelungsstruktur von Art. 12 f. DSG (i. V. m. Art. 4 ff. DSG) resp. Art. 30 f. nDSG (i. V. m. Art. 6 und 8 nDSG) sowie die Details der persönlichkeitsrechtlichen Dogmatik im Rahmen des DSG als dessen *drittes Strukturmerkmal* dargestellt.

752 Vorausschickend in Erinnerung zu rufen sind die Erkenntnisse aus den vorangehenden Teilen, namentlich die beiden bereits beschriebenen Strukturmerkmale des DSG. Sie vervollständigen den Betrachtungsrahmen: Die Analyse im Rahmen

1048 Dazu, dass Art. 28 ZGB und der zivilrechtliche Persönlichkeitsschutz in zahlreichen Spezialgesetzen, auch dem DSG, «herumgeistert», Riemer, sic! 1999, 103 ff., 103; zum allgemeinen Persönlichkeitsrecht Ehmann, in: Stathopoulos/Beys/Philippos/Karakostas (Hrsg.), 113 ff.; eine prägnante Übersicht über die datenschutzgesetzliche Regelung der Verletzungstatbestände im Privatbereich und die Rechtfertigungsgründe findet sich bei Steinauer, in: Schweizer (Hrsg.), 43 ff. und 53, wo er festhält, dass es sich bei den DSG-Normen einzig um eine konkretisierende Wiederholung von Art. 28 DSG handle.

1049 Eine gegenüberstellende Betrachtung des totalrevidierten DSG und der DSGVO legt jüngst auch Baeriswyl, SZW 2021, 8 ff. vor.

der *allgemeinen, «gemeinsamen» und über weite Strecken generalklauselartigen Verarbeitungsgrundsätze* sowie der an diese angekoppelten Neuerungen hat gezeigt, dass in ihnen ergänzende Perspektiven und Dimensionen gegenüber einem defensivrechtlich gedachten Datenschutzrecht, das die Struktur von Art. 28 ZGB rezipiert, angelegt sind. Auch im Rahmen der Beschreibung der *dualen Struktur des DSG* wurde die Anerkennung der Einschlägigkeit der kontextuellen Dimension thematisiert. Herausgearbeitet wurde darüber hinaus, dass mit den jüngsten datenschutzrechtlichen Neuerungen die verantwortlichen personendatenverarbeitenden Stellen primär und nachhaltig in die Pflicht genommen werden, die datenschutzrechtlichen Vorgaben einzuhalten.

753 Damit zeigte sich im Laufe der bisherigen Studie, dass eine subjektivrechtliche, individualrechtliche und deliktsrechtliche Konzeption – wie sie in einer isolierten Betrachtung von Art. 1 (n)DSG und Art. 12 f. i. V. m. Art. 4 DSG resp. Art. 30 f. i. V. m. Art. 6 nDSG durchaus konsequent umgesetzt wird – nicht rein verwirklicht ist. Wird das Herzstück der datenschutzrechtlichen Bestimmungen für den privaten Bereich einbettend analysiert, zeigt sich, dass eine isolierte Betrachtung der datenschutzgesetzlichen Vorgaben als Abbild des zivilrechtlichen Persönlichkeitsschutzes nicht ganz akkurat charakterisiert. Isoliert betrachtet allerdings sind die Bestimmungen des DSG für den privaten Bereich in konsequenter Weise ein Abbild der Konzeption gemäss Art. 28 ZGB. Der *Schutzzweck* des DSG ist demnach für den privaten Bereich ausdrücklich die Persönlichkeit des Datensubjektes, vgl. auch Art. 1 (n)DSG und Art. 12 f. DSG resp. Art. 30 f. nDSG. Eine damit *subjektivrechtliche und – für den privaten Bereich – persönlichkeitsrechtliche Fundierung* hält sich somit bis heute im schweizerischen DSG.[1050] Diese individualrechtliche Anknüpfung datenschutzgesetzlicher Vorgaben für den privaten Bereich gilt gewissermassen als «naturgegeben»: Denn was anderes als das Individuum, der Mensch als Subjekt und damit die Person resp. Persönlichkeit, sollte geschützt werden in Anbetracht von Informationstechnologien, deren Macht in der potentiellen Degradierung des Menschen zum Objekt, zu einer Nummer, beschrieben wird?[1051]

754 In diesem Zusammenhang ist die in kaum einem Beitrag zur Datenschutzgesetzgebung fehlende Kritik an der unglücklichen und missverständlichen Titulierung der Erlasse als «Datenschutz(-gesetz)» zu erwähnen: Mit dem Datenschutzrecht

1050 So unlängst eindrücklich auch die verschiedenen Beiträge im Rahmen der 12. Tagung zum Datenschutz – jüngste Entwicklungen am 5. Februar 2019.

1051 Menschen sollen «nicht einfach Informationsobjekte sein», vgl. Nabholz, 3; vgl. auch Pedrazzini, Wirtschaft und Recht 1982, 27 ff., 32, wonach der Einzelne nicht rechtloses Objekt von Informationsprozessen sein, stattdessen die Kenntnisse und das Bild, welches andere von ihm haben, selbst bestimmen oder beeinflussen können soll; m. w. H. auch Pohle, 18.

resp. den Datenschutzgesetzen würden *nicht* Daten, sondern *Personen*, Menschen, Bürgerinnen und Bürger vor Datenverarbeitungen geschützt.[1052] Denn:

> «Umstrittene Informationsbearbeitungen im öffentlichen wie im privaten Bereich haben uns für die Belange des Persönlichkeitsschutzes unterdessen sensibilisiert, und Datenschutz ist ja nichts anderes als Persönlichkeitsschutz.»[1053]

755 Gleichwohl dokumentiert sich in der Bezeichnung «Datenschutzgesetz» und den hierzu gemachten Ausführungen, dass die datenschutzrechtliche Strukturierung und Herangehensweise in einem *Subjekt-Objekt-Denken* verwurzelt ist. Nicht abgebildet wird mit der Titulierung eine Konzeptionierung, wonach es um die *Gestaltung und Normierung von Datenflüssen* geht. Die Sinnhaftigkeit und Notwendigkeit einer solchen Betrachtungsweise wurde im Laufe dieser Schrift bis hierher an mehreren Stellen dargelegt. Die Neuerungswellen haben eine entsprechende Herangehensweise eindrücklich implementiert. Mit einer Perspektive, welche Personendatenflüsse fokussiert, rückt die Frage nach der Einschlägigkeit von Verarbeitungszusammenhängen und -kontexten in den Blick. Die Analysen zu den Verarbeitungsgrundsätzen mit den neuen Instrumenten, die diese verwirklichen sollen, haben diese prozesshafte Dimension des Datenschutzes vor Augen geführt.

756 Ungeachtet dieser jüngsten Entwicklungen sowie der bis heute von Gesetzes wegen *unmissverständlichen Anknüpfung des DSG im Persönlichkeitsschutz* für den privaten Bereich bleibt die Auseinandersetzung mit dem Rechtsgebiet geprägt von *mannigfaltigen Variationen* in Bezug auf die Nomenklatur, Beschreibungen und Konkretisierungen mit Blick auf Schutzzweck, -ziel und -mechanismen resp. die Regelungsmechanik des DSG. Ebendies ist insofern bemerkenswert, als dass der Gesetzeswortlaut sowie die Kernstruktur der Regelung des DSG eindeutig zu sein scheinen. Es geht im Datenschutzrecht um den Persönlichkeitsschutz in Anlehnung an Art. 28 ZGB. Die Schaffung anderer Überbegriffe resp. Bezüge, z. B. zur Privatheit oder Privatsphäre oder informationellen Selbstbestimmung, könnte sich damit zumindest *prima vista* erübrigen.

757 Dass sich die Schweizer Lehre, Rechtsprechung und Praxis zum DSG mit weiteren Konzepten und Begrifflichkeiten unter dem Titel des Datenschutzrechts befasst, ist gleichwohl gut begründet. An dieser Stelle manifestiert sich eine typologische Herausforderung des Datenschutzes, mit der sich bis heute weltweit die verschiedensten Disziplinen konfrontiert sehen. Es geht um die Kernherausforderung oder -problematik des Datenschutzes und seines Rechts selbst – die

1052 Vgl. Forstmoser, digma 2003, 50 ff., 51; dazu, dass Datenschutzgesetze nicht in erster Linie Daten schützen, sondern eine Degradierung der Bürgerinnen und Bürger zu Informationsobjekten verhindern sollen, Bründler, SJZ 1993, 129 ff., 133; kritisch zu den Begrifflichkeiten Simitis, Nomos-Komm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 und N 26.

1053 Koller, AB 88.032, 5. Juni 1991, 984.

Definierung *«des Privaten»*, das seinerseits selbst dieser Tage als Schirmbegriff für datenschutzrechtliche Ziele figuriert.[1054] Bis heute gilt das «Versagen», den Dachbegriff des «Privaten» dingfest zu machen und griffig zu beschreiben, als ein Hauptproblem der Datenschutzregulierung und als eine Ursache für dessen ungenügende Wirksamkeit.[1055] In diesem Sinne bezeichnete der Sonderberichterstatter der Vereinten Nationen das «Fehlen einer verbindlichen Definition zur Privatsphäre als Haupthindernis für deren umfassenden rechtlichen Schutz».[1056]

758 Illustrativ und indikativ für die Reichhaltigkeit und Weite der Konzepte, aber auch die Orientierungslosigkeit in Bezug auf Schutzziele und -objekte des Datenschutzes auch in der Schweiz sind die im erläuternden Bericht zur Totalrevision des Datenschutzgesetzes auf rund drei Seiten aufgeführten politischen Vorstösse, die im Kontext des Datenschutzes anhängig gemacht wurden:[1057] Besser geschützt werden soll «das Grundrecht auf informationelle Selbstbestimmung»; gefordert wird ein «Eigentum der Person an ihren Daten»; zu stärken sind das «Recht auf Schutz des Privatlebens», die «Privatsphäre und persönliche Freiheit»; gefordert wird ein «Recht auf Vergessen im Internet»; vorgeschlagen wird ein «Recht auf Kontrolle über persönliche Daten» usf. In der Botschaft zur Revision des DSG mittels Totalrevision wurde die Abschreibung mehrerer entsprechender parlamentarischer Vorstösse beantragt.[1058]

759 In den datenschutzgesetzlichen Anfängen referierte die Botschaft zum DSG über das Recht auf informationelle Selbstbestimmung mit den Worten:

> «Jedermann soll, soweit die Rechtsordnung nichts anderes vorsieht, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen und frei über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können».[1059]

760 Insofern sind Präzisierungen angezeigt. Den Ausführungen zur Funktionsweise des DSG im privaten Bereich sei vorausgeschickt, dass das DSG selbst gewissermassen «definitionsblind» und «ohne Etikettierung» eine Regulierung implementiert, die sich konsequent an der Regelungsmechanik von Art. 28 ZGB orientiert und diesen spezifisch für den Umgang mit Personendaten konkretisiert. Ganz ohne Bezugnahme auf Begriffe wie die «Privatsphäre», «informationelle Selbstbe-

1054 Vgl. exemplarisch zur Privatheit Aebi-Müller, N 646 ff., aber auch zu den Kategorien der Privatsphäre und informationellen Selbstbestimmung, N 512 ff. und N 541 ff.

1055 In diesem Zusammenhang zum Inhalt ihres Werks die amerikanische Philosophin Nissenbaum: «It does not carve a pathway through the conceptual quagmire to claim a definition – its definition – of privacy. Nevertheless, it is a book about privacy because it explains why the huge and growing set of technical systems and technology-based practices have provoked and continue to provoke anxiety, protest, and resistance in the name of privacy», 130; zur Privatsphäre als komplexes Konzept, das stets auch wandelbar ist, Hotter, 9 ff.

1056 HRC, Special Rapporteur Right to Privacy 2016, N 9; vgl. EJPD, Erläuternder Bericht, 1 ff., 16.

1057 EJPD, Erläuternder Bericht, 1 ff., 10 ff.

1058 BBl 2017–1084, 17.059, 6941 ff., 6941.

1059 BBl 1988 II 414 ff., 418.

stimmung», «Missbrauchsgesetzgebung», den Blick von einer Definierung resp. Titulierung wegführend wies ebenso Rhinow im Rahmen der parlamentarischen Verhandlungen zur Verabschiedung eines DSG darauf hin, dass dieses

> «im privatrechtlichen Verhältnis die Mechanik des Persönlichkeitsschutzes von Art. 28 ZGB übernimmt».[1060]

761 Mittels konsequenter Referenz auf die persönlichkeitsrechtliche Anknüpfung gemäss Art. 28 ZGB des DSG für den privaten Bereich scheint man den Weg durch das «Dickicht» der unzähligen Definitionsversuche zu dem das Datenschutzrecht prägenden Dachbegriff des Privaten umgehen zu können. Eine Beschreibung könnte sich darauf beschränken, die als Persönlichkeitsverletzung umschriebenen Handlungen und das Rechtfertigungsregime zu benennen, ohne dass damit eine weitere Titulierung einhergehen müsste. Dennoch ist eine Auseinandersetzung mit Definierungs- und Charakterisierungsversuchen zumindest punktuell lohnenswert: Mit ihr lassen sich strukturierende Begrifflichkeiten für das DSG und seine Funktionsweise im privaten Bereich herausarbeiten. Eine präzise Charakterisierung des DSG mit seiner Regelungsmechanik ist ein Fortschritt für den datenschutzrechtlichen Diskurs in der Schweiz, zumal nicht zuletzt in der Allgemeinheit insofern auch Fehlannahmen zu kursieren scheinen.

762 Knüpft das DSG für den Privatsektor an das System des zivilrechtlichen Persönlichkeitsschutzes gemäss Art. 28 ZGB an, ist vorab die entscheidende Frage, wie die Verletzung der Persönlichkeit durch Personendatenverarbeitungen vom DSG umrissen wird. Rezipiert wird das Regime des DSG seinerseits mit einem beachtlichen Variantenreichtum an Begrifflichkeiten und Charakterisierungen. Ebendies sei anhand einiger kurzer Passagen illustriert.

763 Die erste Umschreibung stammt aus dem Evaluationsbericht zum DSG, wobei diese bereits im Licht der bislang generierten Erkenntnisse nicht zu überzeugen vermag. Ebenda liest man:

> «Allgemein gesprochen stellt somit die Bearbeitung von Personendaten durch private Bearbeiter eine widerrechtliche Persönlichkeitsverletzung dar, wenn nicht ein Rechtfertigungsgrund vorliegt.»[1061]

764 Ähnlich, wenn auch ohne Aussage zum Tatbestandselement der Widerrechtlichkeit, wird auch vertreten:

> «Jede Form der privaten Datenbearbeitung ist eine Persönlichkeitsverletzung.»[1062]

765 Aebi-Müller führt unter Referenz auf deutsche Quellen aus:

> «Nicht mehr der Schutz bestimmter Bereiche […] steht nunmehr im Zentrum, sondern der Gedanke, dass dem Betroffenen die Herrschaft über seine Daten und deren Verwen-

1060 Rhinow, AB 88.032, 13. März 1990, 130.
1061 Bolliger/Féraud/Epiney/Hänni, 106.
1062 VPB 68.68. Erw. 31/a.

> dung zukommen soll. Massgebend für das Vorliegen einer Verletzung ist damit der *Wille der Person*, auf dies [sic!] sich die Information bezieht. Kern des Datenschutzgesetzes ist entsprechend dieser Vorstellung ein Recht auf informationelle Selbstbestimmung. Nur der Betroffene bestimmt, welchen Wert er den auf ihn bezogenen Daten zumisst […]. Dieses *Herrschaftsrecht an den eigenen Daten* ergibt sich – obschon der Begriff der informationellen Selbstbestimmung sich im Schweizerischen DSG nicht findet – namentlich aus Art. 12 Abs. 2 Bst. b […], sowie aus Art. 12 Abs. 3 DSG (e contrario) […].»[1063]

766 Und an anderer Stelle weitergehend dieselbe Autorin:

> «Durch das Recht auf informationelle Selbstbestimmung wird die unter der Sphärentheorie begründete Gemeinsphäre vollständig aufgelöst: Es gibt keine Daten mehr, die unabhängig vom Willen des Betroffenen bearbeitet werden können.»[1064]

767 Eine Umschreibung von Rosenthal schliesslich lautet:

> «Um einer Person den Schutz der Persönlichkeit zu erleichtern, hat der Gesetzgeber mit Art. 4 Abs. 1–4 die unwiderlegbare Vermutung aufgestellt, die Persönlichkeit der betroffenen Person sei verletzt. Das ist der einzige Zweck der Bestimmung.»[1065]

768 Eine beachtliche Divergenz für ein und dasselbe Gesetz. Ebendies ist (er)klärungsbedürftig, gerade auch, weil für die zitierten Autorinnen resp. Autoren die Rechtslage in gänzlich unterschiedlicher Weise klar ist. Doch genau darin liegt das Problem.

769 Anders gewendet: Es besteht Klärungsbedarf bezüglich der Persönlichkeitsverletzung durch Personendatenverarbeitungen gemäss DSG im privaten Bereich und, allgemeiner, im Hinblick auf das Schutzobjekt resp. den Schutzzweck sowie die Schutzmechanik. Die nachfolgenden Erörterungen dienen dazu, die persönlichkeitsrechtliche Funktionsweise des schweizerischen Datenschutzgesetzes zu klären. In der Folge soll das Regime einer gesetzeskonformen und präzisen Charakterisierung zugeführt werden.

770 Hierbei wird sich zunächst zeigen, dass sich die markanten Differenzen zwischen den verschiedenen Interpretationen keineswegs auf Auslegungsdetails zurückführen lassen. Vielmehr wird die Analyse des Regimes des DSG für den privaten Bereich die Schlussfolgerung zulassen, wonach die trefflichste Beschreibung der Regelungsmechanik des DSG sich des Begriffs des *Integritätsschutzes* bedient. Er zielt darauf ab, die *elementar(st)en Erwartungen an eine faire Personendatenverarbeitung* zu gewährleisten resp. *missbräuchliche Verarbeitungshandlungen* zu verhindern. Das ist die datenschutzgesetzliche *Basiskonstruktion* für den privaten Bereich, es sei denn, es greifen spezifische Verarbeitungsvorgaben.

1063 M. w. H. Aebi-Müller, N 591 f.
1064 Dies., 611.
1065 Rosenthal, HK-DSG, Art. 4 N 77; vgl. zu den verschiedenen Schutzbegriffen wie Datenschutz, Recht auf informationelle Selbstbestimmung, Recht auf Schutz der Privatsphäre und der Persönlichkeit auch Epiney/Civitella/Zbinden, 7.

771 Grundlegend für das Verständnis der datenschutzgesetzlichen Normierung für den privaten Bereich sind ergänzend die Ausführungen zum *Dualismus* mit dem Ausgangspunkt der prinzipiellen Freiheit der Personenverarbeitung mit Schranken.[1066] Daran anknüpfend und unter Bezugnahme auf die unterschiedlichen Ausgangspunkte für den privaten und öffentlichen Bereich des Bundes wurden die allgemeinen Verarbeitungsgrundsätze dargestellt.[1067] Sie sind der Kern des materiellen Datenschutzrechts, der gleichwohl eine unterschiedliche Bedeutung infolge der unterschiedlichen Ankoppelung für den privaten resp. öffentlichen Bereich findet.

772 Die allgemeinen Verarbeitungsgrundsätze gemäss Art. 4 ff. DSG resp. Art. 6 ff. nDSG spielen eine zentrale Rolle für die *Definierung der Persönlichkeitsverletzung* im privaten Bereich, vgl. Art. 12 Abs. 2 lit. a DSG und Art. 30 Abs. 2 lit. a nDSG. Allerdings erschöpft sich darin das Regime des Datenschutzgesetzes für den privaten Bereich nicht. Vielmehr fügen die Art. 12 Abs. 2 lit. b und lit. DSG resp. Art. 30 Abs. 2 lit. b und c nDSG weitere Ingredienzen ein.

773 Die Analyse von Art. 12 Abs. 2 lit. a–c DSG wird zeigen, dass die *zweite Kammer des dualen Systems* – die Datenschutzgesetzgebung für den privaten Sektor – ein *nuanciertes Regime* darstellt. In diesem werden mehrere Kriterien – objektive, aber auch subjektive – eingesetzt, um die Persönlichkeitsverletzung qua Personendatenverarbeitung konkreter zu definieren.

774 Im Rahmen der Beschreibung dieses Regimes wird insb. auch auf Bedeutung und Funktion der *datenschutzrechtlichen Einwilligung* eingegangen werden, vgl. Art. 12 Abs. 2 lit. b, Art. 12 Abs. 3 und Art. 13 DSG, zudem auch Art. 4 Abs. 5 DSG resp. Art. 30 Abs. 2 lit. b und Art. 30 Abs. 3 nDSG, Art. 31 nDSG sowie Art. 6 Abs. 6 und Abs. 7 nDSG. Die Ausführungen rücken das noch geltende Gesetz vor seiner Totalrevision in das Zentrum. Auf eine vertiefte Darstellung der angepassten und ausgebauten Einwilligungsvorgaben, wie sie das totalrevidierte DSG insb. für spezifisch neu geregelte Konstellationen wie das Profiling vorsieht, wird verzichtet.[1068] Die Vorgaben in Bezug auf die Einwilligung wurde bewusst *nicht* unter dem Titel der allgemeinen Verarbeitungsgrundsätze erörtert, obschon vom Gesetzgeber ebenda eingeordnet. Die Erklärung für die in dieser Arbeit gewählte Systematik ist, dass Art. 4 Abs. 5 DSG resp. neu Art. 6 Abs. 6 und Abs. 7 nDSG die Einwilligung gerade *nicht* als Verarbeitungsgrundsatz resp. Legitimationstatbestand für grundsätzlich verbotene Verarbeitungshandlungen positioniert. Vielmehr umschreibt Art. 4 Abs. 5 DSG einzig die *Anforderungen für eine gültige*

1066 Zweiter Teil, IV. Kapitel.
1067 Zweiter Teil, V. Kapitel.
1068 Verwiesen wird insofern insb. auf die Dissertation von Heuberger, sodann die jüngsten Beiträge zum totalrevidierten DSG; zum Profiling mit Blick auf den Banksektor weiter Vasella, in: Emmenegger (Hrsg.), 189 ff.

Einwilligung genauer, sofern die Einwilligung rechtlich verlangt ist. Ebendies allerdings ist, wie zu zeigen sein wird, nach DSG selbst für den privaten Bereich nur ausnahmsweise der Fall.

775 Die datenschutzgesetzliche Regelung der Schweiz für den privaten Bereich weist, wie zu zeigen sein wird, *verschiedene Komponenten und Ansätze* auf. Sie sind in den Abs. 2 lit. a–c und Abs. 3 von Art. 12 DSG resp. Art. 30 Abs. 2 lit. a–c nDSG und Abs. 3 nDSG abgebildet. Stark ausgeprägt ist die Ingredienz eines *Integritätsschutzes* (Art. 12 Abs. 2 lit. a DSG, Art. 30 Abs. 2 lit. a nDSG); zurückhaltend Eingang findet der Aspekt eines *Selbstbestimmungsrechts* (Art. 12 Abs. 2 lit. b und Abs. 3 DSG, Art. 30 Abs. 2 lit. b und Abs. 3 nDSG), wohingegen sich in prägnanter Weise weiterhin die traditionsreiche *Sphärentheorie* abgebildet findet (Art. 12 Abs. 2 lit. c und Abs. 3 DSG, Art. 30 Abs. 2 lit. c und Abs. 3 nDSG). Obschon das DSG für den privaten Bereich die Schwächen der Sphärentheorie bewältigen wollte,[1069] findet sich weiterhin die an einem sphärentheoretischen Konzept ausgerichtete Zweiteilung zwischen öffentlich versus privat. Damit liesse sich sagen, die kursierenden Umschreibungen hätten alle eine gewisse Berechtigung. Es geht indes fehl, diese in pauschaler und generalisierter Weise als Beschreibung für das datenschutzgesetzliche Regime des privaten Bereichs an sich resp. im Gesamten einzusetzen. Suggeriert werden dann ein Rechtsbestand und ein Regelungsregime, die so (pauschal) vom DSG nicht gewährleistet werden. Zugleich wird damit nicht mehr ersichtlich, wie nuanciert und gleichzeitig konsequent das DSG für den privaten Bereich am zivilrechtlichen Persönlichkeitsschutz ausgerichtet ist. Hierzu sogleich mehr.

B. Regelungsinhalt von Art. 12 f. DSG resp. Art. 30 f. nDSG

776 Der Grundsatz der Bearbeitungsfreiheit ist Ausgangspunkt des Schweizer Systems für den privaten Bereich. Hierbei markieren *qualifizierte Verarbeitungshandlungen* die Schranken der prinzipiellen Verarbeitungsfreiheit, indem diese zugleich die Persönlichkeitsverletzung begründen, vgl. Art. 12 Abs. 1 und Abs. 2 DSG resp. Art. 30 Abs. 1 und Abs. 3 nDSG.

777 Nach schweizerischem DSG ist nicht jede Personendatenverarbeitung prinzipiell verboten; nicht jede Personendatenverarbeitung bedarf eines Erlaubnistatbestandes. Das DSG taxiert auch nach Totalrevision nur die *qualifizierte Personendatenverarbeitung als Persönlichkeitsverletzung, deren Widerrechtlichkeit bei Vorliegen eines Rechtfertigungsgrundes entfallen kann, vgl. Art. 12 f. DSG und Art. 30 f. nDSG*. Umgekehrt und mit anderen Worten bedeutet dies zugleich, dass

1069 Vgl. zu den Mängeln des bisherigen Rechts und der Abwicklung über Art. 28 ff. ZGB Schweizer, 40 ff.

ein weites Feld an Personendatenverarbeitungen *unterhalb der Schwelle der Persönlichkeitsverletzung* und damit innerhalb des freien Verarbeitungsbereiches liegt.

778 Stattdessen geht die DSGVO prinzipiell vom Verarbeitungsverbot sowohl für private als auch für öffentliche Stellen aus. Grundsätzlich bedarf jeder Umgang mit Personendaten eines Erlaubnistatbestandes, vgl. Art. 6 DSGVO. Die DSGVO sieht damit ein gänzlich anderes Regime vor als das DSG mit seinem Dualismus und seiner prinzipiellen Verarbeitungsfreiheit mit Schranken für den privaten Bereich, welche die Struktur des zivilrechtlichen Persönlichkeitsschutzes rezipiert.

779 Gleichwohl sind in der Schweiz mit der Totalrevision neue Instrumente unabhängig von ihrer Einbindung in das persönlichkeitsrechtliche Regime zu beachten. Das totalrevidierte DSG ergänzt den persönlichkeitsrechtlichen Ansatz markant über mehrere neue Elemente, die stets zu beachten und implementieren sind – ungeachtet der Frage, ob eine Personendatenverarbeitung die Schwelle der zivilrechtlichen Persönlichkeitsverletzung über- oder unterschreitet.

780 Der Fokus richtet sich sogleich indes auf *die Kernbestimmungen der datenschutzrechtlichen Persönlichkeitsverletzung* resp. ihre Rechtfertigung und damit die besonderen Bestimmungen zur Datenbearbeitung durch private Personen, vgl. Art. 12 ff. DSG und Art. 30 ff. nDSG. Mit der Totalrevision bleibt die Koppelung der datenschutzgesetzlichen Anknüpfung an den zivilrechtlichen Persönlichkeitsschutz und die Normierung seiner *sedes materiae* weitgehend erhalten. Die besonderen Bestimmungen des DSG für den privaten Bereich, die explizit am Persönlichkeitsschutz anknüpfen, finden nur marginale Änderungen. Ebendies darf aber nicht darüber hinwegtäuschen, dass die Entwicklungen ausserhalb dieser Bestimmungen die persönlichkeitsrechtliche Anknüpfung des DSG neu einbetten.

781 Das Regime gemäss Art. 12 ff. DSG resp. Art. 30 ff. nDSG präsentiert sich weitgehend als Abbild der Struktur von Art. 28 ZGB. Die nachfolgenden Ausführungen widmen sich vorab den Personendatenverarbeitungen, die unterhalb der Schwelle der Persönlichkeitsverletzung liegen. Anschliessend werden die qualifizierten Verarbeitungshandlungen beleuchtet, die eine Persönlichkeitsverletzung verursachen. Es folgt die Betrachtung der Rechtfertigungsgründe sowie des Rechtsschutzes, insb. des zivilrechtlichen Rechtsschutzes gemäss DSG.

1. Nicht persönlichkeitsverletzende Personendatenverarbeitungen

782 Nach DSG sind es im Wesentlichen *zwei Konstellationen*, gemäss denen Personendatenverarbeitungen prinzipiell *nicht als persönlichkeitsverletzend* gelten. Sie sind in Art. 12 Abs. 2 und Abs. 3 DSG resp. Art. 30 Abs. 2 und Abs. 3 nDSG niedergelegt. Abs. 2 umschreibt, wann resp. in welchen Fällen Persönlichkeitsverlet-

zungen qua Personendatenverarbeitung vorliegen – die Konstellation wird als positive Seite von Art. 12 DSG resp. 30 nDSG bezeichnet.[1070] Der negativen Seite widmet sich Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG.

Erstens begründen die Personendatenverarbeitungen keine Persönlichkeitsverletzung, welche in Einklang mit den allgemeinen Verarbeitungsgrundsätzen vorgenommen werden, Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG. 783

Zweitens wird dem Grundsatz nach keine Persönlichkeitsverletzung angenommen bei Personendatenverarbeitungen, die sich auf allgemein zugänglich gemachte Personendaten beziehen, sofern kein ausdrücklicher Widerspruch anhängig gemacht wurde, Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG. 784

Beiden Konstellationen ist gemein, dass die Verarbeitungshandlungen *nicht als hinreichend invasiv* taxiert werden, um die Schwere einer Persönlichkeitsverletzung zu erlangen. In Anlehnung an die in Art. 28 ZGB angelegte Struktur und Dogmatik fehlt es am *qualifizierenden Merkmal* der «hinreichenden Schwere» einer Handlung, eines Verhaltens resp. eines Eingriffs, die diese zur Persönlichkeitsverletzung machen würde. 785

1.1. Verarbeitungsgrundsätze achtende Verarbeitungshandlungen

Die *erste Gruppe von Personendatenverarbeitungen*, die nicht als persönlichkeitsverletzend gilt, umfasst grob diejenigen Verarbeitungshandlungen, welche die allgemeinen Bearbeitungsgrundsätze einhalten, vgl. Art. 12 Abs. 1 und Abs. 2 lit. a *e contrario* i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 1 und Abs. 2 lit. a *e contrario* i. V. m. Art. 6 und Art. 8 nDSG. Kursierende Lehrmeinungen, wonach jede Personendatenverarbeitung eine Persönlichkeitsverletzung begründet oder wonach die Einwilligung des Datensubjektes eine Voraussetzung für eine rechtmässige Datenverarbeitung ist, finden damit im DSG weder vor noch nach seiner Totalrevision eine rechtliche Grundlage. Von Gesetzes wegen greift im privaten Bereich die prinzipielle Freiheit der Datenbearbeitung. Sie wird beschränkt durch Leitplanken in Gestalt der allgemeinen Verarbeitungsgrundsätze. 786

In die Struktur von Art. 28 f. ZGB übersetzt bedeutet dies: Erst *qualifizierte Verarbeitungshandlungen* gelten von Gesetzes wegen als persönlichkeitsverletzend. An erster Stelle sind die Verarbeitungshandlungen, welche die allgemeinen Verarbeitungsgrundsätze missachten, persönlichkeitsverletzend, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG. Die allgemeinen Verarbeitungsgrundsätze, denen 787

1070 Vgl. Rampini, BSK-DSG, Art. 12 N 4.

sich das V. Kapitel widmete, markieren im privaten Bereich den *Grenzverlauf zwischen zu duldender resp. persönlichkeitsverletzender Verarbeitung*.

788 Das datenschutzgesetzliche Regime lässt sich für diese Konstellation wie folgt charakterisieren: Die Vorgaben, die mit den allgemeinen Verarbeitungsgrundsätzen verbürgt werden, gewährleisten mit der Ankoppelung an den prinzipiellen Grundsatz der Verarbeitungsfreiheit im privaten Bereich eine *Garantie der fairen, integren und nachvollziehbaren Datenverarbeitung*. Ebendies steht, ohne die grosse Debatte rund um die Wirkung der Grundrechte im Privatrecht zu eröffnen, durchaus mit der verfassungsrechtlichen Idee gemäss dem Wortlaut von Art. 13 Abs. 2 BV und einem Konzept der Verhinderung von Missbrauch in Einklang.[1071]

789 Der *Integritätsschutz* gemäss Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG wird zwar durch die neu eingeführten Instrumente mit der Totalrevision angereichert um eine organisatorisch-prozesshafte Dimension. Es sind die Verarbeitenden, die zu gewährleisten haben, dass die Personendatenverarbeitungen unter Einhaltung der Verarbeitungsgrundsätze erfolgen. Sie sichern für den Bereich der Personendatenverarbeitung die *Fairness, Integrität resp. Abwesenheit eines Missbrauchs* ab. Die Verarbeitenden sind dazu *proaktiv* verantwortlich, womit das *defensivrechtliche Konzept*, wie es im zivilrechtlichen Persönlichkeitsschutz angelegt ist, ergänzt wird. Die Totalrevision wählt mit der Schaffung neuer Instrumente eine Strategie, die dem materiellrechtlichen Kernbestand des Datenschutzrechts mit seinen Verarbeitungsgrundsätzen Nachachtung verleihen soll. Gleichwohl hängt auch künftig die Effizienz dieses Regimes für den privaten Bereich, das *kein grundsätzliches Verbot* mit Erlaubnistatbeständen vorsieht, wie erläutert nicht unwesentlich davon ab, wie eindeutig die *Verarbeitungsgrundsätze die Demarkationslinien* zwischen persönlichkeitsverletzender und nicht persönlichkeitsverletzender Verarbeitungshandlung fixieren.

790 Die generalklauselartigen Verarbeitungsvorgaben erlangten allerdings in ihrer noch geltenden Fassung nur teilweise strukturierende und konkretisierende Griffigkeit. Das Datenschutzrecht hat bei Lichte betrachtet erst mit der Totalrevision auch in der Schweiz grösseres Interesse im Schrifttum auf sich gezogen. Durch die beschränkten Kompetenzen des EDÖB nach geltendem DSG und der eher rudimentären Lehre konnte für die generalklauselartigen Verarbeitungsgrundsätze

1071 Zu letzterer grundlegend und überzeugend Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), deren Analyse zu einer Qualifikation als Missbrauchsregime führt, 19 ff., 34 ff.; in diese Richtung auch Gächter/Egli, Jusletter vom 6. September 2010, N 8 ff.; dagegen taxiert die h. L., oft ohne Begründung, das Schweizer Regime als Recht der informationellen Selbstbestimmung, vgl. neben Aebi-Müller insb. Schweizer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 2 N 2; Maurer-Lambrou/Kunz, BSK-DSG, Art. 1 N 5 und N 18; vgl. m. w. H. Fasnacht, N 117 ff.

nur punktuell eine stabilisierte Lehre und Rechtsprechung entstehen, vgl. Art. 1 Abs. 3 ZGB, die ebenso für das DSG im privaten Bereich anwendbar ist. Die Grenzen zur datenschutzrechtlichen Persönlichkeitsverletzung, wie sie durch die Verarbeitungsgrundsätze resp. ihre Verletzung markiert werden, bleiben damit bis heute vage.

791 Indem nun am Anfang von Datenverarbeitungsprozessen infolge der prinzipiellen Freiheit der Datenbearbeitung in der Regel die bearbeitenden Stellen stehen, wird ihnen, soweit die strukturierende Lehre und Rechtsprechung fehlt, die Interpretationshoheit über die allgemeinen Verarbeitungsgrundsätze zugewiesen. Sie sind indes aufgrund ihrer eigenen Interessen nicht die geeigneten Personen zur «treuhänderischen» Interpretation der Bearbeitungsgrundsätze. Von ihnen zu verlangen, ihre Handlungen auf die Einhaltung rechtlicher Vorgaben hin zu überprüfen, deren Interpretation selbst den Rechtsexpertinnen und -experten schwerfällt, überzeugt nicht, zumal sich teilweise anspruchsvolle Auslegungsfragen stellen. An dieser Stelle akzentuiert sich die Kritik am generalklauselartigen Regelungsregime für den privaten Bereich, der mit einer bislang schwachen Rechtsdurchsetzung und Durchdringung in der Lehre dazu führte, dass die datenschutzgesetzlichen Vorgaben im privaten Bereich lange im Wesentlichen nur auf dem Papier galten.[1072]

792 Was die Auslegung der allgemeinen Verarbeitungsgrundsätze gemäss Art. 4 DSG resp. Art. 6 nDSG anbelangt, vereinfacht ein gewisser Wertungswiderspruch die Aufgabe nicht: Gemäss Art. 1 (n)DSG ist Zweck des Gesetzes, die Persönlichkeit zu schützen. Eine hieraus abgeleitete Auslegungsregel, wonach das DSG und dessen Generalklauseln stets zugunsten des Datensubjektes und zulasten der Datenbearbeitenden auszulegen sind, überzeugt dennoch nicht. Vielmehr scheint aufgrund der Rechtslage, wonach das DSG für den privaten Sektor den Grundsatz der freien Datenbearbeitung mit Schranken vorsieht und erst die qualifizierte Verarbeitungshandlung eine Persönlichkeitsverletzung auslöst, eine andere Folgerung angezeigt: Für die Auslegung der generalklauselartigen Verarbeitungsgrundsätze ist ihre Einbettung in das Persönlichkeitsrecht angezeigt. Demnach figuriert der Grundsatz der Freiheit der Datenbearbeitung als Prioritätsregel, die Beschränkung ist die Ausnahme.[1073]

793 An dem beschriebenen Konzept gemäss Art. 12 Abs. 2 DSG wird mit Art. 30 Abs. 2 nDSG festgehalten. Damit implementiert die Totalrevision in einem Kernpunkt ein von der DSGVO abweichendes Regime, obschon eine Annäherung an

1072 Zum Vollzugsdefizit, das ein Einhaltungs- wie Durchsetzungsdefizit umfasst, dritter Teil, VII. Kapitel, wobei mit den datenschutzrechtlichen Neuerungen, wie sie die DSGVO und die Totalrevision des DSG bringen, davon auszugehen ist, dass die datenschutzrechtlichen Vorgaben markant an Effizienz gewinnen werden; zu diesen vgl. dritter Teil, VIII. Kapitel, A.

1073 Zur Prioritätsregel Pfaffinger, ZSR 2011, 417 ff.

das Datenschutzrecht der EU erreicht werden sollte.[1074] Art. 6 DSGVO geht auch für private Stellen von einem Verarbeitungsverbot mit Erlaubnistatbeständen aus, wobei die Datenschutzkonformität der Verarbeitungshandlungen zusätzlich an die Einhaltung der Verarbeitungsgrundsätze gemäss Art. 5 DSGVO gebunden wird. Insofern lässt sich sagen, dass die DSGVO ein *zweistufiges Schrankensystem* verankert, auch im privaten Bereich. Das DSG implementiert für den privaten Bereich ein *einstufiges Modell*.

1.2. Allgemein zugänglich gemachte Personenangaben, kein Widerspruch

794 *Die zweite Gruppe von Verarbeitungshandlungen,* für die nach schweizerischem Recht ebenso wenig von einer Persönlichkeitsverletzung ausgegangen wird, ist diejenige nach Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG. Die Totalrevision hält an der Konstellation fest. Demnach wird keine Persönlichkeitsverletzung qua Personendatenverarbeitung begangen, wenn Personendaten bearbeitet werden, die von der sie betreffenden Person *allgemein zugänglich gemacht* wurden, und die Person eine Bearbeitung *nicht ausdrücklich untersagt hat*.

795 Zum ersten Tatbestandselement hält das Bundesverwaltungsgericht im Entscheid Money-House vom 18. April 2017 fest:

> «Im Übrigen bleibt festzuhalten, dass die gesetzliche Vermutung von Art. 12 Abs. 3 DSG, wonach keine Persönlichkeitsverletzung vorliegt, wenn die betroffene Person die Daten allgemein zugänglich gemacht hat, so dass eine unbestimmte Zahl von Personen sie ohne wesentliche Hindernisse in Erfahrung bringen kann, ohne die Bearbeitung ausdrücklich zu verbieten, vorliegend nicht greift. Hierfür wäre erforderlich, dass die betroffene Person ihre Daten mit Wissen und Willen allgemein zugänglich gemacht hat oder durch einen Dritten zugänglich machen liess. Blosses Dulden der Handlung eines Dritten, ohne etwas zum Zugänglichmachen beizutragen, genügt indes nicht. Weiss etwa eine Person, dass sie betreffende Personendaten allgemein zugänglich gemacht werden sollen, z. B. in Form eines Zeitungsberichts, bleibt sie aber passiv, findet Art. 12 Abs. 3 DSG keine Anwendung (Urteil des BVGer A-7040/2009 vom 30. März 2011 E. 9.3 und Rosenthal, a. a. O., Art. 12 DSG Rz 54 ff., insbesondere Rz 59). Weder betreffend die Handelsregisterdaten noch die auf anderen Plattformen wie www.local.ch publizierten Daten stellt die Beklagte nämlich auf eine Einwilligungserklärung der darin genannten Personen ab. Die strittigen Daten werden somit nicht von den betroffenen Personen selber i. S. v. Art. 12 Abs. 3 DSG wissentlich und willentlich auf der Plattform der Beklagten allgemein zugänglich gemacht. Dieser Ausschlussgrund für das Bestehen einer Persönlichkeitsverletzung kommt demnach nicht zum Tragen (vgl. mit Bezug auf die Handelsregisterdaten Urteil des BVGer A-4086/2007 vom 26. Februar 2008 E. 5.1.2). Daran ändert auch ein allfälliges, nicht wahrgenommenes Widerspruchsrecht nichts, da passives Dulden wie soeben erwähnt nicht genügt.»[1075]

1074 Botschaft 2017–1084, 1 ff., 3 ff.
1075 BVGer, A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.4.1.

Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG sind bereits theoretisch betrachtet interessant. Die Norm *fusioniert* zwei für das Recht der Privatheit und das Datenschutzrecht *traditionsreiche Paradigmen*: Kombiniert wird eine Idee der *Selbstbestimmung* mit derjenigen des sphärentheoretisch begründeten Zweikammersystems, das zwischen öffentlich und privat differenziert. 796

Die Bestimmung integriert *zum einen* unübersehbar die *Sphärentheorie* mit einem Binärcode von «öffentlich» sowie «privat» in das Datenschutzgesetz.[1076] Charakteristisch für diese ist ein zwiebelartig, statisch gedachtes Modell von konzentrischen Kreisen, die um die Person angelegt sind, deren Lebenswelt sich in eine Geheim-, eine Privat- und eine Gemeinsphäre gliedern soll.[1077] An dieser Stelle ist nicht der erste Dualismus, der öffentlich i. S. v. staatlich und privat i. S. des Bereiches zivilgesellschaftlicher Beziehungen differenziert, gemeint. Es geht um eine dichotome Strukturierung innerhalb des privaten Sektors, wobei mit der Figur der allgemein zugänglich gemachten Personendaten ein öffentlicher Bereich strukturiert wird, demgegenüber ein privater Bereich abgegrenzt wird.[1078] Damit zeigt sich das DSG als *doppelt duales Gesetz*. 797

Dieser Fingerabdruck der *Sphärentheorie im DSG* gemäss Art. 12 Abs. 3 DSG (expliziter zu finden in Art. 12 Abs. 2 lit. b DSG) und wie er selbst nach Totalrevision mit Art. 30 Abs. 3 nDSG beibehalten wird erstaunt. Denn die Erkenntnis, wonach die Sphärentheorie erhebliche Schwächen unter dem Regime moderner Verarbeitungstechnologien aufweise, trieb die Erarbeitung eines *DSG* mit einem Regelungskorpus auch für den privaten Bereich an.[1079] Die Sphärentheorie gilt seit Dezennien als untaugliches Konzept, die Herausforderungen der Informationsverarbeitungstechnologien zu bewältigen.[1080] Dasselbe gilt für eine daran anknüpfende abstrakte Kategorisierung von Personendaten als gewöhnlich oder besonders schutzwürdig. Gleichwohl hinterlässt die Sphärentheorie bis heute ihre Spuren im DSG, so in Art. 12 Abs. 3 DSG und Art. 30 Abs. 3 nDSG. 798

Zum anderen importiert Art. 12 Abs. 3 DSG die *Idee eines selbstbestimmt handelnden Datensubjektes*. Es handelt sich dabei um eine Figur, der in jüngerer Zeit das Potential zur Bewältigung der datenschutzrechtlichen Herausforderungen zugemessen wird.[1081] Nach Art. 12 Abs. 3 DSG ist es das Datensubjekt, das seine Angaben *allgemein zugänglich macht und damit des Datenschutzes quasi verlustig geht*. Den Datenschutz kann es aktivieren, indem es die Verarbeitung explizit verbietet. Folglich weist die Norm, zumindest theoretisch, eine starke Orientie- 799

1076 Vgl. zu dieser m. w. H. Aebi-Müller, N 512 ff.
1077 Vgl. m. w. H. Dies., N 512 ff.
1078 Vgl. zum ersten Dualismus und zum Privaten im Privaten erster Teil, III. Kapitel, B.
1079 Vgl. BBl 1988 II 414 ff., 418 f.
1080 Vgl. m. w. H. Aebi-Müller, N 512 ff.
1081 Kritisch hierzu Barocas/Nissenbaum, 1 ff., 4.

rung an einer *Idee der Autonomie und Selbstbestimmung des Datensubjektes* auf.[1082]

800 Nicht abschliessend geklärt scheint bezüglich Art. 12 Abs. 3 DSG die Frage, ob für den Fall eines Widerspruches, der ein Verarbeitungsverbot etabliert, eine Verarbeitung aufgrund eines übertrumpfenden anderen Rechtfertigungsgrundes, insb. eines überwiegenden Interesses, zulässig sein kann. Der Widerspruch wäre dann keine «unüberwindbare Barriere» resp. «kein letztes Wort». Vielmehr würde das überwiegende Interesse zu einer Art «Über-Generalklausel».[1083] Weil sich Art. 12 Abs. 3 DSG hierzu nicht äussert, fragt sich, ob es sich um ein qualifiziertes Schweigen oder eine Lücke handelt. Nimmt man eine Lücke an («analog» zu Art. 12 Abs. 1 lit. b DSG und der insofern herrschenden Interpretation) und lässt eine Rechtfertigung zu, wird der Wille des Datensubjektes abgeschwächt. Umgekehrt stärkt eine restriktive Zulassung überwiegender Interessen, die das Verbot des Datensubjektes überwiegen, die Selbstbestimmung.[1084]

801 Diese *zweite Gruppe der nicht persönlichkeitsverletzenden Verarbeitungshandlungen* galt lange als unproblematisch, da sie zum einen an die tradierte Denkweise anknüpft, wonach ein öffentlicher Bereich ungeschützt bleiben soll, zum anderen jener Konstellation auch ein implizites Willenselement des Datensubjektes, das seine Personendaten allgemein zugänglich gemacht hat, innewohnt. Allerdings konterkariert die besagte Regelung den Datenschutz allem voran im Online-Bereich in empfindlicher Weise.[1085] Sie wird aufgrund der Realitäten moderner Informationsverarbeitungstechnologien und damit der faktischen Entwicklungen auf den Prüfstand gestellt.

802 Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG überzeugt bereits aus Praktikabilitätserwägungen nicht: Im Lichte des in der Schweiz beliebten pragmatischen Ansatzes kann nicht davon ausgegangen werden, dass geprüft wird, ob die «allgemein zugänglichen Daten» – wie es das Gesetz verlangt – von der Person *selbst* allgemein zugänglich gemacht wurden. Ob die Einhaltung dieser Voraussetzung in der Realität erstellt wird, ist oftmals zweifelhaft.[1086] Ebenso faktisch an Grenzen stösst die Widerspruchslösung, mit welcher die vorab in den öffentlichen

1082 Insofern wird das Private nicht mit dem Gegenbegriff des Öffentlichen konstruiert, sondern mit der Autonomie verbunden. Die Relation von Privatheit und Autonomie hat namentlich Rössler herausgearbeitet, 83 ff.; vgl. auch Hotter, 29 ff.

1083 Vgl. zu den entsprechenden Termini Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien Kommentar, N 33 und N 45.

1084 Hierzu auch Radlanski, der ebenso darauf hinweist, dass bei Annahme eines Alternativverhältnisses die Datenmacht der Subjekte einschlägig zurückdividiert wird und im Ergebnis aufseiten der Subjekte eine Rechtsposition suggeriert wird – das Recht der Selbstbestimmung –, das so selbst nicht im deutschen System kompromisslos umgesetzt wird, 203.

1085 So auch Rampini, BSK-DSG, Art. 12 N 17; zu Datenverarbeitungen im Online-Bereich vgl. auch Tinnefeld/Buchner/Petri, 387 ff.

1086 Zum Vollzugsdefizit allgemein und vertiefend dritter Teil, VII. Kapitel, A.–C.

Raum entlassenen Personendaten in die Beachtlichkeit der Datenschutzbestimmung zurückverwiesen werden sollen.[1087]

Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG ist allem voran aber konzeptionell problematisch. Die Norm bleibt in einer dichotomen Kategorisierung verwurzelt. Letztere dürfte als Paradigma eines wirksamen Datenschutzrechts überholt sein. Die Bestimmung schränkt den Datenschutz empfindlich ein: Personendaten, die allgemein zugänglich gemacht wurden, gelten quasi als öffentlich und verlieren damit zumindest partiell den datenschutzrechtlichen Rahmen. Damit erstaunt auch nicht, dass von der Lehre insofern beschränkende Auslegungen präsentiert werden.[1088] Ebenso nachvollziehbar ist, dass eine mit Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG vergleichbare Bestimmung der DSGVO *fremd* ist. 803

Die Norm hat mit den Entwicklungen des Internets spezifische Brisanz erlangt. Damit drängt sich die Frage auf, ob ebenda zugänglich gemachte Personendaten nach DSG überhaupt als allgemein zugänglich gemachte Angaben taxiert werden sollen und können. Insofern Rampini: 804

> «Gedacht wurde dabei an allgemein zugänglich gemachte Daten wie die Personalien einer Person, ihre Berufsbezeichnung, Adresse, Telefonnummer usw. sowie an Daten und Meinungen, welche die Person in einer öffentlichen Veranstaltung oder in den Medien über sich selber bekannt gibt […]. Die Bestimmung hat durch die Entwicklung des Internets neue Aktualität und Brisanz erlangt. Im Internet wird – oft sorglos – eine Vielzahl von persönlichen Daten veröffentlicht […]. Einmal veröffentlicht sind die Daten jedermann und weltweit einsehbar.»[1089]

Für das Internet läuft man über Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Gefahr, das «Netz» als potentiell quasi-öffentlichen Bereich zu taxieren, womit Bearbeitungen von ebenda durch das Datensubjekt zugänglich gemachten Personenangaben vermutungshalber als nicht persönlichkeitsverletzend beurteilt werden.[1090] 805

Die Problematik der Bestimmung kann zudem über eine systematische Auslegung abgefedert werden: Von Gesetzes wegen nicht klar ist das Verhältnis von Art. 12 806

1087 Zu den Schwächen von Einwilligungs- und Widerspruchskonzeptionen im Lichte der datenschutzrechtlichen Realitäten unter Hinweis namentlich auf Radlanski vertiefend, insb. 12 ff., 210 ff.

1088 Hierzu namentlich Meier, N 1581 ff.

1089 Rampini, BSK-DSG, Art. 12 N 16 f.

1090 Bezüglich Twitter und sozialen Plattformen im Internet vgl. BGer, 5A_195/2016, 4.7.2016, E 5.3.; Bull, NVwZ 2011, 257 ff., 262; kritisch zu einer solchen Konzeption Zulauf/Sieber, AJP 2017, 548 ff., wobei die Autorinnen sowohl auf Nissenbaums Theorie zur «Privacy in Context», die Empfehlungen des Presserates sowie die Rechtsprechung des EGMR eingehen, der den Schutz einer privaten Zone auch im öffentlichen Raum verbürgt, 551 ff.; zur Lehre und Rechtsprechung mit Blick auf Fotos im Internet Fankhauser/Fischer, in: Fankhauser/Reusser/Schwander (Hrsg.), 193 ff., 195; vertiefend zu den Risiken und Herausforderungen von Social Media Coen, *passim*; illustrativ zu einer solchen Auffassung, wonach im Internet publizierte Informationen öffentlich zugänglich gemachte Informationen seien, Geiser, in: Gschwend/Hettich/Müller-Chen u. a. (Hrsg.), 373 ff., 377; vgl. für Deutschland auch Diercks, PinG 2016, 30 ff. und Göpfert/Wilke, NZA 2010, 1329 ff.

Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG und Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Bleiben die allgemeinen Verarbeitungsgrundsätze einschlägig für den Fall, dass eine Person die sie betreffenden Angaben allgemein zugänglich gemacht und keinen Widerspruch für weitere Verarbeitungen angebracht hat? Oder werden die allgemeinen Verarbeitungsgrundsätze obsolet, weil die Person ihre Daten selbst unwidersprochen «in die Allgemeinheit» entlassen hat? Mehrere Autoren vertreten hierzu zutreffenderweise, dass Art. 12 Abs. 3 DSG nicht von der Einhaltung weiterer datenschutzgesetzlicher Vorgaben, namentlich auch der allgemeinen Verarbeitungsvorgaben gemäss Art. 4 DSG resp. Art. 6 nDSG entbinde.[1091] Mit einer solchen Interpretation wird Art. 12 Abs. 3 DSG resp. Art. 30 einiges von seiner Spannungshaftigkeit, die der Artikel im Lichte der jüngsten technologischen Entwicklungen erlangt hat, genommen. Die Verarbeitung von allgemein zugänglich gemachten Personendaten ist somit im Anwendungsbereich von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG nicht frei; vielmehr müssen die allgemeinen Verarbeitungsgrundsätze i. S. v. Art. 4 DSG resp. Art. 6 nDSG als Minimalstandard berücksichtigt werden. Im Ergebnis führt die Ansicht, wonach die allgemeinen Verarbeitungsgrundsätze weiterhin beachtlich sind, zu einer weitgehenden Korrektur von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG. Mit Fug und Recht fragt sich sodann, inwiefern der Bestimmung noch ein eigenständiger Bereich verbleibt.

807 An dieser Stelle ist die Linse zu öffnen und Art. 12 Abs. 3 DSG systematischer innerhalb einer erweiterten Landschaft zu reflektieren: Allem voran die Analyse zum Zweckbindungsgrundsatz hat ergeben, dass sowohl die *Basierung datenschutzrechtlicher Normierung in einem Dualismus von öffentlich versus privat* als auch die *Beschränkung des Datenschutzrechts auf den Subjektschutz* zu kurz greift. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG führt dazu, dass der private Bereich einer dualistischen und stark sphärentheoretisch orientierten Sichtweise verhaftet bleibt. Als Resultat wird der Datenschutz gegenüber öffentlich resp. allgemein zugänglich gemachten Angaben herabgesenkt.[1092] Zugleich stellt die Bestimmung in zentraler Weise auf den Willen des Subjektes ab, das einerseits seine Angaben «allgemein zugänglich gemacht hat» und andererseits einer Verarbeitung (nicht) widersprochen hat. Im Laufe dieser Studie wurde an mehreren Stellen herausgearbeitet, dass die *datenschutzrechtlichen Herausforderungen mehrdimensional sind*. Das Datenschutzrecht hat über den *Subjektschutz hinaus*, so eine Schlussfolgerung nach einer Analyse des Volkszählungsurteils des Bundesverfassungsgerichts, die Funktion zu erfüllen, die *Integrität spezifischer resp. pluraler Verarbeitungszusammenhänge*, *Bereiche resp. Systeme zu schützen*.

1091 So Rosenthal, HK-DSG, Art. 12 N 53; vgl. weiter Baeriswyl, digma 2009, 99; Meier, N 1577.

1092 Ein Teil der Lehre stellt sich gegen eine solche Lockerung, indem für die Anwendbarkeit und Beachtlichkeit der allgemeinen Verarbeitungsgrundsätze plädiert wird.

Vor diesem Hintergrund greift es zu kurz, das Internet als monolithischen öffentlichen Bereich zu qualifizieren, wobei Datensubjekte mit der Nutzung quasi ihre Einwilligung für (weitgehend unbeschränkte) weitere Verarbeitungshandlungen geben. Ein solches Konzept ist aus einer Datenschutzperspektive *nicht tragfähig*. Im Ergebnis scheinen genau dies auch die Ansichten zu adressieren, die dafür eintreten, dass Art. 12 Abs. 3 DSG nicht von der Einhaltung der allgemeinen Datenschutzvorgaben dispensiert. 808

Für das Internet generiert die unter Treu und Glauben erläuterte Doktrin der «*reasonable expectations of privacy*» Erkenntnisse.[1093] Sie lassen sich zu einer Hypothese verdichten, wonach im Internet und z. B. auf Facebook mit Freunden und Verwandten *zwecks* Beziehungspflege ausgetauschte Angaben *nur zu diesem Zweck geteilt werden*. Ebendies dürfte mit einer vernünftigen Erwartung verbunden sein, wonach diese *Informationen aus dem persönlichen Lebensbereich nicht für einen anderen gesellschaftlichen oder staatlichen Bereich genutzt, beispielsweise nicht für und im privaten oder öffentlichen Arbeitskontext* ausgewertet werden.[1094] Im Ergebnis ist Rampini beizupflichten, der dafür plädiert, dass weitere Personendatenverarbeitungen von im Internet veröffentlichten Personenangaben nur dann nicht persönlichkeitsverletzend sind, wenn sich diese «im Rahmen des aus den Umständen ersichtlichen Verarbeitungszwecks» bewegen.[1095] 809

1.3. Resümee

Für das DSG sind *zwei Hauptkonstellationen* hervorzuheben, in denen die Tatbestandsmässigkeit der Persönlichkeitsverletzung grundsätzlich nicht angenommen wird. Anders gewendet: Das DSG beurteilt die fraglichen Arten von Personendatenverarbeitungen als nicht dergestalt qualifiziert, dass sie die Intensität einer Persönlichkeitsverletzung erreichen würden. Keine Persönlichkeitsverletzung liegt nach Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG grundsätzlich vor, wenn die Verarbeitungshandlung in Einklang mit den allgemeinen Verarbeitungsgrundsätzen steht. Keine Persönlichkeitsverletzung soll zudem vorliegen, wenn gemäss Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Personendaten vom Da- 810

1093 Vgl. hierzu zweiter Teil, V. Kapitel, B.2.3.

1094 Dazu, dass auf Social Network Sites geteilte Angaben «freiwillig einer breiten Öffentlichkeit präsentiert werden» EDÖB, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/onlinedienste/soziale-medien/erlaeuterungen-zu-sozialen-netzwerken.html> (zuletzt besucht am 30. April 2021); anders dagegen OGH-Beschluss vom 30. März 2016, 6 Ob 14/16a – Manipuliertes Facebook-Foto/Strandfoto, wonach das Veröffentlichen von (Personen-)Bildnissen in sozialen Netzwerken wie Facebook regelmässig nur eine bestimmte, vom Betroffenen gewünschte Öffentlichkeit bewirke; zum Thema Datenschutz und Facebook auch Buchner, DuD 2015, 402 ff.; vgl. in diesem Zusammenhang auch Rudin, digma 2010, 48 f.; beachte insofern auch EGMR Nr. 61496/08 – Bârbulescu/Romania, Urteil vom 12. Januar 2016; allgemein zum Recht am eigenen Bild auch BGE 127 III 481; BGE 129 III 715; BGE 138 II 346.

1095 Rampini, BSK-DSG, Art. 12 N 18.

tensubjekt allgemein zugänglich gemacht wurden und dieses einer Verarbeitung nicht widersprochen hat.

811 Beide Konstellationen von Personendatenverarbeitungen, die von Gesetzes wegen als *nicht* persönlichkeitsverletzend taxiert werden, speisen *verschiedene datenschutzrechtliche Konzepte in das DSG ein*.[1096] Mit der Totalrevision wird an diesen festgehalten.

812 Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG lehnt konsequent am Regelungskonzept gemäss Art. 28 ZGB an: Das Regime wird, da es erst *qualifizierte Verarbeitungshandlungen* als persönlichkeitsverletzend beurteilt, als *Integritätsschutz* charakterisiert. Gleichermassen akkurat dürfte eine *Chiffrierung als Missbrauchsgesetzgebung* sein. Die Regelungsmechanik verzichtet auf eine Kategorisierung von öffentlich versus privat und formuliert Vorgaben, die auf den *fairen, redlichen Umgang mit Personendaten abzielen*. Es sind die grossen Verarbeitungsgrundsätze, die als Minimalstandard einzuhalten sind und mit deren Einhaltung die Persönlichkeit der Datensubjekte nicht verletzt wird. Die Verarbeitenden stehen in der Pflicht, diese Regelkonformität sicherzustellen. Mit der Totalrevision wird die *proaktive Rechtseinhaltung durch mehrere Umsetzungsinstrumente akzentuiert. Damit rückt die defensivrechtliche und retrospektive Perspektive, wie sie dem Persönlichkeitsschutz eigen ist, von Gesetzes wegen in den Hintergrund*. Zugleich wird gegenüber der Sphärentheorie ein Perspektivenwechsel vollzogen. Der Fokus liegt auf den Verarbeitenden und der Gewährleistung von Prozessen, die einen Katalog an Mindestanforderungen, ausgedrückt mit den Verarbeitungsgrundsätzen, zu achten haben.

813 Demgegenüber steht Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG konzeptionell in einem Kontrast zu dem beschriebenen prozesshaft gedachten Integritätsschutz. Die Regelung beruht auf einem sphärentheoretisch begründeten dualen wie subjektverhafteten Konzept. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG trägt mit der als untauglich geltenden Kategorisierung von «öffentlich» und «privat» einen Ansatz in das DSG, der in empfindlicher Weise dessen Schutz preisgibt. Insofern ist eine Auslegung, wonach sämtliche im Internet vom Datensubjekt zugänglich gemachten Personendaten als allgemein zugänglich gemacht resp. öffentlich gelten und damit vom Datenschutz exkludiert werden, kritisch. Entsprechend wurden korrigierende Interpretationen vorgeschlagen, wonach selbst im Anwendungsbereich von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG kein Dispens von der Einhaltung der allgemeinen Datenschutzvorgaben gilt. Die DSGVO kennt keine vergleichbare Regelung. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG wird uns an späterer Stelle nochmals beschäftigen, wo gezeigt werden

1096 Zum einen diejenigen, welche die allgemeinen Verarbeitungsgrundsätze einhalten, zum anderen die Verarbeitung von allgemein zugänglich gemachten Personendaten bei fehlendem Widerspruch.

wird, weshalb das Internet gerade *nicht als einheitlicher öffentlicher Bereich* taxiert werden sollte.

Zusammenfassend vereinigt das DSG bei der Definition von Personendatenbearbeitungen, bei denen die Grenze zur Persönlichkeitsverletzung *nicht* überschritten wird, *verschiedene Regelungsmechaniken*. Nach ihrer Betrachtung ist auf die eingangs zitierten Umschreibungen zurückzukommen. Meinungen, wonach jede Personendatenverarbeitung eine Persönlichkeitsverletzung begründe, wonach das Datensubjekt ein «Herrschaftsrecht» über seine Personendaten habe, wonach Personendatenverarbeitungen stets der Einwilligung des Datensubjektes bedürften oder wonach jedermann grundsätzlich selbst über die Verwendung «seiner» Personendaten befinden könne, haben im DSG *keine* Grundlage. Diese Klarstellung ist relevant, zumal andernfalls selbst gegenüber der Allgemeinheit ein Rechtsbestand suggeriert wird, der nach DSG nicht verbürgt wird.[1097] Eine unmittelbare Folge sind enttäuschte Erwartungen, was für ein Rechtsgebiet, das in besonderer Weise auf die Kategorie des Vertrauens angewiesen ist,[1098] besonders schwer wiegt. 814

2. Persönlichkeitsverletzende Verarbeitungen nach DSG

2.1. Vorbemerkungen

Die vorangehende Darstellung der *nicht* persönlichkeitsverletzenden Verarbeitungen befasste sich *indirekt resp. e contrario* zugleich mit den persönlichkeitsverletzenden Handlungen. Es ging um deren Abgrenzung und den entsprechenden Grenzverlauf. Daraus resultieren folglich teilweise Redundanzen. Sie werden zugunsten der Klärung vor dem Hintergrund der facettenreichen Umschreibungen zur Funktionsweise des DSG im privaten Bereich in Kauf genommen. 815

Persönlichkeitsverletzende Personendatenverarbeitungen sind insb. in Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG niedergelegt. In den lit. a–c werden nicht abschliessend die Tatbestände der Persönlichkeitsverletzung konkretisierend umschrieben. 816

Mit der Totalrevision werden Struktur und Inhalt von Art. 12 f. DSG weitgehend übernommen, vgl. Art. 30 f. nDSG. Insofern ist immerhin auf zweierlei hinzuweisen: Der erste Hinweis gilt einer *Bereinigung*. Neu wird die Rechtfertigungsmöglichkeit konsequent aus den Umschreibungen der persönlichkeitsverletzenden 817

1097 Zutreffend Rudin, BJM 1998, 113 ff., 115, der es als unglücklich bezeichnet, dass die Schweizer Lehre auf das Recht auf informationelle Selbstbestimmung i. S. des Volkszählungsurteils und i. S. eines Kontrollrechts referiert.

1098 Hierzu bereits zweiter Teil, V. Kapitel, B.2.; Druey, Rechtswissenschaftliche Abteilung der Universität St. Gallen (Hrsg.), 525 ff.

Tatbestände ausgegliedert. Die Totalrevision führt somit nach, was unter bisherigem DSG zur herrschenden Lehre und Rechtsprechung geworden war. Bot der noch in Kraft stehende Gesetzestext vorab Anlass zu Unsicherheiten, konsolidierte sich eine Auslegung, wonach entgegen der uneinheitlichen Integration von Rechtfertigungsgründen in den drei Literae solche stets zuzulassen sind.[1099] Die zweite Neuerung ist materieller Natur, indem bislang an den Begriff der Bearbeitung von «Persönlichkeitsprofilen» geknüpfte Vorgaben im Rahmen des Themas Profiling einer eigenständigen und anderen Normierung zugeführt werden.

818 Zur Persönlichkeitsverletzung nach DSG vor seiner Totalrevision prägnant Rampini:

> «Wann eine Persönlichkeitsverletzung vorliegt, d. h. wann die Datenbearbeitung die Persönlichkeit der Betroffenen verletzt, wird durch Art. 12 Abs. 2 und Abs. 3 DSG konkretisiert (vgl. die Marginalie), einerseits positiv (Abs. 2), andererseits negativ (Abs. 3). Diese Konkretisierung bleibt notwendigerweise vage.»[1100]

819 Ungeachtet dieser «Vagheit» scheint in einem Punkt Konsens zu bestehen: Der Massstab für die Beurteilung, ob ein Verstoss gegen eine Bearbeitungspflicht nach Art. 12 Abs. 2 lit. a–c DSG eine Persönlichkeitsverletzung begründe, sei ein *objektiver*.[1101] Das subjektive Empfinden der Datensubjekte oder Verantwortlichen sei nicht relevant.

820 Dies vorausgeschickt werden nun die Hauptkonstellationen der Persönlichkeitsverletzung, wie sie der Gesetzgeber nicht abschliessend in Art. 12 Abs. 2 lit. a–c DSG resp. Art. 30 Abs. 2 lit. a–c nDSG aufführt, beleuchtet.

2.2. Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG en détail

821 Innerhalb des Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG werden in den lit. a–c (nicht abschliessend, vgl. den Ingress «insbesondere») drei Tatbestände persönlichkeitsverletzender Personendatenverarbeitung definiert. Die beiden Konstellationen von lit. a und lit. c haben primär einen objektiven Charakter, lit. b hat eher subjektive Qualität.

Lit. a widmet sich den *allgemeinen Verarbeitungsgrundsätzen*, deren Nichteinhaltung als Persönlichkeitsverletzung gilt. Insofern ist auf das V. Kapitel dieses zweiten Teils hinzuweisen.

Lit. b gewährleistet ein *Widerspruchsrecht* des Datensubjektes.

1099 BGE 136 II 205; Auslegungshilfe des BJ; vgl. Rampini, BSK-DSG, Art. 12 DSG N 9b.
1100 Rampini, BSK-DSG, Art. 12 N 3.
1101 Rosenthal, HK-DSG, Art. 4 N 3 und Art. 12 N 3 ff.; Haas, N 68; vgl. Meili, BSK-ZGB, Art. 28 ZGB N 42; Rampini, BSK-DSG, Art. 12 DSG N 6.

Lit. c widmet sich einer spezifischen Bearbeitungshandlung, der *Weitergabe* von «qualifizierten Datenbeständen», insb. von *besonders schützenswerten Personendaten und Persönlichkeitsprofilen an Dritte*.

822 Die vom DSG umschriebenen persönlichkeitsverletzenden Verarbeitungshandlungen kombinieren und fusionieren – wie zu zeigen sein wird – in sich in eindrücklicher Weise unterschiedliche Stossrichtungen und Ansätze: ein Konzept des *Integritätsschutzes*, einen *Autonomieansatz* sowie die *Idee der Sphärentheorie*.[1102]

823 Vorauszuschicken ist: Art. 12 Abs. 2 lit. a DSG lässt sich als «Auffangtatbestand» in dem Sinne bezeichnen, dass er stets dann greift, wenn kein Widerspruch vorliegt oder wenn keine besonders schutzwürdigen Personendaten resp. Persönlichkeitsprofile an Dritte weitergegeben werden. Da es bei den letzteren beiden Konstellationen um spezifische Konstellationen geht, greift über weite Strecken das Regime von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Insofern lässt sich der Absatz – *auch wenn er gewissermassen eine Auffangordnung bildet – als die Grundsatzordnung qualifizieren*. Folglich dürfte die Funktionsweise von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG für eine Qualifizierung des DSG im privaten Bereich im Vordergrund stehen. Der überwiegende Teil der Personendatenverarbeitungen im privaten Bereich wird von den materiellrechtlichen Vorgaben, wie sie Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG formuliert, datenschutzgesetzlich strukturiert.

2.2.1. lit. a – Regime des Integritätsschutzes

824 Hinsichtlich Art. 12 Abs. 1 lit. a DSG stand lange eine Frage im Zentrum der Überlegungen: Handelt es sich bei der Nichterwähnung möglicher Rechtfertigungsgründe um einen Lapsus des Gesetzgebers oder um eine Stärkung des Datenschutzes? Insofern etablierte sich im Anschluss an eine Stellungnahme vonseiten des Bundesamtes für Justiz eine herrschende Lehre und Praxis: Rechtfertigungsgründe sind prinzipiell zuzulassen, allerdings mit Zurückhaltung.[1103] Die Totalrevision bringt mit Art. 30 Abs. 1 lit. a nDSG eine entsprechende Bereinigung.

825 Zur *konzeptionellen Tragweite der Bestimmung*: In einem System der prinzipiellen Verarbeitungsfreiheit, wie es die Schweiz im DSG für den privaten Bereich vorsieht, kommt der *Schrankendefinierung vorrangige Bedeutung* zu. In Bezug auf diese Schranken stehen gemäss Art. 12 Abs. 2 lit. a DSG die allgemeinen Ver-

1102 Letztere sollte mit dem DSG bekanntermassen überwunden werden, vgl. insofern BBl 1988 II 414 ff., 420 f.; Aebi-Müller, m. w. H., N 512 ff.

1103 Vgl. BGE 136 II 508, Regeste und E 5; entsprechend auch EDÖB, Schlussbericht PostFinance, 6, 23.

arbeitungsgrundsätze, vgl. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG, an erster Stelle. Die Totalrevision verweist in Art. 30 Abs. 2 lit. a nDSG auf Art. 6 und Art. 8 nDSG.

826 In beiden Fassungen sind es erst und nur *qualifizierte Personendatenverarbeitungen*, welche die Schranken einer prinzipiell freien Verarbeitung durchbrechen und eine Persönlichkeitsverletzung begründen. An dieser Stelle liegen die Schranken der allgemeinen Verarbeitungsfreiheit in einer Missachtung der materiellrechtlichen Datenschutzvorgaben, der *allgemeinen, weitgehend generalklauselartigen Verarbeitungsgrundsätze*. Sie markieren prinzipiell die Persönlichkeitsverletzung.

827 Die Schweiz regelt im DSG für den privaten Bereich die datenschutzrechtlichen Vorgaben mit einem *einstufigen Schrankenmodell*. Ebendies gilt auch nach Totalrevision. Anders definiert die DSGVO sowohl für den öffentlichen als auch für den privaten Bereich ein *zweistufiges Schrankenmodell*. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG weist damit zunächst eine *materiellrechtliche Schrankenfunktion* auf.

828 Zusätzlich haben Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG eine *Verweisungs- und Koppelungsfunktion*. Die Bestimmung referiert vorab auf die wichtigsten Grenzen der prinzipiellen Verarbeitungsfreiheit, die allgemeinen Verarbeitungsgrundsätze, vgl. insb. Art. 4 DSG und Art. 6 nDSG. Die Verletzung der allgemeinen Verarbeitungsgrundsätze wird an die zivilrechtliche Persönlichkeitsverletzung angekoppelt.

829 Schranken der grundsätzlich freien Verarbeitung resp. persönlichkeitsverletzende Handlungen im privaten Bereich finden sich damit materiellrechtlich in erster Linie *innerhalb* des DSG. Art. 12 Abs. 1 lit. a DSG besagt, dass «insbesondere» die Verletzung bestimmter allgemeiner Verarbeitungsgrundsätze eine Persönlichkeitsverletzung begründe, wobei auf die Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG verwiesen wird. Art. 30 Abs. 2 lit. a nDSG verweist auf Art. 6 und Art. 8 nDSG. Nach DSG sind es die allgemeinen, teilweise generalklauselartigen *Bearbeitungsvorgaben*, die als zweites Strukturmerkmal in diesem zweiten Teil dargestellt wurden, die den *Grenzverlauf zwischen nicht persönlichkeitsverletzender und persönlichkeitsverletzender Personendatenverarbeitung markieren*. Allerdings handelt es sich hierbei, wie das Wort «insbesondere» deutlich macht, um keine abschliessende Ordnung.

830 Art. 12 Abs. 2 lit. a DSG wird als *«Fiktion»*[1104] resp. *«unwiderlegbare Vermutung»*[1105] qualifiziert. Beide Rechtsfiguren, so wird es vertreten, dienen der Über-

1104 So Steinauer, in: Schweizer (Hrsg.), 43 ff., 45.
1105 So Peter, 125.

brückung faktischer Ungewissheit.[1106] Die Qualifizierung liegt wohl in der Vorstellung begründet, wonach quasi «naturgegeben» bestimmte (Verarbeitungs-)Handlungen persönlichkeitsverletzend sein sollen. Der Gesetzgeber hat diese als «naturgegebenes Faktum» freizulegen und abzubilden. Allerdings erschöpft sich die Funktion von Vermutung resp. Fiktion nicht in einem solchen Element. Vielmehr dienen sie dem Gesetzgeber regelmässig als *Qualifikations- und Definitionsinstrument.* Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG, mit welchem der Datenschutzgesetzgeber die Verletzung der allgemeinen Verarbeitungsgrundsätze explizit als Persönlichkeitsverletzung taxiert, hat weniger zum Ziel, faktische Ungewissheit zu überwinden. Vielmehr handelt es sich bei Art. 12 Abs. 1 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG um eine gesetzgeberische Konkretisierung einer Generalklausel, hier der Persönlichkeit und deren Verletzung durch Personendatenverarbeitungen.[1107] Folglich überzeugt die Qualifizierung der Konstruktion im Sinne einer beweisrechtlichen Figur nur teilweise. In erster Linie handelt es sich bei der Gesetzgebung um die generell-abstrakte Konkretisierung eines Rechtsbegriffes, hier der Persönlichkeit.

Der Beweis der *Persönlichkeitsverletzung* und insofern Nichteinhaltung der Ver- 831
arbeitungsgrundsätze durch die Verantwortlichen obliegt gemäss der Regel von Art. 8 ZGB dem Datensubjekt. In der heutigen datenschutzrechtlichen Realität ist ein solcher Beweis indes kaum führbar. Und selbst wenn einem Datensubjekt der Beweis gelingt, dass die allgemeinen Verarbeitungsgrundsätze durch eine Bearbeitungshandlung verletzt wurden, erscheint dies in Anbetracht der Bedeutung von Personendatenverarbeitungen in der heutigen Zeit als Tropfen auf den heissen Stein, der in keiner Weise geeignet ist, das Datenschutzrecht und dessen Einhaltung zu effektuieren.[1108]

Im noch in Kraft stehenden DSG bildet den Kern(tat)bestand der Persönlichkeits- 832
verletzung qua Personendatenverarbeitung die Verletzung der weitgehend *generalklauselartigen, gemeinsamen resp. allgemeinen Verarbeitungsgrundsätze*, Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG, vgl. Art. 30 Abs. 2 lit. a nDSG.

Allerdings wurde an früherer Stelle gezeigt, dass sich ihre konturierende und 833
beschränkende Wirkung faktisch wie theoretisch nur teilweise zu entfalten vermochte. Der Befund wird im dritten Teil unter dem Titel des *Vollzugsdefizites*

1106 Schulbeispiel insofern ist die Vaterschaftsvermutung resp. -fiktion. Vermutungen figurieren auf der Stufe des Beweises und beziehen sich auf strittige Tatsachen; vgl. hierzu die einschlägige Kommentarliteratur.

1107 Indem das Datenschutzrecht am Persönlichkeitsrecht anknüpft, trägt auch diese Anknüpfung den generalklauselartigen Charakter in das Datenschutzrecht; zum Persönlichkeitsrecht mit seiner generalklauselartigen Unbestimmtheit Ehmann, Juristische Schulung, Zeitschrift für Studium und praktische Ausbildung 1997, 193 ff., 193; zur Notwendigkeit von klaren und konsistenten Datenschutzvorgaben Solove, Stan. L. Rev. 2001, 1393 ff., 1461.

1108 Betreffend Vollzugsdefizit dritter Teil, VII. Kapitel.

vertieft. Ursächlich für das sog. Vollzugsdefizit ist auch die generalklauselartige Regelung, angeknüpft an den Grundsatz der Freiheit der Datenbearbeitung.[1109] Neben dieser materiellrechtlichen Problematisierung ist weiter die prozessrechtliche Situation mitverantwortlich dafür, dass das DSG weitgehend ein «Papiertiger» blieb:[1110] Personendatenverarbeitungen werden noch heute selten auf ihre Rechtmässigkeit hin überprüft, da Persönlichkeitsverletzungen kaum je von den Datensubjekten geltend gemacht werden.[1111] Zugleich hat der EDÖB – die Funktionen von Datenschutzbeauftragten wurden von der Gesetzgebung gerade auch als Instrument der Kompensation für ein generalklauselartiges Regelungsregime vorgesehen – nur beschränkte Kompetenzen (die immerhin mit der Totalrevision erweitert werden). Hinzu tritt die über lange Zeit eher schwache wissenschaftliche Durchdringung des DSG namentlich für den privaten Bereich. Eine Folge hiervon ist, dass die so wichtige Konkretisierung der allgemeinen Verarbeitungsgrundsätze als Schranke der grundsätzlich freien Personendatenverarbeitung durch Lehre und Praxis erst ansatzweise bewerkstelligt ist.[1112] Immerhin: Mit der Totalrevision dürfte die eine oder andere Schwäche durch die Schaffung neuer Umsetzungsinstrumente sowie der verschärften Instrumente zur Rechtsdurchsetzung abgemildert werden.

834 Gemäss Art. 12 Abs. 2 lit. a DSG Ingress begründen nicht nur Verstösse gegen die Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG eine «Persönlichkeitsverletzung»; vielmehr ist die Aufführung aufgrund der Wendung «insbesondere» nicht abschliessend. Dieselbe Regelung findet sich in Art. 30 nDSG. Damit kommt der Frage, welche weiteren Verstösse gegen datenschutzrechtliche Vorgaben eine Persönlichkeitsverletzung begründen, zumindest theoretisch betrachtet nicht unwesentliche Bedeutung zu.

835 Welche weiteren Verstösse gegen Vorgaben des DSG als Persönlichkeitsverletzung zu qualifizieren sind, ist nicht abschliessend geklärt. Die Problematik soll anhand von Art. 6 DSG nachgezeichnet werden. Die Bestimmung befasst sich mit den Voraussetzungen des rechtmässigen Transfers von Personendaten ins Ausland.[1113]

1109 Zum hohen Preis der Ansammlung von Generalklauseln im Datenschutzgesetz Simitis, Nomos-Komm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien Kommentar, N 20; zur schwachen Effektivität des Datenschutzrechts Ders., Symposium, 1 ff., 1.

1110 Vgl. Huber, recht 2006, 205 ff.; Drechsler, AJP 2007, 1471 ff.; beispielhaft auch Gogniat, Jusletter vom 20. Juni 2016, N 3, wonach im Rahmen von Personendatenverarbeitungen zahlreiche Persönlichkeitsverletzungen stattfinden; vgl. auch Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.1.

1111 Vgl. dritter Teil, VII. Kapitel, A.2.

1112 Hierzu zweiter Teil, V. Kapitel.

1113 Zur Rechtsanwendung bei internationaler Datenbearbeitung durch Private grundlegend Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.10; vgl. zu den jüngsten verschärfenden Entwicklungen im Zusammenhang mit dem Transfer von Personendaten in die USA <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-80318.html> (zuletzt besucht am 3. Juni 2021).

Die Totalrevision baut insofern die Vorgaben aus, vgl. Art. 16 ff. nDSG und insb. Art. 61 lit. a nDSG, wo eine strafrechtliche Sanktionierung verankert wird.

Art. 6 DSG fehlt in der Aufzählung von Art. 12 Abs. 2 lit. a DSG. Auch die Totalrevision nimmt Verletzungen der Pflichten im Zusammenhang mit dem Auslandstransfer nicht explizit in den Katalog der Persönlichkeitsverletzung auf. Die fehlende ausdrückliche Qualifizierung von Verstössen gegen die entsprechenden Vorgaben als Persönlichkeitsverletzung ist in Anbetracht der Tatsache, dass Personendaten heute kaum mehr lokal innerhalb der Ländergrenzen verarbeitet werden und das Schlagwort der Globalisierung Hand in Hand mit jenen der Digitalisierung und der Informationsgesellschaft geht, bemerkenswert.[1114] Dass Daten isoliert lokal bearbeitet werden, wird zur Ausnahme; in der Regel agieren diverse Verarbeiter als Verantwortliche und Auftragsverarbeitende in einer Art Netzwerkstruktur über Landesgrenzen, ja die Grenze des Erdballes hinweg.[1115] 836

Art. 6 DSG definiert Vorgaben an den Datentransfer ins Ausland, wobei ein spezifisches Instrumentarium zum Schutz der Datenbearbeitungs*pflichten* beim Transfer ins Ausland und der Überprüfung ihrer Einhaltung vorgesehen wird. Zudem greifen die strafrechtlichen Sanktionsmöglichkeiten nach Art. 34 DSG bei einem Verstoss gegen die Meldepflicht. 837

Spricht dieses besondere Schutzinstrumentarium dafür, dass der individualrechtliche Rechtsschutz qua Persönlichkeitsrecht ausgeschlossen wird? 838

Passadelis scheint für eine solche Interpretation einzutreten, indem er die Bestimmung von Art. 6 DSG (vgl. Art. 16 ff. nDSG) als *öffentlich-rechtliche Norm* qualifiziert. Der Rechtsweg wäre daran anknüpfend nicht derjenige über das Zivilgericht. Anders dagegen wohl Maurer-Lambrou/Steiner mit den Worten: 839

> «[…] [D]as Fehlen einer Datenschutzgesetzgebung, welche einen angemessenen Schutz gewährleistet, gilt gesetzlich als eine schwerwiegende Persönlichkeitsverletzung (Art. 6 Abs. 1 DSG).»[1116]

Wertungsmässig scheint m. E. die Gravität der Verletzungen der Vorgaben über den Auslandstransfer äquivalent zu den Verletzungshandlungen nach Art. 4, Art. 5 und Art. 7 DSG zu sein, womit ohne Weiteres auf eine Persönlichkeitsverletzung zu schliessen wäre. Diese Ansicht vertritt nach meinem Verständnis ebenso Rampini.[1117] Um die weiteren, nicht explizit enumerierten persönlichkeitsverletzenden Handlungen als Persönlichkeitsverletzung zu taxieren, dürfte neben der 840

1114 Illustrativ insofern Hoffmann-Riem, AöR 1998, 513 ff., 533 f.
1115 Ders., a. a. O., Rz 6.1 f.; die DSGVO anerkennt die «Grenzenlosigkeit» von Personendaten nicht zuletzt durch ihr vereinheitlichendes Regime wie den extraterritorialen Anwendungsbereich, vgl. Art. 3 DSGVO; vgl. zur sog. Deterritorialisierung als eine Aporie des Informationsrechts Hoeren, 20 f.
1116 Maurer-Lambrou/Steiner, BSK-DSG, Art. 6 N 11.
1117 Rampini, BSK-DSG, Art. 12 N 9a.

Frage nach der qualitativen Äquivalenz namentlich eine *funktionelle Betrachtung* resp. eine Fokussierung auf die Auswirkung einschlägig sein. Im Zuge der jüngsten Revisionswelle, aber auch den jüngsten Entwicklungen zu den Privacy Shields aufgrund der erfolgreichen Initiativen des Datenschutzaktivisten Max Schrems gewinnen internationale Datentransfers und die damit einhergehenden datenschutzrechtlichen Risiken markant an Bedeutung.[1118] Mit dem Transfer von Personendaten in ein «unsicheres Drittland» kann der Datenschutz weitgehend unterlaufen werden. Aufgrund dieser Auswirkungen dürfte ausser Frage stehen, dass die Verletzung der Vorgaben im Zusammenhang mit dem Auslandstransfer eine Persönlichkeitsverletzung begründet. Anders dagegen dürfte namentlich die Verletzung von neuen Datenschutzpflichten, die eine (interne) Hilfsfunktion haben, so das Bearbeitungsverzeichnis oder die Dokumentationspflicht, nicht direkt zur Annahme einer Persönlichkeitsverletzung führen.

841 Die Frage, welche Pflichtverstösse, die nicht explizit zu den enumerierten Bearbeitungsgrundsätzen nach Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. nDSG gehören, als persönlichkeitsverletzend zu gelten haben, ist im Übrigen weitgehend ungeklärt und soll an dieser Stelle auch keiner umfassenden Klärung zugeführt werden.[1119]

842 Es handelt sich indes – wegen der nicht griffigen Rechtsdurchsetzung – um eine weitgehend theoretische Frage. Je grosszügiger Verstösse gegen das DSG als Persönlichkeitsverletzung qualifiziert werden, desto stärker wird – theoretisch und formell betrachtet – die individualrechtliche Position der Datensubjekte ausgestaltet. Weil allerdings Persönlichkeitsverletzungen infolge Personendatenverarbeitung kaum je von den Individuen moniert werden, ist mit der grosszügigen Inklusion von Datenschutzverstössen in die Persönlichkeitsverletzung nicht viel für die Wirksamkeit des DSG gewonnen. Selbst eine *grosszügige Inklusion* von Verstössen gegen Verarbeitungsvorgaben im DSG in die Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG führt *faktisch nicht zu einer nennenswerten Effektuierung des Datenschutzgesetzes* im privaten Bereich.

843 Damit präsentiert sich ein paradoxer Befund: Ein Regime, das auf den Schutz der Persönlichkeit abzielt, erfährt keine merkliche Stärkung durch eine grosszügige Auslegung und Ausweitung der nicht abschliessend aufgeführten persönlichkeitsverletzenden Tatbestände gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Im Gegenteil – das Gesetz schafft weitere Unsicherheiten über dieje-

1118 Vgl. insofern <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-80318.html> (zuletzt besucht am 20. September 2021).

1119 Fraglich insb. betr. die Meldepflicht gemäss Art. 6 DSG, die Informationspflicht gemäss Art. 14 DSG, die Einhaltung der Vorgaben nach Art. 8, Art. 10a, Art. 11a Abs. 3 oder Art. 35 DSG; m. w. H. Rosenthal, HK-DSG, Art. 4 N 2 sowie Art. 12 N 3 und N 14.

nigen hinausgehend, die das generalklauselartige Regime ohnehin in ein Regime hineinträgt.

Als Kernbefund für Art. 12 Abs. 2 lit. a DSG – und damit als Kernbefund für das DSG im privaten Bereich selbst – ist festzuhalten: Innerhalb des DSG haben datenverarbeitende Stellen im privaten Bereich die allgemeinen Verarbeitungsgrundsätze namentlich gemäss Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG zu beachten, um *keine* Persönlichkeitsverletzung mittels ihrer Datenverarbeitungshandlungen zu begehen, vgl. Art. 12 Abs. 1 lit. a DSG. Bei Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG handelt es sich um die Implementierung eines *Integritätsschutzes* – ebendies erscheint als die treffende Bezeichnung des Regimes. Nicht jede Personendatenverarbeitung ist gemäss dem schweizerischen Querschnittsgesetz persönlichkeitsverletzend, vielmehr ist es erst die *qualifizierte Verarbeitung*, die als Persönlichkeitsverletzung gilt. Die Demarkationslinie wird von den allgemeinen Verarbeitungsgrundsätzen und deren Verletzung gezogen. Sie bilden die Schranken der freien, sprich unterhalb der Persönlichkeitsverletzung liegenden Datenverarbeitung. An dieser Konzeption hält die Totalrevision mit Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG weitgehend fest. 844

Die allgemeinen Verarbeitungsgrundsätze – im privaten Sektor eingebettet in den Persönlichkeitsschutz – sollen *faire und angemessene Verarbeitungsprozesse sowie Datenflüsse gewährleisten*.[1120] Damit geht es im *privaten Bereich*, mangels abweichender Vorgaben durch spezifische Regelungen, auch um eine Art der Sicherstellung der *Lauterkeit im Umgang* mit Personendaten, die Verhinderung übermässiger Personendatenverarbeitungsprozesse, die Gewährleistung allgemeinster Grundsätze der Redlichkeit oder auch Fairness im Umgang mit Personenangaben. 845

Folglich ist der für das Informations- und Datenschutzrecht so enge Bezug zum Vertrauen, zu Art. 2 ZGB, aber auch zum Wortlaut von Art. 13 Abs. 2 BV mit seinem Gegenbegriff hergestellt. Diese als allgemeines Regime greifende Konzeption der Vorgaben bei Personendatenverarbeitungen im *privaten Bereich* lässt nun wiederum – trotz der Ankoppelung an die subjektivrechtliche Persönlichkeitsverletzung – ebenso für individualrechtlich geschulte Juristinnen und Juristen die Strukturierung eines gesellschaftlichen Bereichs, eines *privaten Lebensbereiches* sichtbar werden. Indem der *Integritätsschutz* gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG derjenige ist, der im Sinne einer «Grundordnung» mangels Anwendbarkeit einer besonderen Regelung greift (vgl. zu Art. 12 846

1120 Zu diesem Konzept grundlegend Nissenbaum, 1 ff., 129 ff. Eine Betrachtungsweise, die sich auf Datenflüsse bezieht, lässt sich in der Schweiz bei Gächter/Egli, Jusletter vom 6. September 2010, N 90 ff., erkennen; auch Gogniat, Jusletter vom 20. Juni 2016, N 16 verwendet das Bild vom Datenstrom; den Datenfluss als Betrachtungsgegenstand der datenschutzrechtlichen Analyse zu definieren, schlägt auch Helfrich, 29 f., vor.

Abs. 2 lit. b und lit. c DSG resp. Art. 30 Abs. 2 lit. b und lit. c nDSG sogleich), ist die Begrifflichkeit geeignet, eine akkurate Titulierung der Grundsatzregelung für den privatrechtlichen Datenschutz zu liefern.

847 Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG regelt *nicht abschliessend* die allgemeinen Schranken der prinzipiell freien Personendatenverarbeitung, deren Missachtung eine Persönlichkeitsverletzung begründen. Damit ist es angezeigt, auch *Vorgaben ausserhalb des DSG* in die Betrachtung zu integrieren. In Erinnerung zu rufen sind datenschutzrechtlich zentrale, abweichende Bestimmungen, namentlich die *Geheimhaltungspflichten*, deren Verletzung strafbewehrt ist, vgl. insb. Art. 35 DSG und Art. 320 ff. StGB resp. Art. 62 nDSG.

848 Spezialgesetzliche Geheimhaltungspflichten betreffend den Umgang mit Personendaten korrigieren den gemäss DSG als Querschnittsgesetz gewählten Ausgangspunkt der prinzipiellen Verarbeitungsfreiheit für den privaten Bereich. Sie werden regelmässig als Verletzung des Rechtmässigkeitsprinzips, Art. 4 Abs. 1 DSG resp. Art. 6 Abs. 1 nDSG, präsentiert, womit sie über Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG in das persönlichkeitsrechtliche System einfliessen. Sie gelten insb. für Personen bestimmter Berufsgattungen wie der Ärzteschaft, Anwaltschaft usf. Gerade in den *kontext-, branchen- und bereichsspezifischen Geheimhaltungspflichten* – die sich als Ausnahmen der prinzipiell freien Datenbearbeitung mit Schranken gemäss DSG für den privaten Sektor lesen lassen und deshalb hier erwähnt werden – bestätigt sich die herausgearbeitete *dynamische, systemische sowie akzessorische Dimension* des Datenschutzrechts.[1121]

849 Geheimhaltungspflichten, wie sie *ausserhalb des DSG* statuiert werden, *derogieren die grundsätzlich freie Personendatenverarbeitung* im privaten Bereich mit Schranken für qualifizierte Verarbeitungen. Es genügt nicht, die Verarbeitung unter Einhaltung der allgemeinen Verarbeitungsgrundsätze vorzunehmen. Vielmehr bedarf es vorab einer Legitimation für die Bearbeitung, z. B. in Gestalt einer Einwilligung des Datensubjektes. Anders gewendet: Geheimhaltungspflichten schotten Datenflüsse für spezifische Bereiche bzw. Systeme ab resp. formulieren strengere Vorgaben an eine «Transmission». Geheimhaltungspflichten können somit als Staudämme beschrieben werden, die den Fluss von Personendaten aus einem System, in welchem die Personen in spezifischen Rollen agieren, beispielsweise als Ärztin und Patientin, in ein anderes System verhindern sollen. Damit ein entsprechender Personendatenfluss rechtmässig erfolgt, bedarf es der Erfüllung zusätzlicher datenschutzrechtlicher Vorgaben. In der Nomenklatur von Nissenbaum, die einen richtungsweisenden Beitrag zur Überdenkung datenschutzrecht-

1121 Herausgearbeitet im Rahmen der Analyse des Zweckbindungsgrundsatzes sowie der Argumentation im Volkszählungsurteil des Bundesverfassungsgerichts, vgl. zweiter Teil, V. Kapitel, 4.

licher Konzepte vorgelegt hat, handelt es sich bei den Geheimhaltungspflichten um eines von mehreren sog. *Transmissionsprinzipien*.[1122]

Mit diesem Terminus erfasst die Wissenschaftlerin die nuancierten Möglichkeiten zur Gestaltung von Informationsflüssen – Freiwilligkeit und Einwilligung, Gegenseitigkeit, Anonymisierung usf. –, wobei Transmissionsprinzipien definieren, unter welchen Bedingungen Personendaten von einer Partei zu einer anderen Partei eines bestimmten Kontextes transferiert werden sollen oder nicht.[1123] Die *ratio* von Geheimhaltungspflichten beschränkt sich indes nicht isoliert auf den Schutz der Persönlichkeit, wie im Rahmen der Analyse des Volkszählungsurteils und des Statistikgeheimnisses gezeigt wurde. Auch das Arztgeheimnis dient nicht einzig dem Schutz der Persönlichkeit des konkreten Patienten oder der Vertrauensbeziehung zwischen einer konkreten Ärztin und dem Patienten. Vielmehr dient dieses zugleich dem Schutz der Funktionstüchtigkeit, der Integrität des Gesundheitssektors selbst. Denn die ärztliche Versorgung und die Gesundheit als allgemeines Gut können nur dann effizient und sinnvoll sichergestellt werden, wenn Patienten vertrauensvoll ihre gesundheitlichen Themen mit der Ärztin teilen können.[1124] Wird dies nicht garantiert, riskiert man z. B., dass hochansteckende Krankheiten unbehandelt bleiben und sich ausbreiten, einzig und allein, weil jemand mangels Gewährleistung der Diskretion durch den Arzt eine Konsultation meidet. 850

Indem Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG ein nicht abschliessendes Regel-Ausnahme-Regime bezüglich der prinzipiellen Verarbeitungsfreiheit und ihrer Schranken sowie bezüglich der Persönlichkeitsverletzung vorsieht, wird erneut der Facettenreichtum des schweizerischen Datenschutzrechts – jeglicher Fokussierung auf die Persönlichkeitsverletzung und der Qualifizierung der «Basiskonstruktion» des DSG für den privaten Bereich als Integritätsschutz zum Trotz – in den Blick genommen. Kontextspezifische Geheimhaltungspflichten korrigieren die prinzipielle Verarbeitungsfreiheit gemäss DSG für den privaten Bereich und grenzen ausdifferenzierte Subsysteme im «privaten Bereich» aus informationeller Perspektive ab. Auch der «private Bereich» entpuppt sich als nicht als homogener Bereich. 851

Um das Bild zu vervollständigen, ist auf eine Entwicklung hinzuweisen, wie sie die jüngsten datenschutzrechtlichen Neuerungswellen bringen. Im Rahmen der Analyse von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a DSG wurden mehrere Schwächen des materiellrechtlichen Kernstückes des DSG für den privaten Bereich thematisiert. Das generalklauselartige, in den Persönlichkeitsschutz eingebettete Regime lässt Griffigkeit vermissen. An diesem Defizit setzen die datenschutzrechtlichen Neuerungen an: Neu werden die Verarbeitenden *proaktiv in* 852

1122 Vgl. Nissenbaum, 145 f.
1123 Vertiefend zur Konstruktion sowie zum Konzept dritter Teil, IX. Kapitel.
1124 Vgl. Nissenbaum, insb. 171 ff., aber auch 159 f.

die Pflicht zur Einhaltung der Vorgaben genommen. Die DSGVO verankert explizit einen Ansatz der *Accountability*.[1125] Den Verarbeitenden werden umfassende Dokumentations- und Rechenschaftspflichten auferlegt. Sie müssen jederzeit belegen können, dass ihre Personendatenverarbeitungen *in Einklang mit den rechtlichen Vorgaben*, auch den allgemeinen Verarbeitungsgrundsätzen, stehen.

853 Gerade mit Blick auf die faktische Einhaltung der allgemeinen Verarbeitungsgrundsätze ist deshalb auch das neue Basisinstrument in Erinnerung zu rufen: Das Verarbeitungsverzeichnis, Art. 30 DSGVO resp. Art. 12 nDSG. Mit diesem wird die Landschaft der Verarbeitungsprozesse abgebildet. Es ermöglicht Transparenz sowie die Überprüfbarkeit der Verarbeitungsprozesse auf ihre Konformität mit den Verarbeitungsgrundsätzen und -vorgaben. Insofern werden an *erster Stelle* die Verarbeitenden in die Pflicht genommen. Parallel werden mit den neuen Datenschutzerlassen die behördlichen Prüfungs- und Interventionsmöglichkeiten ausgebaut.

854 Mit den skizzierten Neuerungen wird die im zivilrechtlichen Deliktsrecht, defensivrechtlich, abwehrrechtlich strukturierten Persönlichkeitsrecht basierende Konzeption bisheriger Datenschutzgesetzgebung in *markanter Weise ergänzt*. Der Datenschutzgesetzgeber fokussiert nicht mehr ausschliesslich auf die Eingriffs- und Verletzungshandlung sowie eine darauffolgende Abwehrhandlung des Datensubjektes in Gestalt eines zivil- und individualrechtlichen Rechtsschutzes wegen datenschutzrechtlicher Persönlichkeitsverletzung, vgl. hierzu Art. 15 DSG und Art. 32 nDSG. Vielmehr setzen die datenschutzrechtlichen Neuerungen früher an. Das Augenmerk richtet sich quasi vorgeschaltet verstärkt auf die Sicherstellung der Einhaltung der Verarbeitungsvorgaben, wofür die Verarbeitenden in der Pflicht stehen. Die Einhaltung des materiellrechtlichen Herzstückes des Datenschutzes wird abgesichert über mehrere neue Umsetzungsinstrumente.

855 Ein Verarbeitungsverzeichnis, das gerade auch die Konformität der Verarbeitungshandlungen mit den *allgemeinen und abstrakten Verarbeitungsgrundsätzen effektuiert*, ist dort von besonderer Relevanz, wo diese *allgemeinen Verarbeitungsgrundsätze* die einzige Schranke der prinzipiellen Verarbeitungsfreiheit darstellen, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG. Im zweistufigen Regime der DSGVO dient das Verarbeitungsverzeichnis dazu, die Einhaltung *beider Schranken* – das Vorliegen eines Legitimationsgrundes sowie die Einhaltung der allgemeinen Verarbeitungsgrundsätze – zu gewährleisten und durch die Verarbeitenden wie durch die Behörden überprüfbar zu machen.

856 *Zusammenfassend* ist zu statuieren, dass Art. 12 Abs. 2 lit. a i. V. m. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8

1125 Vgl. Art. 24 und Art. 30 DSGVO.

nDSG einen *Integritätsschutz* implementiert. Für den privaten Bereich gilt gemäss DSG kein allgemeines Verarbeitungsverbot. Vielmehr findet die prinzipielle Verarbeitungsfreiheit ihre wichtigsten Schranken anhand der allgemeinen Verarbeitungsgrundsätze. Persönlichkeitsverletzend sind *qualifizierte Verarbeitungshandlungen*, mithin diejenigen, welche die allgemeinen Verarbeitungsgrundsätze, vgl. insb. Art. 4 DSG, aber auch Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG, resp. Art. 6 und Art. 8 nDSG missachten.

857 Die grosszügige Inklusion von Verstössen gegen Vorgaben des DSG in die nicht abschliessend enumerierten Tatbestände der Persönlichkeitsverletzung gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG bauen den Datenschutz *nur in theoretischer Hinsicht* aus. Weil Persönlichkeitsverletzungen durch qualifizierte Personendatenverarbeitungen nicht nur von den Datensubjekten kaum je festgestellt werden, ist über die Integration weiterer Verstösse gegen Datenschutzvorgaben in die Persönlichkeitsverletzung nicht viel gewonnen. An einem solchen konzeptionellen Schwachpunkt scheinen die datenschutzrechtlichen Neuerungen anzusetzen, welche konkrete Umsetzungsinstrumente vorsehen, wie das Verarbeitungsverzeichnis oder allgemeine Dokumentations- und Rechenschaftspflichten.[1126]

858 Mit ihnen vollzieht sich ein Perspektivenwechsel, denn der Fokus richtet sich nicht «erst» auf die «persönlichkeitsverletzende Datenverarbeitung». Vielmehr werden die Verarbeitenden *früher* durch *konkrete Umsetzungsinstrumente* in die Pflicht genommen, womit die Einhaltung der Datenschutzvorgaben effizienter gewährleistet werden soll. Ebendies ist für ein Regime von besonderer Bedeutung, das von einer prinzipiellen Verarbeitungsfreiheit ausgeht und die Schranken in erster Linie generalklauselartig definiert, vgl. Art. 12 Abs. 2 lit. a i. V. m. Art. 4 DSG resp. Art. 30 Abs. 2 lit. a i. V. m. Art. 6 und Art. 8 nDSG. In entsprechenden Neuerungen deutet sich ein Sichtwechsel an, indem primär die Verarbeitenden für ihre Handlungen in die Pflicht genommen werden. Neu sind verschiedene prozedurale und organisatorische Massnahmen durch diese zu ergreifen, um dem materiellrechtlichen Kernbestand des Datenschutzes proaktiv Nachachtung zu verschaffen. Die isolierte materiellrechtliche, persönlichkeitsrechtliche Fokussierung auf einen abwehr- und deliktsrechtlich gedachten Subjektschutz wird aufgeweicht resp. ergänzt. Das bisherige materiellrechtlich basierte Datenschutzrecht für den privaten Bereich lastete in erster Linie auf einem abwehrrechtlich begründeten Persönlichkeitsschutz. Neu wird der Schutz des Individuums auf organisatorische wie prozedurale Instrumente umgelagert, was auch der faktischen Verwirklichung der Verarbeitungsgrundsätze dienen soll.

1126 Hierzu dritter Teil, VIII. Kapitel, A.2.6.

859 Eine differenzierte Sicht auf das Schweizer Datenschutzregime wurde nicht nur anhand eines Blicks auf seine jüngsten Entwicklungen sichtbar. Vielmehr konnte bereits anhand des geltenden Regimes nach Art. 12 Abs. 2 lit. a DSG die hohe Differenziertheit des Gesetzes nachgewiesen werden. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG schaffen zwar die *Grundsatzkonstruktion* des schweizerischen Datenschutzrechts. Sie verankern für den privaten Bereich die prinzipielle Verarbeitungsfreiheit mit Schranken in den allgemeinen Verarbeitungsgrundsätzen, deren Missachtung eine Persönlichkeitsverletzung begründen. Dieser sog. «Integritätsschutz» findet seine wohl einschlägigste Abweichung in spezifischen Geheimhaltungspflichten. Die bereichs- und kontextspezifischen Geheimhaltungspflichten, welche die prinzipielle Verarbeitungsfreiheit des DSG durchbrechen, zeigen eindrücklich, dass das schweizerische Datenschutzrecht keineswegs isoliert die Person vor unfairen Verarbeitungshandlungen schützt. Vielmehr zielen solche, die Basiskonstruktion des DSG derogierende Geheimhaltungspflichten über den Schutz der Person hinausgehend auf den Schutz der Funktionstüchtigkeit resp. Integrität spezifischer gesellschaftlicher Bereiche, beispielsweise des Gesundheitsbereiches, ab. Gleichwohl sind Art. 12 Abs. 2 lit. a DSG, weniger ausgeprägt Art. 30 Abs. 2 lit. a nDSG, als Kernbestimmungen und Basiskonstruktionen des DSG zu sehen, indem die Schranken der grundsätzlichen Verarbeitungsfreiheit durch allgemeine Verarbeitungsgrundsätze markiert werden, deren Missachtung eine Persönlichkeitsverletzung begründet. Für diese datenschutzgesetzliche Basiskonstruktion des privaten Bereichs wird die Charakterisierung als *Integritätsschutz* vorgeschlagen.

2.2.2. lit. b – Widerspruchslösung

860 Eine Persönlichkeitsverletzung liegt nach dem allgemeinen Regime des DSG für den privaten Bereich zudem dann vor, *wenn Personendaten entgegen dem ausdrücklichen Willen der betroffenen Person bearbeitet werden*. Die noch geltende Fassung gemäss Art. 12 Abs. 2 lit. b DSG integriert den Passus «ohne Rechtfertigungsgrund» und wählt die Formulierung «entgegen dem ausdrücklichen Willen».

861 Mit der Totalrevision wird auf die Integration der Rechtfertigungsgründe in Art. 30 Abs. 2 lit. b nDSG verzichtet: Während sich Art. 30 nDSG konsequent mit der Tatbestandsmässigkeit befasst, sind die Rechtfertigungsgründe in Art. 31 nDSG niedergelegt. Der «zivilrechtliche resp. individualrechtliche» Rechtsschutz für den Datenschutz im privaten Bereich findet sich in Art. 32 nDSG. Neu wird in Art. 30 Abs. 2 lit. b nDSG von einer der Personendatenbearbeitung «entgegengestellten ausdrücklichen Willenserklärung» gesprochen. Nachfolgend wird nicht im Detail auf die mit der Totalrevision einhergehenden Veränderungen in Bezug

auf die Anforderungen betreffend einen gültigen Widerspruch eingegangen. Die Neuerungen im Zusammenhang mit den Willenserklärungen, welche die Totalrevision bringt, bedürfen einer eigenständigen Untersuchung. An dieser Stelle erfolgt eine konzeptionelle Analyse, um Erkenntnisse für den in dieser Studie entwickelten Paradigmenwechsel zu generieren.

Mit Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG findet der *Wille des Datensubjektes* in die allgemeine Datenschutzgesetzgebung Eingang. Gleichwohl handelt es sich dabei namentlich nach Totalrevision des DSG nicht um die einzige Norm, die an diesem subjektiven Element, dem Willen des Datensubjektes, anknüpft. 862

Nach Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG führt eine Verarbeitung entgegen einem *Widerspruch des Datensubjektes zu einer Persönlichkeitsverletzung*. Eine *Persönlichkeitsverletzung* liegt gemäss Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG dann vor, wenn eine Datenbearbeitung *gegen den ausdrücklichen Willen* (resp. neu entgegen ausdrücklicher Willenserklärung) der betroffenen Person erfolgt. Allerdings kann diese gerechtfertigt werden, sofern Rechtfertigungsgründe ausserhalb des Willens des Datensubjektes dessen Widerspruch überwiegen, vgl. Art. 13 DSG resp. Art. 31 nDSG. 863

Diese *Widerspruchslösung* für den privaten Sektor im schweizerischen DSG ist eine logische Folge des gewählten Ansatzes. Sie ist eine *konsequente Umsetzung des gewählten Ausgangspunktes der Freiheit der Datenbearbeitung*, die beschränkt wird: Dies geschieht basierend auf die lit. b der besagten Bestimmungen aufgrund eines Widerspruchs des Datensubjektes. 864

Die Widerspruchslösung dürfte durchaus als Selbstbestimmungsansatz qualifiziert werden. Denn mit ihr wird der Wille des Datensubjektes zu einem Kriterium der (un)zulässigen Personendatenverarbeitung. Gleichwohl ist zu betonen, dass das Recht auf informationelle Selbstbestimmung untrennbar mit dem Volkszählungsurteil des Bundesverfassungsgerichts einhergeht. Mit einem «Recht auf informationelle Selbstbestimmung», bei welchem der Widerspruch die prinzipielle Verarbeitungsfreiheit durchbricht, ist ein *anderes Konzept verbunden,* als es mit dem im Volkszählungsurteil geprägten Grundrecht auf informationelle Selbstbestimmung der Fall ist. In beiden Konstruktionen kommt zwar dem Willen resp. der Selbstbestimmung des Datensubjektes Relevanz zu. Nach DSGVO sowie verfassungsgerichtlicher Rechtsprechung allerdings bildet die Einwilligung einen Erlaubnistatbestand zur Durchbrechung eines prinzipiellen Verarbeitungsverbotes. Die strukturellen Differenzen wurden in der Schweiz lange nicht hinreichend gewürdigt. Erst die intensivierte Auseinandersetzung, wie sie von den datenschutzrechtlichen Neuerungswellen angestossen wurde, führt zu treffliche- 865

ren Beschreibungen des Konzepts des DSG. Insofern ist auch auf die Studie von Fasnacht aus dem Jahr 2017 hinzuweisen.[1127]

866 Die «informierte Einwilligung» hat in Europa nicht nur im Datenschutzrecht Hochkonjunktur, sondern ebenso im Bereich des (Bio-)Medizinrechts.[1128] Anders gewendet: Juristisch gewinnt ein Konzept der Selbstbestimmung dort an Einfluss, wo es um die Emanzipation des Menschen von den Technologien geht. Fasnacht gibt unter dem Titel «Datenschutzgrundrecht» und Art. 13 Abs. 2 BV einen systematischen Überblick über das weite Spektrum an Auslegungen – von Missbrauchsordnungen bis zum Recht auf informationelle Selbstbestimmung.[1129] Im Ergebnis schliesst er sich der Ansicht an, wonach Art. 13 Abs. 2 BV als Recht auf informationelle Selbstbestimmung zu lesen sei: «Der Einzelne soll grundsätzlich selbst bestimmen können, wer seine Personendaten wie bearbeitet.»[1130] Da es sich um ein Grundrecht handle, das bekanntlich nicht direkt im Privatrecht gelte, entfalte das Recht auf informationelle Selbstbestimmung gemäss Art. 35 BV über den zivilrechtlichen Persönlichkeitsschutz Wirkung. Die datenschutzrechtliche Einwilligung fungiere hier als Rechtfertigungsgrund: Sie rechtfertige eine Persönlichkeitsverletzung.[1131] Die Aussage ist nicht falsch. Sie expliziert indes die konzeptionellen Differenzen in Bezug auf die Rolle des Willens des Datensubjektes nicht hinreichend. Hierzu daher einige klärende Ausführungen.

867 Das Volkszählungsurteil des Bundesverfassungsgerichts hat die datenschutzrechtlichen Entwicklungen in Deutschland, ja in Europa nachhaltig geprägt.[1132] Hervorzuheben sind *zwei Aspekte*: Erstens hat das Volkszählungsurteil verfassungsrechtliche Vorgaben für den Umgang mit *Personendaten im öffentlichen Bereich*, also durch *staatliche Stellen*, formuliert. Zweitens wurde mit dem Volkszählungsurteil und seinen Ausführungen zum Recht auf informationelle Selbstbestimmung ein Systemwechsel vollzogen: Ein bisher auf die Verhinderung von missbräuchlichen Personendatenverarbeitungen gerichteter Datenschutz wurde

1127 Fasnacht, *passim*; zur datenschutzrechtlichen Einwilligung auch Heuberger, N 267 ff.; allgemein zur Einwilligung im System des Persönlichkeitsschutzes gemäss Art. 28 ZGB Haas, *passim*; zu rechtsdogmatischen Fragen der rechtfertigenden Einwilligung vgl. Kothe, AcP 1985, 105 ff.

1128 Vgl. Barocas/Nissenbaum in ihren verschiedenen Beiträgen; zur informierten Einwilligung als Ausdruck des verfassungsrechtlich verbürgten Selbstbestimmungsrechts im Kontext des Biomedizinrechts eine Übersicht über die Lehrmeinungen Karavas, Körperverfassungsrecht, 222 ff.; zur Frage, ob Selbstbestimmung im Zeitalter der Biotechnologie überhaupt möglich ist, vgl. Fateh-Moghadam, BJM 2018, 215 ff.; zur informierten Einwilligung gemäss DSG insb. Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.

1129 Fasnacht, N 96 ff.

1130 Ders., N 206.

1131 Ders., N 217 ff.

1132 Vgl. Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 27 ff., der das Urteil als Zäsur beschreibt; Buchner, 31 f.; kritisch zur Staatszentrierung Vesting, in: Ladeur (Hrsg.), 155 ff.

ersetzt durch ein prinzipielles Verarbeitungsverbot mit Schranken.[1133] Der Schutz von Personendaten wurde zur Regel, der staatliche Zugriff zur Ausnahme. Gesetzgeberisch umgesetzt mündete dies in ein grundsätzliches Verarbeitungsverbot mit Erlaubnistatbeständen.[1134]

868 Heute wird dieses Regime des prinzipiellen Verarbeitungsverbots mit Erlaubnistatbeständen in der DSGVO *gleichermassen* für Personendatenverarbeitungen durch öffentliche Stellen *wie private Verantwortliche vorgesehen, vgl. Art. 6 DSGVO*. Jegliche Personendatenverarbeitung, nicht nur die qualifizierte, bedarf eines Erlaubnistatbestandes. Zudem sind die Verarbeitungsgrundsätze gemäss Art. 5 DSGVO sowie weitere neuen Vorgaben einzuhalten. Die Gültigkeit des Prinzips des Verarbeitungsverbotes mit Erlaubnistatbestand, wie es ursprünglich für den öffentlichen Bereich entwickelt wurde, wird auf den privaten Bereich ausgedehnt. Mangels anderweitigen Ermächtigungsgrundes fällt als Erlaubnistatbestand für die Personendatenverarbeitung gemäss Art. 6 Abs. 1 lit. a DSGVO die *Einwilligung* der betroffenen Person in Betracht. Gleichzeitig operiert auch die DSGVO mit dem Instrument des Widerspruches, mittels dessen eine aufgrund eines anderen Erlaubnistatbestandes vorab legitimierte Personendatenverarbeitung qua Widerspruch des Subjektes zu einer unrechtmässigen Verarbeitung wird: So hat die Kommission Personendatenverarbeitungen zum Direktmarketing als «legitimate interest» im Sinne von Art. 6 Abs. 1 lit. f DSGVO anerkannt.[1135] Die in diesem Sinne zulässige Personendatenverarbeitung kann indes durch einen Widerspruch des Datensubjektes verboten werden. Folglich wird eine Personendatenverarbeitung zum Zwecke des Direktmarketings definitiv unzulässig.

869 Ebendies entspricht nicht dem Ansatz des DSG, auch nicht nach seiner Totalrevision. Die Einwilligung figuriert gemäss DSG im privaten Bereich gerade nicht als Erlaubnistatbestand für prinzipiell verbotene Verarbeitungshandlungen. Vielmehr dreht das Widerspruchsrecht gemäss Art. 12 Abs. 2 lit. b DSG resp. Art. 30

1133 Vgl. Buchner, 27 ff., insb. 43; von Gallwas, NJW 1992, 2785 ff., 2788 ff. wird der entscheidende Wandel darin verortet, dass das Subjekt mit der Anerkennung eines Rechts auf informationelle Selbstbestimmung grundsätzlich Herr über die es betreffenden Personendaten ist, ihm ein prinzipielles Entscheidungsrecht zusteht; Eberle, in: Wilhelm (Hrsg.), 113 ff., 114 ff., der vom Prinzip «in dubio pro securitate» spricht, weil prinzipiell jede Personendatenverarbeitung als Gefährdung des Persönlichkeitsrechts taxiert wird; die vom Autor präsentierte These, wonach das Grundrecht auf informationelle Selbstbestimmung erst aus dem jeweiligen Gesellschaftsbereich heraus seine Struktur erhalte, stiess auf Widerstand, vgl. ebenda, 123.

1134 Vgl. Buchner, 43.

1135 Hierzu dritter Teil, VIII. Kapitel, A.; erläuternd zur Direktwerbung auch die Orientierungshilfe der deutschen Datenschutzkonferenz (DSK), abrufbar unter: <https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Entschliessungen_Datenschutzkonferenz/Inhalt/96_-Konferenz/Orientierungshilfe-der-Aufsichtsbehoerden-zur-Verarbeitung-von-personenbezogenen-Daten-fuer-Zwecke-der-Direktwerbung-unter-Geltung-der-Datenschutz-Grundverordnung-_DS-GVO_/OH_Werbung_Stand_07_11_2018.pdf> (zuletzt besucht am 30. April 2021); zur Direktwerbung als datenschutzrechtlich relevante Form der Werbung früh Schineis, 119 ff.

Abs. 2 lit. b nDSG den gesetzgeberischen Entscheid für die prinzipielle Verarbeitungsfreiheit einzelfallbezogen in ein Verbot um.[1136]

870 Unbestritten wird mit einem Widerspruch ebenso ein «Selbstbestimmungsrecht» des Datensubjektes adressiert. Es handelt sich indes nicht um das identische Konzept, wie es mit dem Volkszählungsurteil des Bundesverfassungsgerichts hervorging und wie es heute gemäss DSGVO auch für den privaten Bereich gilt. Ein «Recht auf informationelle Selbstbestimmung» ist untrennbar mit dem Volkszählungsurteil des Bundesverfassungsgerichts und dessen Gehalt verknüpft. Eine Folgerung war die Implementierung eines prinzipiellen Verarbeitungsverbotes mit Erlaubnisvorbehalten.

871 Somit überzeugt es nicht, wenn für das schweizerische Datenschutzrecht pauschal für den privaten Bereich vom Recht auf informationelle Selbstbestimmung gesprochen wird.[1137] Die konzeptionellen Unterschiede werden damit ignoriert, zumal es die Einwilligung ist, die genuin mit dem Recht auf informationelle Selbstbestimmung assoziiert wird.[1138] Zugleich wird ein Rechtsbestand suggeriert, der so im schweizerischen Datenschutzrecht nicht gewährleistet wird. In der Schweiz kommt gemäss Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG dem Widerspruch (und gerade nicht der Einwilligung), entsprechend dem Konzept der Freiheit der Datenbearbeitung, die Funktion eines *Verbotstatbestandes* zu. Immerhin: Auch in der Schweiz weisen Spezialbestimmungen der Einwilligung die Funktion eines Erlaubnistatbestandes zu, insb. die beruflichen Geheimhaltungspflichten. Weiter ist der Wille des Datensubjektes als Rechtfertigungsgrund relevant, Art. 13 Abs. 1 DSG und Art. 31 Abs. 1 nDSG, insb. bei persönlichkeitsverletzenden Handlungen nach Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG.

872 Die Schweiz integriert folglich den *Willen des Datensubjektes in nuancierter Weise* in das DSG. Dies geschieht indes *nicht* in Gestalt eines Erlaubnistatbestands für dem Grundsatz nach verbotene Personendatenverarbeitungen. Wenn das Datensubjekt mit einem Widerspruch nach Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG die grundsätzlich erlaubte Personendatenverarbeitung *verbieten* kann, mag man darin die Verbürgung eines «Selbstbestimmungsrechts» se-

1136 Vgl. für Deutschland dazu, dass primär der Gesetzgeber aufgerufen ist, zwischen einem Verbot mit Einwilligungsvorbehalt und einer Erlaubnis mit Widerspruchsmöglichkeiten zu entscheiden, Ohly, 195.

1137 Ungeachtet dieser grundlegenden Differenzen ist eine Praxis zu problematisieren, unter der gewissermassen zur Sicherheit die datenschutzrechtliche Einwilligung eingeholt wird, obschon eine Verarbeitungshandlung dieser nicht bedürfte. Nach DSGVO für den Fall, dass ein anderweitiger Legitimationsgrund vorliegt, nach DSG für den Fall, dass die Personendatenverarbeitung innerhalb der Schranken stattfindet. Die datenschutzrechtliche Einwilligung zur «Sicherheit» einzuholen, ist problematisch, da sie eine «Selbstbestimmung» des Datensubjektes suggeriert, obschon die Verantwortlichen auch ohne diese verarbeiten dürften.

1138 Vgl. Radlanski, 271.

hen. Dies mit dem Argument, dass es im Ergebnis das Datensubjekt ist, das mittels Verbotes darüber entscheidet, wer welche Personendaten über es bearbeitet. Mehrere Punkte sind zu ergänzen:

Erstens besteht – wie gesagt – eine markante Differenz zwischen einem Recht auf informationelle Selbstbestimmung, das mittels eines Systems des grundsätzlichen Verarbeitungsverbotes umgesetzt wird, und einem System der grundsätzlichen Verarbeitungsfreiheit mit Schranken und darin eingebetteter Widerspruchslösung. Es handelt sich – konsequent implementiert – um diametral auseinandergehende Ansätze. 873

Diese Klarstellung wird anhand eines *Exkurses* in das Transplantationsrecht erhärtet: Das Zustimmungserfordernis ist fester Bestandteil des Transplantationsgesetzes, vgl. insb. Art. 5, Art. 8 Abs. 2, Art. 13 Abs. 3, Art. 39 f., Art. 48 Abs. 1 Ziff. 1 und Ziff. 2 Transplantationsgesetz.[1139] Organe oder sonstige Körpersubstanzen zu Transplantationszwecken zur Verfügung zu stellen, bedarf in der Schweiz *de lege lata* der erklärten, informierten Einwilligung des «Organträgers». Dies kann beispielsweise durch einen Spenderausweis dokumentiert werden. Die Knappheit an Spenderorganen hat hierzulande die Debatte um die Abkehr vom Zustimmungsmodell und die Hinwendung zu einem Widerspruchsmodell ausgelöst. Sie setzte sich nicht durch: Der Nationalrat schloss sich einer Empfehlung des Bundesrates an und verwarf am 5. März 2015 eine entsprechende Änderung.[1140] Damit werde – so der Fernsehbericht – auf einen Systemwechsel verzichtet.[1141] Im Bereich des Transplantationsrechts wird selbst in der allgemeinen Medienberichterstattung und nicht nur in der Fachliteratur der *grundlegende Unterschied zwischen einer Einwilligungs- und der Widerspruchslösung* unmissverständlich thematisiert. 874

Ganz anders im Bereich des Datenschutzgesetzes, wo diese Systemdifferenz lange nicht adäquat erfasst wurde. Ein Systemwechsel, wie er in der Schweiz für das Transplantationsgesetz diskutiert wurde – wenn auch in die entgegengesetzte Richtung –, stand hierzulande selbst mit der Totalrevision des DSG nicht zur Debatte. Er wurde nicht diskutiert, obschon mit ihm eine Annäherung an die 875

1139 Bundesgesetz über die Transplantation von Organen, Geweben und Zellen vom 8. Oktober 2004, SR 810.21.

1140 Parlament, Transplantationsgesetz, Teilrevision, Bern 2015, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20130029> (zuletzt besucht am 30. April 2021); vgl. Tagesanzeiger, Parlament lehnt automatische Organspende ab, Zürich 2015, <https://www.tagesanzeiger.ch/schweiz/standard/Parlament-lehnt-automatische-Organspende-ab/story/26647013> (zuletzt besucht am 30. April 2021).

1141 SRF, Organspende: Nationalrat gegen Widerspruchslösung, Zürich 2015, <http://www.srf.ch/news/schweiz/session/organspende-nationalrat-gegen-widerspruchsloesung> (zuletzt besucht am 30. April 2021).

DSGVO erreicht werden sollte. Letztere sieht für den privaten Bereich das prinzipielle Verarbeitungsverbot vor, vgl. Art. 6 DSGVO.[1142]

876 *Zweitens*: In einem System mit Ausgangspunkt der Verarbeitungsfreiheit mit Widerspruchslösung ist die *Erkennbarkeit der Datenverarbeitung* und damit die Transparenz notwendige Vorbedingung der Funktionstüchtigkeit einer Widerspruchslösung. Theoretisch und formalgesetzlich greifen insofern Grundsätze der Transparenz resp. Erkennbarkeit, wobei eine Vorgabe der angemessenen Informierung über ein Widerspruchsrecht ebenso anerkannt wird.[1143] Dessen ungeachtet können mit Blick auf die datenschutzgesetzliche Widerspruchslösung die *faktischen Rahmenbedingungen und damit die datenschutzrechtliche Realität* nicht ausgeblendet werden: Kaum ein Datensubjekt überschaut, wer wann welche Personendaten über es verarbeitet. Hieran werden auch die mittels Totalrevision ausgebauten Informations- und Transparenzvorgaben nicht viel ändern. Zwar wird über viel mehr informiert werden, doch die Informiertheit der Datensubjekte wird damit nicht zwangsläufig angehoben. Somit dürfte in Bezug auf die Transparenz, die das Widerspruchsrecht faktisch effektuieren soll, von Defiziten ausgegangen werden.[1144] Das Widerspruchsrecht bleibt bei Lichte betrachtet über weite Strecken eine kühne Fiktion.[1145]

877 *Drittens* soll – entgegen einem Widerspruch des Datensubjektes – eine Verarbeitung gleichwohl zulässig sein, sofern hierfür ein anderweitiger Rechtfertigungsgrund vorliegt.[1146] Dies dürfe zwar nur ganz ausnahmsweise der Fall sein.[1147] Weil indes namentlich das konturlose überwiegende Interesse oftmals die beschränkende Wirkung vermissen lässt, schwächt das Schweizer Recht die Bedeutung des Willens des Datensubjektes in Gestalt eines Widerspruchs ab. Es wäre angezeigt, dass der *Gesetzgeber selbst* entsprechende, einen *Widerspruch* übertrumpfende Interessen *konkreter definiert* würde.[1148]

878 Die Widerspruchslösung und ihre konkretisierende, einbettende Rechtsgestaltung ist folglich kein Garant und Regime, das eine Titulierung als «Recht auf informationelle Selbstbestimmung» in überzeugender Weise trägt. Dies gilt *a fortiori* in Anbetracht der Unübersichtlichkeit durchgeführter Datenbearbeitungen in einem

1142 Botschaft 2017–1084, 1 ff., 3 ff.
1143 Hierzu Rosenthal, HK-DSG, Art. 12 N 26.
1144 Vertiefend zum Vollzugsdefizit dritter Teil, VII. Kapitel, A. und B.; zur mangelnden Effektivität vgl. Simitis, Symposium, 1 ff.
1145 Ein Befund, der übrigens ebenso für die informierte Einwilligung gilt, vgl. insofern vertiefend dritter Teil, VIII. Kapitel, A.4.2.2.
1146 Vgl. Art. 12 Abs. 2 lit. b DSG, der explizit die Rechtfertigung zulässt; Rampini, BSK-DSG, Art. 12 N 13.
1147 Vgl. BGE 136 III 508, Regeste.
1148 Nach DSGVO gilt gemäss Kommission das Direktmarketing als «legitimate interest» und Erlaubnistatbestand. Ein Widerspruch des Datensubjektes allerdings macht eine entsprechende Verarbeitung per se verboten; eine wiederum übertrumpfende Rechtfertigung ist nicht denkbar.

System mit prinzipieller Verarbeitungsfreiheit, der Tatsache defizitärer Rechtseinhaltung ebenso in Bezug auf die Transparenz sowie eine Rechtslage, wonach ein Widerspruch durch gesetzlich nicht präzis umrissene «überwiegende Interessen» beiseitegeschoben werden kann.

879 Unter dem Titel des Widerspruchsrechts sind abrundend die Anglizismen «*opt-out*» und «*opt-in*» zu thematisieren.[1149] Das Begriffspaar *opt-in und opt-out* wird zur Systembezeichnung für das Einwilligungs- oder Widerspruchsmodell, womit der jeweils gewählte prinzipielle Ausgangspunkt korrigiert wird, verwendet.[1150] Für diese konzeptionellen Grundsatzdimensionen wird die Bezeichnung *opt-in und opt-out im weiteren Sinne* vorgeschlagen.[1151] Das Begriffspaar von *opt-out und opt-in im engeren Sinne* adressiert damit zusammenhängend die Art und Weise, wie eine datenschutzrechtliche Willenserklärung *formularmässig* erklärt wird resp. wie ein (elektronisches) Formular auszugestalten ist.[1152]

880 Das Schweizer System wird neuerdings regelmässig als eines des *opt-out* beschrieben.[1153] Mit Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG dürfte es als *opt-out im weiteren Sinne* zu qualifizieren sein. Weil selbst der Widerspruch im Rahmen des Systems prinzipieller Verarbeitungsfreiheit mit Schranken «übertrumpft» werden kann, sollte das Regime des DSG für den privaten Bereich präzisierend als ein *relatives opt-out im weiteren Sinne taxiert werden*. Die *Widerspruchslösung* gemäss DSG verlangt die *ausdrückliche* Erklärung, was m. E. ein aktives Verhalten bedingt. Ein konkludentes oder passives Verhalten scheint nicht geeignet, um einen gültigen Widerspruch anzubringen. In diesem Zusammenhang ist zudem zu beachten, dass die datenbearbeitenden Stellen einen Hinweis auf das Widerspruchsrecht anzubringen haben, womit dessen Wahrnehmung in angemessener Weise durch die betroffene Person eingeräumt wird.[1154]

881 Für *Rechtsordnungen mit Einwilligungsmodell und -erfordernis* werden hinsichtlich formulartechnischer Gestaltungsmöglichkeiten verschiedene Versionen diskutiert: Als *opt-in im engeren Sinne* wird im elektronischen Kontext eine Erklärungsmodalität bezeichnet, in welcher neben dem einschlägigen Text ein Kästchen angebracht ist, das leer ist. Das Datensubjekt hat durch aktives Setzen eines Häkchens seine Einwilligung zu erklären. Das *opt-out im engeren Sinne* dagegen erfolgt dergestalt, dass eine Checkbox leer ist und das Leerlassen als «vermutete

1149 Insofern auch Buchner, DuD 2015, 402 ff., 403; Fasnacht, N 398 ff.; hierzu ebenso Langhanke, 65 ff.; sodann Hoeren, LMK 2008, 65 f.
1150 Hierzu Radlanski, 18; für dieses System Art. 6 DSGVO.
1151 Ders., 18 f.
1152 Zum Ganzen Rogosch, 32 ff., 132; Radlanski, 19, m. w. H.; Heuberger, N 189 ff.; Fasnacht, N 398 ff.; Buchner, DuD 2010, 52.
1153 So Hussein, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.114; Fasnacht, N 402 ff.
1154 Vgl. Rosenthal, HK-DSG, Art. 12 N 26.

Einwilligung» gilt. Das Setzen eines Häkchens gilt als verweigerte Einwilligung. Es finden sich auch Mischformen. Einschlägiges Kriterium für die Qualifizierung ist das Aktivwerden des Datensubjektes im Rahmen seiner Einwilligungserklärung, wobei nur das Tätigwerden der betroffenen Person als *opt-in im engeren Sinne* gilt.[1155]

882 Die Unterscheidung von *opt-in und opt-out im engeren Sinne* ist nicht bloss begrifflicher oder theoretisch-formeller Natur. Sie ist hoch relevant aufgrund eines statistisch belegten Befundes: Demnach verhält sich ein grosser Teil der Menschen gerade im Internet hinsichtlich Formulareinwilligungen *passiv*: Eine Voreinstellung wird in aller Regel nicht geändert.[1156] Anders gewendet bedeutet dies, dass eine Einwilligung *proaktiv* deutlich seltener erteilt wird als eine *passive Einwilligung*, bei der die «Einwilligung» voreingestellt ist und das Datensubjekt diese aktiv beseitigen müsste. Vor diesem Hintergrund erstaunt nicht, dass im Anwendungsbereich der DSGVO verlangt wird, dass Verantwortliche die «erteilte Einwilligung» nachweisen können müssen, wobei es einer bestätigenden Handlung bedarf. Sie wird elektronisch durch *Anklicken* eingeholt.[1157]

883 Die Herausforderungen von Einwilligungskonstruktionen erschöpfen sich indes nicht darin. Denn selbst bei ausdrücklich zu erteilenden Zustimmungen zeichnet sich ab, dass diese oft rein *schematisch* erfolgen. Die Erfüllung der Gültigkeitsvoraussetzungen – Informiertheit und Freiwilligkeit – stehen damit auf dem Spiel. Die Situation präsentiert sich dergestalt, dass die unmittelbar verfolgten Interessen resp. das primäre Ziel, aufgrund dessen das Datensubjekt beispielsweise das Internet nutzt – Bestellung einer Sache, Suche nach Informationen –, mittelbare Interessen gänzlich absorbieren und datenschutzrechtliche Erwägungen verdrängen. Wer im Internet ein Hotel betrachten möchte, will nicht Einwilligungserklärungen studieren; wer ein Buch bestellen will, klickt sich durch die datenschutzrechtlichen Erfordernisse durch, um dieses Ziel möglichst effizient zu erreichen. Paradoxerweise rückt damit faktisch die von den Menschen erklärte hohe Bedeutung, die sie dem Datenschutz zuweisen, in den Hintergrund.

884 Damit ist ein datenschutzrechtlicher Brennpunkt offensichtlich: Die Tragfähigkeit von Einwilligungskonstruktionen als Lösungsansatz für datenschutzrechtliche Herausforderungen wird – obschon gesetzgeberisch eine Kernstrategie – kritisch beleuchtet.[1158] Entsprechende Studien stammen aus Rechtskreisen mit jeweils an-

1155 M. w. H. Radlanski, 19.

1156 Rogosch, m. w. H., 13; Buchner, DuD 2010, 39 ff. und DuD 2010, 52; Radlanski, 20; vgl. zur Ineffizienz von Opt-out-Lösungen im Internet Solove, Stan. L. Rev. 2001, 1393 ff., 1458.

1157 Jüngst insofern DSK, Kurzpapier Nr. 20, Einwilligung nach der DSGVO, <https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Internationales/Datenschutz-Grundverordnung/Kurzpapiere_der_DSK_als_Auslegungshilfen_zur_DSGVO/DSK_KPNr_20_Einwilligung.pdf> (zuletzt besucht am 30. April 2021).

1158 Insb. durch Nissenbaum sowie Barocas/Nissenbaum, aber auch Radlanski.

derem Regime als dem schweizerischen – aus Deutschland und den USA. Mit der Berücksichtigung ihrer Erkenntnisse kann unter Umständen der Umweg über ein nicht effektives Rechtsinstrumentarium (namentlich: Selbstbestimmungs- resp. informed consent-Lösungen) vermieden werden. Vorab ist indes das Bild des schweizerischen datenschutzgesetzlichen Systems zu vervollständigen.

2.2.3. lit. c – Sphärentheoretische Relikte

885 Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG werden primär konzeptionell dargelegt. Anknüpfend an die Analyse zu Art. 12 Abs. 2 lit. a und lit. b DSG resp. Art. 30 Abs. 2 lit. a und lit. b nDSG lässt sich einleitend feststellen, dass Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG die beiden beleuchteten Regelungsansätze bestätigen: Nach DSG für den privaten Bereich begründet erst die *qualifizierte Verarbeitungshandlung* eine Persönlichkeitsverletzung. Gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG erfolgte die Qualifizierung anhand der Verarbeitungs*handlung*, die *grundsatzwidrig vorgenommen wurde*. Das Qualifizierungsmerkmal ist ein *objektives*. In Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG erfolgt die Qualifizierung durch den *Widerspruch*, womit das subjektive Qualifizierungskriterium greift. Das Qualifikationskriterium gemäss Art. 12 Abs. 2 lit. c DSG wird primär in einer bestimmten *«Natur und Kategorisierung von Personendaten»* verortet: Es geht um besonders schutzwürdige Personendaten oder Persönlichkeitsprofile, Art. 3 lit. c und lit. d DSG, wobei diese *Dritten* nicht bekannt gegeben werden dürfen. Art. 12 Abs. 2 lit. c DSG erklärt somit eine spezifische Verarbeitungshandlung, die *Weitergabe* von *besonders schutzwürdigen Personenangaben* oder *Persönlichkeitsprofilen an Dritte*, vgl. Art. 3 lit. c und lit. d DSG, als persönlichkeitsverletzend. Mit der Totalrevision wird das sog. Persönlichkeitsprofil fallen gelassen. Stattdessen werden das Profiling und die automatisierte Einzelfallentscheidung eingeführt, worauf nicht spezifisch eingegangen wird. Art. 30 Abs. 1 lit. c nDSG beschränkt sich neu auf besonders schutzwürdige Personenangaben i. S. v. Art. 5 lit. c nDSG.

886 Die Kategorie der sog. «besonders schutzwürdigen Personendaten» hat eine lange Tradition. Seit jeher knüpfen datenschutzrechtliche Erlasse an die Verarbeitung solcher spezifischer Personendaten erhöhte Schutzvorgaben, wobei die Kataloge sowie die hieran angeknüpften rechtlichen Konsequenzen teilweise variieren.[1159] Das DSG misst bestimmten Personendaten eine spezifische Qualität i. S. einer erhöhten Sensitivität zu, womit ein grösseres Risiko für die Beeinträch-

1159 Vgl. Art. 3 lit. c DSG und nach Totalrevision ergänzt Art. 5 lit. c Ziff. 1–Ziff. 6 nDSG; Art. 6 der Europarats-Konvention Nr. 108; zur Definierung spezifischer Personendaten, ohne von besonders schützenswerten Daten zu sprechen, Art. 4 Ziff. 13–Ziff. 15 DSGVO.

tigung der Persönlichkeit und Grundrechte korreliert wird. Folglich sieht das Gesetz besondere Schutzvorkehrungen vor.[1160] Während im öffentlichen Bereich die rechtmässige Verarbeitung einer gesetzlichen Grundlage im formellen Sinne bedarf, liefern die besonders schützenswerten Personendaten im privaten Bereich ein Anknüpfungskriterium für die Definierung der Persönlichkeitsverletzung, sofern diese Dritten weitergegeben werden. In Bezug auf die Kategorie werden mehrere Begründungsansätze und Herangehensweise beschrieben.[1161]

887 Indem das DSG nicht jede Verarbeitung qualifizierter Personendaten oder Personendatenbestände verbietet, hält es konsequent an seinem Grundsatzentscheid der prinzipiell freien Personendatenverarbeitung fest. Es rückt von diesem nur für eine spezifische *Verarbeitungshandlung, die «Bekanntgabe an Dritte», ab*. Damit vereint die Bestimmung *mehrere Facetten*:

888 Vorab findet sich das *traditionsreiche Konzept einer abstrakten und statisch angelegten Sphärentheorie*. Demnach soll bestimmten Personendaten abstrakt eine spezifische Qualität eigen sein. Gewisse Angaben gelten, wenn auch in Art. 3 lit. c DSG resp. Art. 5 lit. c nDSG aufgeführt, quasi naturgegeben und abstrakt als intim, persönlich, privat, sensitiv oder – in den Worten des DSG – «besonders schutzwürdig».[1162] Folglich implementiert das DSG für solche Angaben ein spezifisches Regime. Die *Weitergabe* von *besonders schutzwürdigen Daten* (und DSG vor seiner Totalrevision: Persönlichkeitsprofilen) an *Dritte* gilt als Persönlichkeitsverletzung.

889 In der Regelung lässt sich damit zugleich die *dynamische Dimension des Datenschutzes* nachweisen: Es geht um Datenflüsse, die einer Ordnung zuzuführen sind. Die Sichtweise ist gerade für eine Norm wie Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG bemerkenswert. *Prima vista* veranlassen die Regeln dazu, das Datensubjekt und das Objekt resp. Quasi-Objekt – die besonders schutzwürdige Personenangabe – als Anknüpfungskategorien zu sehen. Die Produktivität einer dynamischen Sichtweise für den Datenschutz, welche Personendatenflüsse in den Blick nimmt, wurde bisher an mehreren Stellen hervorgehoben – allem voran anhand der Geheimhaltungspflichten sowie dem Zweckbindungsgrundsatz. Zudem vollziehen die jüngsten datenschutzrechtlichen Neuerungen eine Abkehr von einem Konzept, welches das Datensubjekt und die Personenangabe als Quasi-Objekt ins Zentrum der Aufmerksamkeit rückt.

890 In Erinnerung gerufen seien die Erwägungen des Bundesverfassungsgerichts im Volkszählungsurteil. Es gelte zu verhindern, dass im Kontext der Volkszählung

1160 Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff., 97.
1161 Dies., a. a. O., 97 ff., 100 f., wobei die Autorin auf den öffentlichen Bereich fokussiert und attestiert, dass die Einwilligung als Surrogat einer gesetzlichen Grundlage nur in ganz engen Schranken zulässig ist.
1162 Hierzu Epiney/Hofstötter/Meier/Theuerkauf, 23 ff.

generierte Personendaten weiteren Verwaltungseinheiten zur Erfüllung ihrer Vollzugsaufgaben zufliessen. Wenn auch das Urteil den öffentlich-rechtlichen Bereich betrifft, lässt sich eine parallele Stossrichtung in Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG ausmachen: Mit der Bestimmung soll der «Übertritt» von Datenflüssen und Personendaten aus einem bestimmten Verarbeitungskreislauf bei einem bestimmten Verarbeiter, gebunden an einen bestimmten Zweck und Verarbeitungszusammenhang, in einen anderen Verarbeitungskreislauf zu einem *Dritten* beschränkt werden.

Prägend für Art. 12 Abs. 2 lit. c i. V. m. Art. 3 lit. c DSG resp. Art. 30 Abs. 2 lit. c i. V. m. Art. 6 lit. c nDSG bleibt der Abdruck der *Sphärentheorie*, obschon das DSG deren Schwächen überwinden wollte.[1163] Die Feststellung, wonach die Einteilung von Lebensäusserungen, Eigenschaften usf. in privat resp. geheim/intim und öffentlich zu kurz greife, gab einen Impetus zum Erlass spezifischer Datenschutzregulierungen. Denn die Auswertung vieler in der «Öffentlichkeit» zur Kenntnis genommener Angaben könnten zu einem Persönlichkeitsprofil verdichtet werden, woraus grundlegende Aussagen über eine Person mit entsprechenden Risiken resultieren. Diese Erkenntnis rezipiert Art. 12 Abs. 2 lit. c DSG mit seinen Schutzvorgaben betreffend *Persönlichkeitsprofile*. 891

Im Übrigen zeigt sich Art. 12 Abs. 2 lit. c DSG und Art. 30 Abs. 2 lit. c nDSG mit der Kategorie der *besonders schutzwürdigen Personenangaben* als Relikt der Sphärentheorie. Die sog. Sphärentheorie hatte sich ursprünglich zur Konkretisierung eines Persönlichkeitsgutes in Deutschland entwickelt. Sie wurde später in der Schweiz für den privatrechtlichen Bereich zur Konkretisierung von Art. 28 ZGB rezipiert.[1164] Aus zivilrechtlicher Perspektive ist es die Metapher der Zwiebel, nach welcher menschliche Lebensbereiche im Sinne konzentrischer Kreise in eine Gemeinsphäre resp. öffentliche Sphäre, eine Privatsphäre und eine Geheim- resp. Intimsphäre gegliedert werden. Das Bundesgericht bezieht sich bis heute auf dieses Konzept, neuerdings in BGE 142 III 263. Seine Regeste lautet: «Datenschutzgesetz, Art. 28 ff. ZGB; Videoüberwachung in einem Miethaus. Beurteilung der Zulässigkeit einer Videoüberwachungsanlage in einer Liegenschaft mit Mietwohnungen (E. 2).» Es ging um die Beurteilung der Zulässigkeit einer Videoüberwachung einer Mietliegenschaft in diversen Bereichen und Räumlichkeiten, unter anderem im Eingangsbereich. Die Parteien wie die Vorinstanzen erhoben die «Privatsphäre» zum Kernelement ihrer Argumentation. Die Erwägungen differenzieren hinsichtlich der Überwachung des Aussenbereichs und der Übergänge zu den Waschräumen gegenüber dem Innenbereich. Im Zusammenhang mit der Fortwirkung der Sphärentheorie über das 20. Jahrhundert hinaus ist sodann BGE 136 III 410 zu nennen: In dem Entscheid ging es um die Observation einer 892

1163 Vgl. BBl 1988 II 414 ff., 418 f.
1164 Vertiefend m. w. H. Aebi-Müller, N 512 ff.

versicherten Person durch einen Privatdetektiv, wobei das Bundesgericht mit E 2.2. auf die sog. Geheim- und Privatsphäre als Beurteilungskriterium abstellte.[1165] Illustrativ hinsichtlich der Anknüpfung auch zeitgenössischer Datenschutzbelange an die Idee des Privatsphärenschutzes – und der Ehre – ist ebenso der Beitrag von Rusch/Kummer aus dem Jahr 2015.[1166] In ihrem Aufsatz beleuchten sie die zivilrechtliche Relevanz des «forced outing». Die sexuelle Orientierung und die entsprechende Information mag als Inbegriff einer «natürlicherweise intimen» Personenangabe gelten. Folglich figurieren in Art. 3 lit. c Ziff. 3 DSG resp. Art. 6 lit. c Ziff. 3 nDSG die «Angaben über die Intimsphäre» unter den *besonders schützenswerten Personenangaben*. Auch Rusch/Kummer beziehen sich auf die Sphärentheorie als Persönlichkeitsgut i. S. v. Art. 28 Abs. 1 ZGB. Ihr gemäss werden die Geheim-, Privat-, und Öffentlichkeitssphäre abgegrenzt. Entsprechend der Zuweisung werden einer Angabe nuancierte Schutzvorgaben zugemessen. In einem Einzeiler behaupten auch Rusch/Kummer unter Berufung auf Aebi-Müller für das Datenschutzgesetz die Verbürgung eines Rechts auf informationelle Selbstbestimmung, aus dem ggf. ein Entscheidungsmerkmal für die subjektive Interpretation der Sphären gezogen werden könne. Dies ist nicht die Stelle, die erwähnten Entscheide oder das unfreiwillige Outing von Homosexualität vertieft zu analysieren. Die kurze Darstellung sollte illustrieren, inwiefern die Sphärentheorie noch heute ein Element für die Argumentation im Rahmen des (rechtlichen) Umgangs mit Personendaten ist.

893 Dass eine abstrakte Kategorisierung von Personendaten in gewöhnliche und besonders schutzwürdige sowie daran anknüpfend die Definierung der Datenschutzvorgaben nicht tragfähig ist, hielt das Bundesverfassungsgericht mit dem Volkszählungsurteil 1983 fest, indem es ausführte:

> «2. Die Verfassungsbeschwerden geben keinen Anlass zur erschöpfenden Erörterung des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite dieses Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt. Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum mehr.

1165 Die Problematik der Observation führte die Schweiz in einem sozialversicherungsrechtlichen Fall sogar vor den EGMR. In EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016 kommt der Europäische Gerichtshof für Menschenrechte (EGMR) mit 6 zu 1 Stimmen zu dem Schluss, dass die Schweiz Art. 8 der Europäischen Menschenrechtskonvention (EMRK) verletzt hat, weil im schweizerischen Recht eine hinreichend präzise rechtliche Grundlage für die Foto- und Videoüberwachung von Versicherten fehlt.

1166 Rusch/Kummer, AJP 2015, 916 ff.

> Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: […].»[1167]

Die Bedeutung des *Verwendungszusammenhanges* als einschlägiges Element zur Gestaltung datenschutzrechtlicher Vorgaben, die nicht isoliert auf den Schutz des Individuums gerichtet sind, stattdessen auch auf den Schutz gesellschaftlicher Institutionen und Kontexte mit ihren Zielen und Erwartungen, wird im letzten Teil dieser Arbeit zukunftsweisend vertieft.[1168] 894

Für Art. 12 Abs. 2 lit. c DSG lässt sich festhalten, dass er Relikte des sphärentheoretischen Konzepts aufweist. Es ist indes nicht die Verarbeitung von besonders schutzwürdigen Personenangaben per se, die eine Persönlichkeitsverletzung auslöst. Vielmehr vervollständigt erst die *Weitergabe an Dritte* den Tatbestand. Damit markiert das Gesetz, dass es zugleich der Datenfluss ist, der mitentscheidend für die datenschutzrechtliche Beurteilung ist. Die Bestimmung hat damit, ähnlich wie Art. 12 Abs. 3 DSG, einen hybriden Charakter. Entsprechend finden sich ebenso an dieser Stelle Impulse für die Entwicklung eines neuen paradigmatischen Ansatzes. Zunächst wurde gezeigt, dass eine abstrakte Definierung und Zuweisung eines gewissen Personendatums zu den «gewöhnlichen» Personendaten oder zu den besonders schützenswerten Personendaten nicht taugt: Wie Simitis für den Namen beschreibt, ist es ein Trugschluss, diesen pauschal als nicht besonders schützenswert zu taxieren – findet sich dieser auf der Liste eines Verbrecherringes ist die Verarbeitung des Namens mit hohen Risiken für die betroffene Person verbunden. Umgekehrt stammen die jeweils als besonders schützenswert definierten Personendaten stets aus einem gewissen Kontext: Es sind Angaben zur Gesundheit, zur Religion, zur Sexualität usf. Und indem die Schweiz die Weitergabe an Dritte – den Transfer – als persönlichkeitsverletzend definiert, erkennt und anerkennt das DSG, dass es nicht die abstrakte Natur einer gewissen Kategorie von Personendaten ist, die zu Risiken führt, sondern ihr Transfer in andere Bereiche. 895

3. Zusammenfassung zur Persönlichkeitsverletzung nach DSG

Es ist der Schutz der Persönlichkeit, Art. 1 (n)DSG, an welchem das DSG sein Regelungskonzept für den privaten Bereich mit Art. 12 f. DSG resp. Art. 30 ff. nDSG konsequent ausrichtet. Den Ausgangspunkt bildet für den privaten Bereich 896

1167 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 176 f.

1168 Richtungsweisend für den kontextuellen Ansatz Nissenbaum, *passim*; vgl. als Andeutung Murphy, Geo. L.J. 1996, 2381 ff., 2400 mit den Worten: «I raise the point because I believe it is related to a noneconomic justification for privacy – the concern that information can be „taken out of context" or „misused".»

die *prinzipielle Verarbeitungsfreiheit mit Schranken*. Ein grundsätzliches Verarbeitungsverbot, das von Erlaubnistatbeständen durchbrochen wird, ist dem DSG für den privaten Bereich fremd. Vielmehr setzt das DSG insofern an *qualifizierten Verarbeitungshandlungen* an, wobei die persönlichkeitsverletzenden Personendatenverarbeitungen mit Art. 12 Abs. 2 DSG resp. Art. 30 Abs. 2 nDSG durch ein differenziertes Instrumentarium konkretisiert werden. Auf den vorangehenden Seiten wurden die Verarbeitungshandlungen beleuchtet, die das DSG explizit, wenn auch nicht abschliessend, vgl. Ingress zu Art. 12 DSG und Art. 30 nDSG, als *persönlichkeitsverletzend* definiert. Während in Abs. 2 lit. a–c drei Konstellationen vom Gesetzgeber als Persönlichkeitsverletzung vordefiniert werden, ist bis heute nicht abschliessend geklärt, welche weiteren Rechtsverstösse eine Persönlichkeitsverletzung begründen.

897 *E contrario* wurden vorab zwei Hauptgruppen von Verarbeitungshandlungen umrissen, die *unterhalb* der Demarkationslinie zur Persönlichkeitsverletzung liegen. Erstens diejenigen, welche die allgemeinen Verarbeitungsgrundsätze einhalten, vgl. Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Zweitens gelten nach Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Verarbeitungen von Personendaten, die das Datensubjekt selbst allgemein zugänglich gemacht hat, nicht als persönlichkeitsverletzend, sofern das Datensubjekt die Verarbeitung nicht ausdrücklich untersagt hat. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG lässt sich als Hybrid bezeichnen, der Aspekte der Sphärentheorie wie die Idee einer Selbstbestimmung inkludiert. Die Verarbeitung von Personendaten, die das Subjekt selbst allgemein zugänglich gemacht hat, beurteilt das Gesetz als grundsätzlich nicht persönlichkeitsverletzend, es sei denn, es läge ein Verbot durch das Datensubjekt vor. Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG ist in verschiedener Hinsicht problematisch. Konzeptionell liegt sein Defizit darin, dass er der dichotomen Vorstellung von öffentlich versus privat verhaftet bleibt. Eine Vorstellung, wonach im Internet zugänglich gemachte Personendaten gewissermassen öffentlich sind und folglich dem Datenschutz weitgehend entzogen werden, ist nicht haltbar.

898 In Bezug auf die *qualifizierten und damit persönlichkeitsverletzenden Verarbeitungshandlungen* wurde *Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG*, welcher die Verletzung der allgemeinen Verarbeitungsgrundsätze als persönlichkeitsverletzend taxiert, als Verbürgung eines *Integritätsschutzes* beschrieben. Die Tatbestandsmässigkeit der Persönlichkeitsverletzung wird objektiv bestimmt, die Qualifizierung der Eingriffsintensität liegt in der Verletzung der allgemeinen Verarbeitungsgrundsätze. Letztere lassen sich als Mindestanforderungen der fairen Personendatenverarbeitung beschreiben. Ihre Einhaltung resp. Verletzung markiert die Grenze resp. Schranke zur persönlichkeitsverletzenden Personendatenverarbeitung. Mit dieser Grundsatzregelung wird kein System informa-

tioneller Selbstbestimmung, das von einem prinzipiellen Verarbeitungsverbot ausgeht und in dem die allgemeinen Verarbeitungsgrundsätze eine zweite Schranke bilden, vorgesehen. Die jüngsten rechtlichen Neuerungen reagieren u. a. auch auf die ungenügende Griffigkeit generalklauselartiger Datenschutzvorgaben in der Praxis. Sie ergänzen die deliktsrechtliche Fokussierung des persönlichkeitsrechtlich basierten Datenschutzrechts, indem neu an erster Stelle die Verantwortlichen durch verschiedene konkrete Umsetzungsinstrumente sowie Dokumentations- und Rechenschaftspflichten früher und nachdrücklicher in die Pflicht genommen werden. Insofern wird ein Perspektivenwechsel vollzogen, wobei der Fokus von der deliktsrechtlichen, abwehrrechtlichen Konzeption einer Persönlichkeitsverletzung abgewendet und die Einhaltung der Datenschutzvorgaben zu einer genuinen und primären Aufgabe der Verarbeitenden wird. Neue organisatorische und prozedurale Instrumente ergänzen das bislang im Persönlichkeitsschutz basierte materielle Datenschutzrecht. Damit soll dieses faktisch effektuiert werden. Die Einhaltung des Datenschutzrechts wird zu einer Compliance- und Governance-Aufgabe.[1169]

899 *Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG* implementiert eine *Widerspruchslösung*. Der Tatbestand integriert ein subjektives Kriterium. Mit dem Widerspruch wird der von Gesetzes wegen geltende Ausgangspunkt der prinzipiell freien Personendatenverarbeitung für den Einzelfall umgekehrt. Das durch Widerspruch begründete Verarbeitungsverbot kann indes durch überwiegende Interessen der Verantwortlichen übertrumpft werden. Die Bestimmung wurde deshalb als Ansatz eines Autonomieschutzes bezeichnet. Es handelt sich um ein relatives *opt-out im weiteren Sinne*. Die Widerspruchslösung ist kongruent für ein System mit prinzipieller Verarbeitungsfreiheit. Von einem Recht auf informationelle Selbstbestimmung zu sprechen, das untrennbar mit dem Volkszählungsurteil des Bundesverfassungsgerichts assoziiert wird, vermag auch im Lichte dieser Bestimmung des DSG nicht zu überzeugen. Ebendies erhärtete ein vergleichender Blick auf das Transplantationsrecht.

900 Zu *Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c nDSG* wurde festgestellt, dass auch dieser Tatbestand an die qualifizierte Verarbeitung anknüpft. Hierbei begründet insb. die Weitergabe von besonders schutzwürdigen Personenangaben an Dritte eine Eingriffsintensität, welche die Persönlichkeitsverletzung des Datensubjektes markiert. Die Bestimmung zeigt Relikte der Sphärentheorie, indem sie an in abstrakter Weise kategorisierte, besonders schutzwürdige Personendaten anknüpft. Die Einschlägigkeit des Verarbeitungszusammenhanges für die Gestaltung der datenschutzrechtlichen Vorgaben wird damit nicht hinreichend anerkannt. Dennoch deutet sich in Art. 12 Abs. 2 lit. c DSG resp. Art. 30 Abs. 2 lit. c

1169 Vgl. dritter Teil, VIII. Kapitel, A.2.6.; insofern insb. auch Art. 24 DSGVO.

nDSG eine *dynamische und potentiell systemische datenschutzrechtliche Betrachtungsweise* an. Angesetzt wird am Transfer von qualifizierten Personendaten an Dritte. Weil in der Norm gleichzeitig Relikte der Sphärentheorie wie auch Elemente ihrer Überwindung angelegt sind, hat sie einen hybriden wie transformativen Charakter.

901 Die Analyse des persönlichkeitsrechtlichen Regelungsregimes des DSG ergab, dass es stets darum ging, die Demarkationslinie zu konkretisieren, wobei es qualifizierte Verarbeitungshandlungen sind, die als Persönlichkeitsverletzung taxiert werden. Das DSG ist damit in seinen Kernbestimmungen im privaten Bereich konsequent dem *abwehr-, deliktsrechtlich und individualrechtlich konzipierten Persönlichkeitsrecht* verpflichtet. Die datenschutzrechtlichen Neuerungen liefern indes eine markante Ergänzung, indem zahlreiche neue Instrumente den Datenschutz weiter auf organisatorische und prozedurale Instrumente umlagern.

902 Datenverarbeitungen, welche die Qualifizierung als persönlichkeitsverletzend erlangen, ziehen die Frage nach der *Widerrechtlichkeit resp. Rechtfertigung* nach sich. Entsprechend der für das Persönlichkeitsrecht entwickelten Dogmatik begründet die Verletzung eines absolut geschützten Rechtsgutes die Widerrechtlichkeit; diese kann allerdings im Falle des Vorliegens eines *Rechtfertigungsgrundes* entfallen.[1170] Nachfolgend wird auf die einzelnen Rechtfertigungsgründe eingegangen, wobei der rechtfertigenden Einwilligung besonderes Augenmerk gilt. Im Ergebnis kann aufgrund der fundierten Betrachtung des Rechtfertigungssystems eine noch präzisere Charakterisierung des DSG für den privaten Sektor erfolgen. Es geht an dieser Stelle nicht darum, eine weitere Theorie beispielsweise zur Frage, ob die Rechtfertigungsgründe tatbestandsausschliessend oder rechtfertigend wirken, anzufügen.[1171] Ebenso wenig geht es um eine grundsätzliche Analyse der Rechtfertigungsgründe. Vielmehr sollen diese spezifisch hinsichtlich ihrer Funktion im Datenschutzrecht beleuchtet werden, um hieraus Anhaltspunkte zur Gestaltung eines wirksamen Datenschutzrechts zu gewinnen.

4. Rechtfertigungsregime gemäss DSG

4.1. Ausgangslage – Text- und Wertungsdifferenzierung

903 Einleitend ist auf die Diskrepanz in der Gesetzesredaktion mit Blick auf die noch in Kraft stehende Version des DSG und die Erwähnung des Rechtfertigungsmechanismus einzugehen. Ebendiese wird zwar mit der Totalrevision bereinigt, indem Art. 30 Abs. 2 und Abs. 3 nDSG konsequent nur die persönlichkeitsverletzende Verarbeitung adressieren. Die Rechtfertigungsgründe werden einzig in

1170 Vgl. Art. 13 DSG.
1171 Vgl. Haas, 33 ff.; grundlegend zur Einwilligung im Privatrecht Ohly, *passim*.

Art. 31 nDSG niedergelegt. Dennoch sind die Ausführungen zum bisherigen DSG aufschlussreich, auch für die Zeit nach dem Inkrafttreten der Totalrevision.

Art. 12 Abs. 2 lit. a DSG und Art. 12 Abs. 3 DSG sehen bei ihrer Umschreibung des Tatbestandes der Persönlichkeitsverletzung durch Datenverarbeitung die Möglichkeit einer Rechtfertigung nicht vor. Dagegen verweisen Art. 12 Abs. 2 lit. b und lit. c DSG explizit auf diese. Als Rechtfertigung fungieren die Einwilligung, überwiegende private oder öffentliche Interessen sowie gesetzliche Rechtfertigungsgründe, vgl. Art. 13 DSG und Art. 28 Abs. 2 ZGB. Wie allerdings sind diese gesetzgeberischen Differenzen zu verstehen? Die Frage hat während längerer Zeit die datenschutzrechtliche Auseinandersetzung absorbiert. In die Sprache der Methodenlehre übersetzt, handelt es sich um eine Auslegungsfrage. Klärungsbedürftig ist, ob es sich um eine echte Lücke, qualifiziertes Schweigen oder ein redaktionelles Versehen handelt. Bevor Art. 12 Abs. 2 DSG mit der Teilrevision von 2008 angepasst wurde, lautete Art. 12 Abs. 2 lit. a DSG: «Er darf insbesondere nicht ohne Rechtfertigungsgrund Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten.» In der geltenden Fassung lautet Art. 12 Abs. 2 lit. a DSG, Stand 1. Januar 2008: «Er darf insbesondere nicht Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten.» 904

Über die Bedeutung der Streichung der Passage «ohne Rechtfertigungsgrund» entbrannte eine intensive Debatte: Der EDÖB verortete darin, dass die Rechtfertigungsgründe aus dem Text von Art. 12 Abs. 2 lit. a DSG gestrichen wurden, nicht aber aus lit. b und ebenso wenig aus lit. c, eine datenschutzrechtliche *Stärkung*. Er vertrat infolge der differenzierenden Formulierungen in den drei Literae, dass Verstösse gegen Datenbearbeitungsgrundsätze nach der damaligen Teilrevision *nicht* mehr rechtfertigungsfähig wären.[1172] Anders die Position eines namhaften Teils der Lehre.[1173] Das Bundesamt für Justiz sah sich in der Folge veranlasst, am 10. Oktober 2006 eine Auslegungshilfe zu publizieren: Es interpretierte den Willen des Gesetzgebers dahingehend, dass eine Rechtfertigung von Persönlichkeitsverletzungen infolge Verletzung der Bearbeitungsgrundsätze nicht grundsätzlich ausgeschlossen sei. Vielmehr habe der Gesetzgeber verdeutlichen wollen, dass die Rechtfertigung von Verstössen gegen die enumerierten Grundsätze nicht vorschnell angenommen werden dürfe.[1174] Dieser Auslegung folgte das Bundesgericht in BGE 136 II 508, dem sog. *Logistep-Entscheid vom 8. September 2010*. Es hielt fest, dass *entgegen dem Wortlaut* von Art. 12 Abs. 2 lit. a DSG auch für die hier bezeichneten Konstellationen eine *Rechtfertigung* denkbar 905

1172 BGE 136 II 508, E 5.2. und E 6.3.

1173 Immerhin sei angemerkt, dass es sich bei den Schreibenden zum grossen Teil um praktizierende Anwälte in internationalen Wirtschaftskanzleien handelt.

1174 Vgl. Auslegungshilfe des BJ vom 10. Oktober 2006, Ziff. 3.1.

sei. Allerdings dürfe dies *nur mit grosser Zurückhaltung* angenommen werden.[1175] Im konkreten Fall beurteilte das Bundesgericht vorab IP-Adressen als personenbezogene Daten i. S. v. Art. 3 lit. a DSG. Sie wurden gesammelt, um eine Urheberrechtsverletzung verfolgbar zu machen. Da allerdings das Zusammentragen der Daten über P2P-Netzwerkteilnehmer für diese nicht erkennbar war, sah das Gericht darin eine Verletzung der Grundsätze der Erkennbarkeit sowie der Zweckbindung gemäss Art. 4 Abs. 3 und Abs. 4 DSG. Die damit begangene Persönlichkeitsverletzung beurteilte das Bundesgericht als widerrechtlich und *verneinte* das Vorliegen eines rechtfertigenden überwiegenden privaten oder öffentlichen Interesses.[1176] BGE 138 II 346, das sog. Google-Street-View-Urteil, bestätigte die zurückhaltende Zulassung von Rechtfertigungsgründen im Anwendungsbereich von Art. 12 Abs. 2 lit. a DSG: Zwar sei ein Verstoss gegen die Grundsätze von Art. 4, Art. 5 Abs. 1 und Art. 7 DSG gemäss Art. 12 Abs. 2 lit. a DSG als Persönlichkeitsverletzung zu taxieren, eine Rechtfertigung sei entgegen dem Wortlaut der Norm dennoch nicht ausgeschlossen. Sie dürfe indes nur äusserst zurückhaltend angenommen werden.[1177] Die Teilrevision des DSG von 2008, bei der aus Art. 12 Abs. 2 lit. a DSG der Passus «ohne Rechtfertigungsgrund» gestrichen wurde, änderte mithin an der Rechtslage – so das Bundesgericht und das Bundesamt für Justiz – nichts oder wenig: Der Gesetzgeber habe «nicht grundsätzlich vom heutigen System abweichen» wollen. Immerhin wurde eine Nuancierung anerkannt, indem Rechtfertigungsgründe bei Verletzungen der allgemeinen Verarbeitungsgrundsätze zwar nicht generell ausgeschlossen, aber doch nur ausnahmsweise denkbar seien. Damit wird die Bedeutung der allgemeinen Verarbeitungsgrundsätze als *minimal standard* der fairen Personendatenverarbeitung unterstrichen.

906 Mit der Totalrevision wird der Gesetzestext entsprechend angepasst, vgl. Art. 30 nDSG. In sämtlichen die Persönlichkeitsverletzung umschreibenden Tatbeständen gemäss lit. a–c wird auf eine Thematisierung der Rechtfertigungsgründe verzichtet. Sie werden in Art. 31 nDSG geregelt. Die Totalrevision sieht folglich eine Bereinigung dergestalt vor, dass sie für sämtliche persönlichkeitsverletzenden Handlungen, auch diejenigen entgegen den Grundsätzen, die Rechtfertigung zulässt, was in konsequenter Weise die Umsetzung des Systems von Art. 28 ff. ZGB darstellt.

907 Ob an der Auslegung, wonach Rechtfertigungsgründe *bei Verletzungen der allgemeinen Bearbeitungsgrundsätze zurückhaltend zuzulassen sind*, festgehalten wird, wird sich erst weisen. M. E. sprechen hierfür gewichtige Argumente: Vorab

1175 Vgl. BGE 136 II 508, Regeste und E 5; entsprechend auch EDÖB, Schlussbericht PostFinance, 6, 23.
1176 BGE 136 II 808, E 6.
1177 BGE 138 II 364, E 7.2.

handelt es sich bei der Präzisierung, wonach erhöhte Anforderungen an die Stichhaltigkeit von Rechtfertigungsgründen zu verlangen sind, um eine gefestigte Praxis. Ein Abweichen hiervon scheint mit der Neufassung des DSG nicht beabsichtigt und die Praxisänderung müsste entsprechend gut begründet sein. Hinzu tritt ein gewichtiges materiellrechtliches Argument: Der Ansatz, wonach die allgemeinen Bearbeitungsgrundsätze die bedeutsamste Schranke der prinzipiell freien Datenbearbeitung im privaten Bereich definieren, wurde als *Integritätsschutz* bezeichnet. Er implementiert Mindestanforderungen an faire resp. nicht missbräuchliche Personendatenverarbeitungen. Insofern lassen sie sich als Minimalstandard beschreiben, dessen Verletzung – weil es sich um Basiselemente einer Integritätsgesetzgebung handelt – *nur ausnahmsweise gerechtfertigt* werden soll. Namentlich das überwiegende private Interesse (i. d. R. als wirtschaftliches Interesse), das allzu gerne und leicht ins Feld geführt wird, sollte restriktiv zugelassen werden. Entsprechend wird hier dafür plädiert, dass die Zurückhaltung bei der Anerkennung von Rechtfertigungsgründen bei der Konstellation der Persönlichkeitsverletzung gemäss Art. 30 Abs. 2 lit. a nDSG weiterhin gilt. Aus der Eliminierung der Rechtfertigungsverweise aus sämtlichen Literae resultiert keine Nivellierung in der Zulassung von Rechtfertigungsgründen.

908 Erhärtet wird die Begründung für diese Interpretation wegen der *systemischen Dimension des Datenschutzrechts*. Die Einhaltung der Bearbeitungsgrundsätze gemäss Art. 4 ff. DSG resp. Art. 6 und Art. 8 nDSG resp. deren Verletzung hat *nicht* nur eine individual- und subjektivrechtliche Dimension. Wie anhand des Zweckbindungsgrundsatzes herausgearbeitet wurde, zielen diese wie das Datenschutzrecht im Allgemeinen zugleich darauf ab, die *Angemessenheit von Datenflüssen* zu steuern. Dazu gehört, dass ein Datenfluss in einem bestimmten Flussbett verläuft und dieses nicht resp. nur unter Einhaltung bestimmter Vorgaben verlässt, und dass Personendaten nicht zu einem anderen Zweck in ein anderes Flussbett umgeleitet werden. Damit wird, über den Schutz des Subjektes hinaus, der Schutz der Integrität von Systemen und Subsystemen gewährleistet.[1178] Einen Verstoss gegen den Zweckbindungsgrundsatz als Kernprinzip der allgemeinen Verarbeitungsgrundsätze aufgrund primär individual- und subjektivrechtlich geprägter Interessen der Datenverarbeitenden zu rechtfertigen, bedeutet nichts anderes, als einen elementaren datenschutzrechtlichen Ansatz, dessen vollständiger Bedeutungsgehalt indes bislang nur ungenügend zur Kenntnis genommen wurde, auszuhöhlen.

909 Indem die Verarbeitungsgrundsätze einen *materiellrechtlichen Mindeststandard* gewährleisten und *nicht nur dem Subjektschutz, sondern auch dem Systemschutz* dienen, sollen rein individuell ausgerichtete Eigeninteressen der verarbeitenden

1178 Richtungsweisend für eine solche Konzeption die Beiträge von Nissenbaum.

Stellen als Rechtfertigung von grundsatz- und damit persönlichkeitsverletzenden Verarbeitungshandlungen nur angenommen werden, wenn die Integrität der jeweiligen Bereiche, in welche die Personendatenverarbeitungen eingebettet sind, dennoch gewahrt wird. Gerade die Rechtfertigung von Verstössen gegen datenschutzrechtliche Minimalstandards, die in einem System mit grundsätzlicher Verarbeitungsfreiheit – anders als im System des prinzipiellen Verarbeitungsverbots – die einzige Schranke definieren, sollte auch in der totalrevidierten Fassung weiterhin zurückhaltend zugelassen werden.

910 Weitere gewichtige Fragen zu den Rechtfertigungsgründen, die einen Einfluss auf die Steuerungswirkungen und das Schutzniveau im Datenschutzrecht haben, sind damit nicht geklärt: Eine Kernfrage ist, ob ebenso bei den Tatbeständen von Art. 12 Abs. 2 lit. b und lit. c DSG Zurückhaltung geboten ist. Offen ist sodann, ob persönlichkeitsverletzende Verarbeitungen nach Art. 12 Abs. 3 DSG, wenn das Datensubjekt die Verarbeitung von zuvor allgemein zugänglich gemachten Personendaten ausdrücklich verbietet, namentlich durch überwiegende Interessen gerechtfertigt werden kann oder ob der Widerspruch als eine Art Vorrecht zur unüberwindbaren Schranke der Verarbeitung wird. Der Tatbestand äussert sich hierzu, ähnlich wie Art. 12 Abs. 2 lit. a DSG, nicht. Die Zulassung von Rechtfertigungsgründen für diesen Tatbestand entspräche der Regelung von Art. 12 Abs. 2 lit. b DSG. Letztere Bestimmung lässt eine Bearbeitung gegen den Widerspruch der Person zu, sofern ein Rechtfertigungsgrund vorliegt. Die Regelungsmechanismen weisen denn auch Parallelen auf. Allgemein entspricht eine generelle Rechtfertigungsmöglichkeit persönlichkeitsverletzender Handlungen dem Konzept von Art. 28 ZGB. In Anbetracht dieser Ausgangslage scheint die Zulassung von gesetzlichen Rechtfertigungsgründen ausser Frage zu stehen. Die Herausforderung allerdings liegt in der Koordination des eine Verarbeitung verbietenden Willens des Datensubjektes mit Interessen der Verarbeitenden. Der Wille in Gestalt des Widerspruches des Datensubjektes kann nicht prinzipiell das einzige und allein ausschlaggebende Kriterium für die Unzulässigkeit einer Personendatenverarbeitung sein. Ebenso wenig allerdings sind Interessen der Verarbeitenden (oft wirtschaftliche Interessen) per se geeignet, einen Entscheid des Datensubjektes zu übertrumpfen. Denn stets ist ebenso zu berücksichtigen, dass der Datenschutz nicht nur eine individualrechtliche, sondern auch eine systemische Schutzdimension aufweist. Letztere wird uns vertieft im dritten Teil dieser Arbeit beschäftigen.

911 Eine Kernherausforderung zeigt sich somit in der Koordination des Willens des Datensubjektes mit den von den verarbeitenden Stellen angerufenen überwiegenden eigenen Interessen.[1179] Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG führen

1179 Vgl. in diesem Zusammenhang auch Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 33 ff und N 44 ff.; zum Facettenreichtum dieser Interessen, wobei hierbei sehr oft

einen Katalog von Konstellationen auf, in denen potentiell ein überwiegendes Interesse der Verarbeitenden angenommen wird.

Eine interessante Lösung hat sich im Rahmen der DSGVO herausgebildet. Im Rahmen ihres grundsätzlichen Verarbeitungsverbotes mit Erlaubnistatbeständen, vgl. Art. 6 DSGVO, soll im Kontext des sog. Direktmarketing folgende Mechanik gelten: Das nicht qualifizierte Direktmarketing kann prinzipiell über das *legitimate interest* datenverarbeitender Verantwortlicher erlaubt sein; eine Einwilligung wird für den fraglichen Verarbeitungszweck und die entsprechende Verarbeitungstätigkeit nicht generell vorausgesetzt. Sofern allerdings ein Datensubjekt einen Widerspruch einlegt, ist die Personendatenverarbeitung zu Marketingzwecken *endgültig verboten*.[1180] 912

Umgekehrt steht ausser Frage, dass Personendatenverarbeitungen aus bestimmten Gründen ungeachtet des Willens des Datensubjektes zulässig sind: Bereits aus dem Anwendungsbereich von Art. 28 ZGB ist die Situation bekannt, wonach aufgrund überwiegender Informationsinteressen ein Bericht in der Presse veröffentlicht wird, selbst wenn keine Einwilligung resp. kein Widerspruch vorliegt.[1181] Vor diesem Hintergrund sollten auch für die Konstellation von Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 3 nDSG Verarbeitungen entgegen einem Widerspruch des Datensubjektes – wenn auch zurückhaltend resp. aus gewichtigen Gründen – zulässig sein (hierzu vertiefend sogleich). Damit wird Kongruenz zur Interpretation von Art. 12 Abs. 2 lit. b DSG resp. Art. 30 Abs. 2 lit. b nDSG geschaffen. Ein solcher Auslegungsentscheid wird untermauert vom Grundsatzentscheid des DSG für den privaten Sektor mit seiner prinzipiellen Verarbeitungsfreiheit. Zusammenfassend ist für Art. 12 Abs. 3 DSG eine analoge Interpretation, wie sie für Art. 12 Abs. 2 lit. a DSG vom Bundesamt für Justiz sowie vom Bundesgericht formuliert wurde und die eine parallele Regelung in Art. 12 Abs. 2 lit. b DSG findet, anzunehmen. 913

Ob für die datenschutzgesetzlichen Tatbestände der Persönlichkeitsverletzung allgemein und auch nach Totalrevision Zurückhaltung in Bezug auf die Zulassung von Rechtfertigungsgründen angezeigt ist, ist damit nicht abschliessend geklärt. Namentlich das überwiegende Interesse der Verarbeitenden stellt ein neuralgisches Element für die Gewährleistung eines effizienten Datenschutzrechts dar. Dies gilt *a fortiori* für die Schweiz in ihrem DSG für den privaten Bereich, wo 914

---

wirtschaftlich motivierte Effizienzerwägungen im Vordergrund stehen, allerdings auch weitere Interessen auszumachen sind, dritter Teil, IX. Kapitel.

1180 Hierzu ebenso Art. 21 Abs. 2 und Art. 6 lit. f DSGVO; DSGVO ErwG 47; Buchner/Petri, Beck-Komm.-DSGVO, Art. 6 N 176; vgl. auch Helfrich, NomosKomm-DSGVO, Art. 21 N 44; Datenschutzkonferenz DSK, Kurzpapier Nr. 3 vom 29. Juli 2017, 1 ff.; WP 29/217, legitimate interests, 18 ff.

1181 Vgl. BGE 143 III 297, E 6.3.; BGE 127 III 481, E 3; zum Entscheid und den Figuren der absoluten und relativen Person der Zeitgeschichte auch Vogt/Wiget, in: Arter/Jörg (Hrsg.), 129 ff., 150 f.

aufgrund des Ausgangspunktes und der Konstruktion, wonach erst qualifizierte Verarbeitungen eine Persönlichkeitsverletzung begründen, materiellrechtlich ein niedriges Schutzniveau vorgesehen wird. Ebendieses kann immerhin gehalten werden, wenn die Rechtfertigungsgründe für sämtliche Tatbestände der datenschutzgesetzlichen Persönlichkeitsverletzung und nicht nur für Art. 12 Abs. 2 lit. a DSG restriktiv eröffnet werden. Umgekehrt führt die grosszügige Zulassung von Rechtfertigungsgründen auch für Art. 12 Abs. 2 lit. b, lit. c und Art. 12 Abs. 3 DSG zu einer weiteren substantiellen Absenkung des Schutzes der Datensubjekte in ihrer Persönlichkeit.

915 Ebendies sollte, wie zu zeigen sein wird, insb. nicht allein aus überwiegenden wirtschaftlichen Interessen der Verarbeitenden zugelassen werden. Vielmehr sollten *kontextuelle Erwägungen* ein Kernelement der Evaluation bilden.[1182] Nach diesen grundlegenden strukturellen Erwägungen ein kurzer Blick auf die einzelnen Kategorien von Rechtfertigungsgründen bei persönlichkeitsverletzenden Verarbeitungshandlungen durch Private. Das Regime entspricht vor wie nach Totalrevision des DSG demjenigen von Art. 28 ZGB.

4.2. Gesetzliche Rechtfertigungsgründe

916 Die *gesetzlichen Rechtfertigungsgründe* bereiten theoretisch wie praktisch wenig Schwierigkeiten. Es ist der Gesetzgeber, der hier die Gewichtung und Abwägung vornimmt. Gesetzliche Bearbeitungspflichten und -rechte, die als Rechtfertigungsgründe für persönlichkeitsverletzende Personendatenverarbeitungen figurieren, finden sich in einer Vielzahl von Erlassen.[1183] Exemplarisch zu nennen sind Aufklärungs- und Bearbeitungspflichten gemäss Art. 3 ff. des Geldwäschereigesetzes oder Art. 28 ff. des Konsumkreditgesetzes, die Aufbewahrungspflicht gemäss Art. 985 OR, Offenlegungspflichten nach Gesellschaftsrecht, Art. 663c OR, oder gemäss Art. 20 und Art. 31 des Börsengesetzes, Auskunftspflichten, Zeugnispflichten usf.; erwähnenswert ist ebenso Art. 384 Abs. 1 ZGB.

917 Wiederum ist eine Reflexion im Lichte des Grundsatzentscheides für den Ausgangspunkt angezeigt: Bei einem System mit prinzipiellem Verarbeitungsverbot greift die Notwendigkeit eines Erlaubnisvorbehaltes in einem Gesetz auf «oberster Stufe» und für «gewöhnliche», sprich «jede» resp. «nicht qualifizierte» Verarbeitung. Anders im System der grundsätzlichen Verarbeitungsfreiheit mit Schranken, wie sie das DSG für den privaten Bereich vorsieht: Die gesetzliche Grundlage liefert im System der prinzipiellen Verarbeitungsfreiheit einen Rechtfertigungsgrund für qualifizierte, sprich persönlichkeitsverletzende Verarbeitungshandlungen. Trotz dieser Differenz verwebt sich in beiden Systemen über die Gesetzes-

1182 Vertiefend insofern dritter Teil, IX. Kapitel.
1183 Eine gute Übersicht bietet Rampini, BSK-DSG, Art. 13 N 18.

grundlage das allgemeine Regime mit einem jeweils spezifischen Regime, das Kontexten, Systemen usf. Rechnung trägt. Über die gesetzlichen Rechtfertigungsgründe, die nach DSG persönlichkeitsverletzende Verarbeitungshandlungen zu rechtmässigen Handlungen machen, vgl. Art. 13 DSG und Art. 31 nDSG werden namentlich *Spezialgesetzgebungen und sektor- oder branchenspezifische Erlasse* einschlägig. Die gesetzlichen Rechtfertigungsgründe sind damit gleichzeitig ein wichtiges und konkretes Instrumentarium zur *Gestaltung von Datenflüssen* sowie zur Koordinierung von verschiedenen Verarbeitungszusammenhängen, -kontexten sowie -prozessen. Insofern lassen sich die gesetzlichen Rechtfertigungsgründe als *Brücken* oder *Koordinationsstellen* bezeichnen. Die allgemeine Datenschutzgesetzgebung für den privaten Sektor wird damit an der Stelle der gesetzlichen Rechtfertigungsgründe neuerdings als *Teilordnung des Datenschutzrechts* positioniert. Sie ist, wie anhand des Rechtmässigkeitsprinzips dargestellt, in ein ausdifferenziertes Netz von weiteren Erlassen eingebettet.[1184] Anhand der gesetzlichen Rechtfertigungsgründe präsentiert sich der private Bereich des DSG erneut nicht als einheitlicher, monolithischer Bereich. Vielmehr konstituiert sich dieser sog. Privatbereich aus pluralen Subsystemen, wobei über die *gesetzlichen Rechtfertigungsgründe kontextspezifische Erwartungen*, die der Gesetzgeber für spezifische Regulierungsbereiche anerkannt hat, in das allgemeine Datenschutzregime integriert werden.

An dieser Stelle, an welcher der Fokus auf die Rechtfertigung einer Persön- 918
lichkeitsverletzung im Rahmen des Individualgüterrechtsschutzes gerichtet ist, bestätigt sich die systemische und dynamische Facette des Datenschutzrechts. Sie verändert eine Sicht, welche das Datensubjekt und das Personendatum als Quasi-Objekte ins Visier nimmt. Über die Rechtfertigungsgründe qua Gesetz werden Personendatenflüsse und -verarbeitungsprozesse innerhalb und zwischen verschiedenen Verarbeitungszusammenhängen und -kontexten als Gegenstand datenschutzrechtlicher Regulierung sichtbar.[1185] Auch anhand der gesetzlichen Rechtfertigungsgründe lässt sich selbst im schweizerischen DSG mit seiner konsequenten Anknüpfung im zivilrechtlichen Persönlichkeitsschutz eine Regelungskonzeption freilegen, die den Fluss von Personendaten normiert, die Flussbetten sowie das Delta in den Blick nehmen. Ladeur hat für dieses Delta den Begriff des *Knotenpunktes* geprägt und dessen Relevanz für den Datenschutz betont.[1186] Anhand der gesetzlichen Rechtfertigungsgründe zeigt sich – auch wenn diese

1184 Hierzu zweiter Teil, V. Kapitel, B.1.

1185 Eine solche Sichtweise wurde namentlich anhand des Zweckbindungsgrundsatzes herausgearbeitet, zweiter Teil, V. Kapitel, B.4.

1186 Ladeur, Vortrag, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021); eine solche Perzeption drängt sich gerade auch mit Blick auf das Internet auf mit seiner netzwerkartigen und konnexionistischen Struktur, Vesting, in: Ladeur (Hrsg.), 155 ff., 162 f.

prima vista einzig und allein der konkreten Rechtfertigung einer spezifischen Persönlichkeitsverletzung dienen –, dass es gerade nicht isoliert um den Schutz der Persönlichkeit des Datensubjektes und allfälliger individueller Interessen der Verarbeitenden geht. Vielmehr werden dem Grundsatz nach persönlichkeitsverletzende Personendatenverarbeitungen *von Gesetzes wegen* gerechtfertigt, wobei bereichs-, kontext-, systemspezifische Erwartungen verfolgt und adressiert werden. Sie zielen darauf ab, die in den spezifischen Bereichen einschlägigen Ziele und Zwecke zu gewährleisten.

919 Eine solche Betrachtungsweise der gesetzlichen Rechtfertigungsgründe macht die *Relevanz der jeweiligen Rollen der Akteure* im *jeweiligen Verarbeitungskontext* sichtbar, wie sie selbst für das Datenschutzgesetz als Querschnittsgesetz einschlägig ist.[1187] Massgeblich ist im Rahmen der Verarbeitungsprozesse und der Prüfung allfälliger Rechtfertigungsgründe für persönlichkeitsverletzende Handlungen zum einen, ob die verarbeitende Person als *Arbeitgeber*, als *Kreditinstitut* resp. Finanzdienstleistungen anbietendes Institut, als *Verwaltungsrat*, als *Ärztin* usf. Personendaten verarbeitet. Zum anderen scheint das DSG selbst grob geschnitzt von der «Persönlichkeit», der natürlichen Person, dem Individuum für den «privaten Sektor» auszugehen.[1188] Das betroffene Datensubjekt erscheint auf den ersten Blick als eine «fixe und einheitliche Figur». Anhand der gesetzlichen Rechtfertigungsgründe allerdings zeigt sich dieses Subjekt in seinem Facettenreichtum und seinem «changierenden» Charakter. Es nimmt differenzierte Rollen ein, womit es auch datenschutzrechtlich um eine Persönlichkeit geht, die gewissermassen und wiederum «ausdifferenziert» anhand ihrer Rollen agiert. Es geht darum, dass eine persönlichkeitsverletzende Verarbeitungshandlung gegenüber einer Patientin, einem Versicherungsnehmer, einer Anlegerin usf. aufgrund einer gesetzlichen Grundlage gerechtfertigt werden kann. Mit anderen Worten wird ein *Konnex* zwischen einem vorab aufgrund des Querschnittsgesetzes des DSG als fix und undifferenziert beschriebenen Datensubjekt («Einheitssubjekt», «Persönlichkeit») und einem in ähnlicher Weise nicht nuanciert wahrgenommenen «Verarbeiter» zu den jeweils im Hintergrund stehenden und einbettenden Handlungsbereichen hergestellt. Im Rahmen der Geheimhaltungspflichten wurde zur Beschreibung dieser Ausgangslage der Begriff der *Akzessorietät* vorgeschlagen. Weiter gedacht heisst dies, dass beispielsweise die Weitergabe von

1187 Früh zur Ausdifferenzierung von Gesellschaftssystemen und zur Relevanz von hieran anknüpfenden Rollen auch für das Datenschutzrecht Mallmann, 36 ff.

1188 Für den öffentlichen Bereich wird grob vom «Bundesorgan» und von der «Bürgerin» ausgegangen, wobei hierbei das Legalitätsprinzip und die Notwendigkeit einer spezifischen gesetzlichen Grundlage Ausdifferenzierungen für den öffentlichen Bereich bringen, der ebenso wenig ein einheitlicher Bereich ist, sich stattdessen aus pluralen Unterbereichen konstituiert. Das Bundesverfassungsgericht hat dies mit seinem Volkszählungsurteil und seinen Erwägungen zum Zweckbindungsgrundsatz sichtbar gemacht; aufschlussreich zu Teilbereichen innerhalb der Persönlichkeit, die ihrerseits Systeme abbilden, Fried, Yale L.J. 1968, 475 ff., 478.

Gesundheitsangaben über eine Person an eine bestimmte Stelle durch einen Arzt, der grundsätzlich dem Arztgeheimnis untersteht, für den Fall von ansteckenden Krankheiten im Interesse der allgemeinen Gesundheit geboten sei.[1189] Eine solche Personendatenverarbeitung soll entsprechend zwecks Erfüllung eines allgemeinen gewichtigen Interesses, des allgemeinen Gesundheitsschutzes, unter Umständen selbst mangels Einwilligung des Datensubjektes unter Einhaltung allfälliger prozeduraler Vorgaben, möglich sein. Eine grundsätzlich persönlichkeitsverletzende Verarbeitungshandlung wird dann – zum Schutz kontextueller Integrität – von Gesetzes wegen gerechtfertigt.[1190]

Die persönlichkeitsverletzende Verarbeitungshandlungen *legitimierenden Gesetzestatbestände dienen folglich der Funktionstüchtigkeit und dem Schutz der Integrität jeweils spezifischer Kontexte mit den ebenda formulierten und zu gewährleistenden Zielen*.[1191] Indem Bewertungen und Interessen aus spezifischen Kontexten aufgrund einer generell-abstrakten Beurteilung als schutzwürdig anerkannt werden, lässt sich der gesetzliche Rechtfertigungsgrund als *Brücke* bezeichnen. Datenschutzrecht ist damit – trotz der allgemeinen Ordnung im DSG als sog. Querschnittsgesetz – bereits heute *systembezogenes Recht*. 920

4.3. Überwiegende Interessen

Die überwiegenden privaten wie öffentlichen Interessen werden als Rechtfertigungsgründe für Persönlichkeitsverletzungen qua Personendatenverarbeitungen allgemein in Art. 13 Abs. 1 DSG resp. Art. 31 Abs. 1 nDSG genannt. Konkretisiert werden Konstellationen potentiell überwiegender Interessen in den Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG. Die gesetzliche Enumerierung möglicher überwiegender Interessen entbindet nicht davon, ihr Vorliegen für den konkreten Fall zu belegen. Anders gewendet: Sie gelten nicht von Gesetzes wegen absolut. 921

Die Generalklausel der überwiegenden privaten und öffentlichen Interessen lädt zu grosszügigen Interpretationen vonseiten der Datenverarbeitenden ein. Datenschutzrechtlich wird namentlich das überwiegende private Interesse als *Blanko-Ermächtigung* kritisiert.[1192] Heute lassen sich vonseiten der Verantwortlichen für nahezu jede Personendatenverarbeitung Interessen anführen, die als überwiegend beurteilt werden könnten. An erster Stelle dürften wirtschaftliche Interessen figurieren, zumal Personendaten als das «Gold» resp. «Öl des 21. Jahrhunderts» gel- 922

1189 Nissenbaum, 173.
1190 Vgl. die Meldepflicht gemäss Art. 12 Abs. 1 des Bundesgesetzes über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiegesetz, EpG, SR 818.101).
1191 Nissenbaum, 173.
1192 Vgl. Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 33 ff und N 44 ff.

ten.[1193] Die Gesetzessystematik mag den datenverarbeitenden Stellen aufgrund des Grundsatzentscheides für die Freiheit der Datenbearbeitung mit Schranken durchaus rechtlich begründeten Anlass geben, von einer grosszügigen Interpretation zulässiger überwiegender privater Interessen auszugehen.[1194]

923 Immerhin sollen, *pro memoria*, Rechtfertigungsgründe für Persönlichkeitsverletzungen gemäss Art. 12 Abs. 2 lit. a DSG nur zurückhaltend angenommen werden. Dies hat spezifisch für die Figur des überwiegenden Interesses Relevanz. Eine solch zurückhaltende Annahme von Rechtfertigungsgründen ist ebenso nach Totalrevision zu fordern, insb. für die Konstellation gemäss Art. 30 Abs. 2 lit. a nDSG. Wie weit aber geht diese Zurückhaltung resp. worin finden sich orientierende Gewichtsteine resp. Evaluationskriterien, um zu bestimmen, welche überwiegenden privaten Interessen persönlichkeitsverletzende Verarbeitungshandlungen rechtfertigen? Lehre und Rechtsprechung äussern sich hierzu nicht vertieft. Anhaltspunkte liessen sich vorab aus den von Gesetzes wegen konkretisierten Konstellationen des überwiegenden Interesses gemäss Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG finden. Weitere Richtungshinweise finden sich in einem Befund, wonach die Gründe zur Rechtfertigung persönlichkeitsverletzender Personendatenverarbeitungen nicht isoliert individualrechtlicher Provenienz sind. Vielmehr ist in diesem Punkt die dynamische sowie systemische Dimension des Datenschutzrechts zu berücksichtigen. Ebendies soll für die *überwiegenden öffentlichen oder privaten Interessen* gelten. Unmittelbar sichtbar wird dies anhand von Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG, der *nicht abschliessend* denkbare überwiegende Interessen, die der Erfüllung spezifischer Verarbeitungszusammenhänge und -kontexte dienen, aufführt. Art. 31 Abs. 2 nDSG sieht gewisse Anpassungen im Vergleich zu Art. 13 Abs. 2 DSG, auf die indes an dieser Stelle nicht vertiefend eingegangen wird.

924 Eine Inspiration- und Interpretationsquelle lässt sich in Bezug auf die Interessenabwägungen anhand eines auf den ersten Blick vielleicht gewagten Exkurses in das Vereinsrecht finden. Im Vereinsrecht kommt Zweckerwägungen – ähnlich wie im Datenschutzrecht – eine hohe Bedeutung zu. Über einen vernetzten Blick auf Zweckerwägungen im Rahmen des Vereinsrechts lassen sich Richtungshinweise für das Datenschutzrecht generieren. Die beklagte Orientierungs- und Steuerlosigkeit des «überwiegenden Interesses» lässt durch eine Integration von Zweckerwägungen reduzieren. Mit anderen Worten: Das Defizit der Figur der «überwiegenden Interessen» wird datenschutzrechtlich durch eine

1193 Vgl. kritisch m. w. H. Hürlimann/Zech, sui-generis 2019, 89 ff., 90; Flückiger, NZZ vom 1. Februar 2016; Grassegger, 10; zum Gold, das aus Analysen von grossen Datenbeständen generiert wird, Beranek Zanon, in: Thouvenin/Weber (Hrsg.), 86 ff., 89; zum hohen wirtschaftlichen Wert von Personendaten Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 151.

1194 Vgl. zweiter Teil, IV. Kapitel, B.3.2.

Ankoppelung von Zweckerwägungen abgeschwächt, wobei eben das Vereinsrecht für einen differenzierten Blick auf die Zweckrelevanz aufschlussreich ist. Konkreter geht es um die Herausforderung, das *Verhältnis zwischen mehreren verschiedenen Zwecken, zwischen mittelbarem und unmittelbarem Zweck*, zu koordinieren. Eine solche Zweckdifferenzierung ist für das Vereinsrecht typisch. Das Vereinsrecht wird geprägt von der Unterscheidung zwischen *ideellem und wirtschaftlichem* Zweck.[1195] Für einen rein wirtschaftlichen Zweck darf nicht die Vereinsform gewählt werden. Entsprechend konstanter Bundesgerichtspraxis liegt ein wirtschaftlicher Zweck dann vor, wenn ein Verein wirtschaftliche Vorteile generieren möchte *und* diese an die Mitglieder selbst zurückfliessen sollen.[1196] Es geht in dieser Konstellation um ein *isoliertes und eigenes Profitinteresse*, für welches das Gefäss des Vereins nicht zur Verfügung stehen soll. Die Vereinsform ist zulässig, wenn zwar ein Vorteil generiert wird, dieser allerdings Dritten und nicht dem Verein resp. seinen Mitgliedern selbst zufliesst.

925 Parallele Erwägungen lassen sich für den Datenschutz anstellen: Im Rahmen der Personendatenverarbeitung liegt es für die Verarbeitenden nahe, den *eigenen* Profit, der (vermeintlich) durch möglichst unbeschränkte Personendatenverarbeitungsprozesse erzielt werden kann, als «überwiegendes privates Interesse» anzuführen. Die Relevanz der Staffelung von Interessen und Zwecken wurde für das Datenschutzrecht anhand der Analyse des Zweckbindungsgrundsatzes herausgearbeitet.[1197] Im Rahmen der Beurteilung, wann aus einer Perspektive des Datenschutzes Interessen als überwiegend zu qualifizieren sind, liesse sich dieser für das Vereinsrecht längst bekannte, nuancierte Ansatz mit seiner Differenzierung zwischen primären Zwecken, Zielen und Interessen sowie oft dahinterstehenden wirtschaftlichen Interessen fruchtbar machen: Unter Umständen liesse sich die «Vermutung» erhärten, wonach eine persönlichkeitsverletzende Verarbeitungshandlung dann von einem überwiegenden Interesse getragen ist, wenn mit ihr der *unmittelbare Zweck und das primäre Ziel des Kontextes*, in den die Verarbeitungshandlung eingebettet ist, effizienter erreicht werden. Einzig und allein die Generierung von *wirtschaftlichem Gewinn und Profit in eigenem Interesse* vermag – isoliert betrachtet – hierzu namentlich dann nicht zu genügen, wenn sich die persönlichkeitsverletzende Verarbeitungshandlung nicht in einem rein ökonomischen Kontext vollzieht, sondern stattdessen Ziele und Zwecke weiterer gesellschaftlicher Bereiche auf dem Spiel stehen, in denen die Personendatenverarbeitungsprozesse eingebettet sind. Anders gewendet: Wirtschaftliche Interessen von Verantwortlichen, die mittels Personendatenverarbeitungen verfolgt werden, dürfen die Integrität weiterer gesellschaftlicher Kontexte mit ihren

1195 Vgl. Art. 52 Abs. 2, Art. 59 Abs. 2 und Art. 60 Abs. 1 ZGB; vgl. BGE 88 II 209; BGE 90 II 333.
1196 Vgl. m. w. H. Jakob, KuKo-ZGB, Art. 60 N 1 f.
1197 Vgl. hierzu zweiter Teil, V. Kapitel, B.4.

Zielen und Zwecken nicht untergraben. In einem solchen Sinne liessen sich die überwiegenden Interessen in einer für das Datenschutzrecht produktiven Weise strukturieren, kanalisieren und unter Umständen limitieren.

926 Die umrissene Stossrichtung wird im letzten Teil dieser Arbeit fundiert werden, wobei exemplarisch und spezifisch die Observation im Versicherungskontext zur «Beweisführung» herangezogen wird. Bei letzterer geht es darum, Leistungsbeziehende mittels Privatdetektivs geheim zu observieren, um einen allfälligen Betrug aufzudecken. Die Praxis, für die nunmehr eine gesetzliche Grundlage geschaffen wurde, stösst gleichwohl auf gesellschaftlichen Widerstand.[1198] Nissenbaum dienen die gesellschaftlichen Reaktionen des Widerstandes und des Empörens als Detektor oder Indikator, wonach kontextspezifische Erwartungen verletzt werden. Sie setzt diese als Instrumentarium für ihre Argumentation ein.[1199]

927 Eine ähnliche Konstellation wie in der geheimen Versicherungsobservation liegt den Logistep-Entscheiden zugrunde. Die Logistep AG, welche aufgrund einer von ihr entwickelten Software das Surfverhalten von Internetnutzerinnen und -nutzern trackte, verfolgte an erster Stelle ein *eigenes monetäres Interesse*. Die Ermittlung von Urheberrechtsverletzungen dagegen, so das Bundesgericht, sei Aufgabe staatlicher Behörden.[1200] Folglich liess das Bundesgericht ein überwiegendes Interesse nicht als Rechtfertigungsgrund zu.[1201] Der Entscheid ist damit ein Illustrationsbeispiel dafür, wie für das Datenschutzrecht der Schweiz – hier anhand der Rechtsprechung zu den überwiegenden Interessen als Rechtfertigungsgrund für eine persönlichkeitsverletzende Personendatenverarbeitung – die Einschlägigkeit *pluraler* Verarbeitungszusammenhänge sowie Gesellschaftsbereiche anerkannt wird. Die Relevanz des Schutzes von Systemen sowie Subsystemen mit ihren jeweiligen spezifischen Zwecken, Interessen, Akteuren und Rollen wird auch hier adressiert.

928 Dass diese Schutzrichtung trotz der dualistischen Struktur mit seiner persönlichkeitsrechtlichen Anknüpfung für den privaten Bereich im DSG angelegt ist, verdeutlicht zudem der Blick auf die vom Gesetzgeber konkretisierten potentiellen Konstellationen, in denen überwiegende Interessen angenommen werden: Sie beziehen sich auf jeweils spezifische Verarbeitungszusammenhänge und Kontexte, z. B. den Medienkontext oder die Forschung.

929 Nachdem über die gesetzliche Grundlage sowie die überwiegenden Interessen zur Rechtfertigung persönlichkeitsverletzender Personendatenverarbeitungen die

1198 Vgl. vertiefend dritter Teil, IX. Kapitel, B.
1199 Nissenbaum, 3; zur Welt der Gefühle im Zusammenhang mit (enttäuschten) Erwartungen Luhmann, Systeme, 370 ff.
1200 BGE 136 II 508, E 6.3.2.
1201 BGE 136 II 508, E 5 und E 6, insb. E 6.3.3.; beachte insofern die Teilrevision des URG.

Integration kontextspezifischer Erwägungen selbst im persönlichkeitsrechtlichen und damit subjektivrechtlich angeknüpften Datenschutzrecht resp. Datenschutzgesetz als Querschnittsgesetz sichtbar gemacht wurde, soll nunmehr auf die Bedeutung der Einwilligung des Datensubjektes als Rechtfertigungsgrund eingegangen werden. Da hinsichtlich der Bedeutung, Rolle und Funktion der datenschutzrechtlichen Einwilligungen Unsicherheiten und Fehlannahmen bestehen, widmen sich die folgenden Ausführungen diesen vertieft.

4.4. Die rechtfertigende Einwilligung gemäss DSG

4.4.1. Einordnung

Die Schweiz kennt in ihrem DSG für den privaten Bereich das Einwilligungserfordernis als Erlaubnistatbestand für prinzipiell verbotene Personendatenverarbeitungen *nicht*. Ebendies gilt auch nach Totalrevision und mit Blick auf Art. 6 Abs. 6 und Abs. 7 nDSG. Vielmehr spielt die Einwilligung im DSG die Rolle als Rechtfertigungsgrund für persönlichkeitsverletzende Personendatenverarbeitungen, vgl. auch Art. 13 Abs. 1 und Art. 31 Abs. 1 nDSG. Ein solches Einwilligungskonzept ist logische Konsequenz des Ausgangspunktes der generellen Verarbeitungsfreiheit mit Schranken, den das DSG für den privaten Bereich wählt.[1202] Schranken, deren Durchbrechung die Persönlichkeitsverletzung markieren, bilden namentlich die Verletzung der allgemeinen Verarbeitungsgrundsätze, der Widerspruch des Datensubjektes, die Weitergabe von besonders schutzwürdigen Angaben und Persönlichkeitsprofilen an Dritte, vgl. Art. 12 Abs. 2 DSG und Art. 30 Abs. 2 nDSG. Die Einwilligung des Datensubjektes figuriert gemäss DSG somit als Rechtfertigungsgrund für qualifizierte Verarbeitungshandlungen, die als persönlichkeitsverletzend taxiert werden und die nicht durch einen anderen Rechtfertigungsgrund legitimiert sind.[1203] Obschon punktuell nachgeschaltet zu den Rechtfertigungsgründen qua Gesetz oder überwiegendem Interesse gilt die Einwilligung faktisch als bedeutsam(st)er Rechtfertigungsgrund.[1204] Hierzu die folgenden Anmerkungen: 930

Einbettend ist unter Berücksichtigung des Dualismus zunächst zu erwähnen, dass die Einwilligung im öffentlichen Bereich von vornherein keine grosse Relevanz hat.[1205] Gesprochen wird dort, wo Personendaten zu einem «öffentlichen 931

1202 So auch Vasella, Jusletter vom 16. November 2015, N 1.
1203 Die jederzeitige Widerrufsmöglichkeit einer Einwilligung gemäss allgemeinen Grundsätzen wird nachfolgend nicht thematisiert.
1204 Rampini, BSK-DSG, Art. 13 N 3; Vasella, Jusletter vom 16. November 2015, N 2.
1205 Exemplarisch und spezifisch in Bezug auf besonders schützenswerte Informationen Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff., 101 ff., 105 ff., 110.

Zweck» und damit regelmässig basierend auf einer gesetzlichen Grundlage bearbeitet werden, von einer «Entprivatisierung» der Person.[1206]

932 Die Systematik des DSG ist nur teilweise überzeugend. Die Gültigkeitsvoraussetzungen der Einwilligung sind in den allgemeinen Verarbeitungsgrundsätzen niedergelegt, vgl. Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG. Ebendies kann zu der Annahme verleiten, wonach das Einwilligungserfordernis ein allgemeiner Verarbeitungsgrundsatz ist.[1207] Die Lektüre der Bestimmungen erhellt, dass sich die Bestimmung *einzig* mit den Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung beschäftigt, dort, wo eine Einwilligung geboten ist. Die Bestimmungen statuieren selbst kein Einwilligungserfordernis. Die Konstruktion weist gewisse Parallelen zu Art. 3 ZGB auf. Letzterer verbürgt keinen allgemeinen Gutglaubensschutz. Vielmehr stellt der Artikel eine Vermutung zum guten Glauben auf für den Fall, dass dieser von einer anderen Bestimmung als schutzwürdig taxiert wird.

933 Die Einbettung der Gültigkeitsvoraussetzungen für die datenschutzrechtliche Einwilligung innerhalb der allgemeinen Verarbeitungsgrundsätze, Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG, ist mindestens teilweise irreführend. Sie verleitet zu falschen Annahmen über die verbürgte Rechtsposition. Die Gesetzessystematik mag mitursächlich sein für eine Rezeption und schematische Qualifikation des schweizerischen Datenschutzrechts auch für den privaten Bereich als Regime der Selbstbestimmung. Zumindest in der Allgemeinheit wird ein falscher Eindruck hinsichtlich der Positionierung der Einwilligung nach schweizerischem DSG vermittelt. Die Gültigkeitsanforderungen gemäss Art. 4 Abs. 5 DSG beziehen sich nach dem System des DSG für den privaten Bereich prinzipiell auf die *rechtfertigende Einwilligung gegenüber qualifizierten Verarbeitungshandlungen*, vgl. Art. 12 f. DSG und Art. 30 f. nDSG. Die datenschutzrechtliche Einwilligung ist keineswegs Erfordernis zur Erlaubnis jedweder Personendatenverarbeitungen.

934 Relativierend ist immerhin auf Art. 6 Abs. 2 lit. b DSG resp. Art. 17 Abs. 1 lit. a nDSG hinzuweisen, wonach die Einwilligung des Datensubjektes im Einzelfall insb. für den Transfer von Personendaten in ein sog. unsicheres Drittland eingeholt werden soll.[1208]

935 Innerhalb des DSG für den privaten Bereich bewegt sich die Relevanz der datenschutzrechtlichen Einwilligung in den folgenden Schranken: Von vornherein

1206 Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 197.

1207 Die Gültigkeitsvoraussetzungen für die Einwilligung nach der Totalrevision werden Anlass zu einigen Diskussionen in Lehre und Rechtsprechung nicht nur mit Blick auf die dogmatischen Details geben, vgl. insofern bereits zu den entsprechenden Aufsätzen.

1208 Zu den Entwicklungen im Zusammenhang mit dem US Privacy Shield <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/medien/medienmitteilungen.msg-id-80318.html> (zuletzt besucht am 3. Juni 2021).

nicht greift die rechtfertigende Einwilligung für persönlichkeitsverletzende Verarbeitungen gemäss Art. 12 DSG resp. Art. 30 nDSG. Für die Tatbestände nach Art. 12 Abs. 1 lit. b und Art. 12 Abs. 3 DSG sowie Art. 30 Abs. 1 lit. b und Art. 30 Abs. 3 nDSG ist der *Widerspruch* des Datensubjektes begründend für die Persönlichkeitsverletzung. In diesen Konstellationen kann der Einwilligung keine sinnvolle Rolle zukommen. Ihre Hauptbedeutung erlangt die datenschutzrechtliche Einwilligung für Datenverarbeitungen, welche die allgemeinen Verarbeitungsgrundsätze missachten und deshalb persönlichkeitsverletzend sind, Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG (was die Widerrechtlichkeit indiziert). Zudem kann sie ihre Relevanz entfalten im Zusammenhang mit der Weitergabe von besonders schutzwürdigen Daten und Persönlichkeitsprofilen an Dritte ohne anderweitigen Rechtfertigungsgrund nach Art. 12 Abs. 1 lit. c DSG.[1209] Art. 30 Abs. 1 lit. c nDSG adressiert nur noch die Weitergabe von besonders schutzwürdigen Angaben an Dritte; das Persönlichkeitsprofil wird aus der gesetzlichen Regelung entfernt.

Dass der datenschutzrechtlichen Einwilligung ungeachtet dieses normativ eher 936
engen Rahmens *faktisch – sprich in der Praxis* – eine so hohe Relevanz zugewiesen wird, mag als Bestätigung gelesen werden, wonach der Autonomie und Selbstbestimmung des Datensubjektes hohes Gewicht beigemessen wird. Paradoxerweise allerdings ist die Aussage, wonach die Einwilligung in der Schweizer Unternehmenspraxis eine wichtige Rolle spielt, keineswegs nur als positive Aussage für den Datenschutz zu verstehen. Die Einwilligung dient primär zur Rechtfertigung eines Verstosses gegen das als Integritätsschutz bezeichnete Regime von Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG. Weil allerdings die allgemeinen Verarbeitungsgrundsätze als *Minimalstandard der fairen Personendatenverarbeitung* zu gelten haben und im schweizerischen System die Hauptschranke der Personendatenverarbeitung bilden, ist das hohe Gewicht, das der Einwilligung in der Datenschutzpraxis zugemessen wird, problematisch. Denn die Einhaltung der allgemeinen Verarbeitungsgrundsätze wird unter Umständen pauschal und blanko «gewaved». Eine solche rein formalistische Herangehensweise vermag allerdings dem Datenschutz nicht gerecht zu werden. Erhärtet wird diese Kritik durch den Befund, wonach die Verarbeitungsgrundsätze *systemische Schutzerwägungen* integrieren. Sie sollen nicht beliebig der breitangelegten, gleichwohl aber individualrechtlichen Dispositionsbefugnis anheimgestellt werden. Zudem ist in Erinnerung zu rufen, dass sich die Auslegung etabliert hat, wonach Rechtfertigungsgründe im Rahmen von Art. 12 Abs. 2 lit. a DSG nur mit Zurückhaltung zuzulassen sind. Es gibt folglich mehrere Einwände, die eine Prio-

1209 In diesem Sinne auch Vasella, Jusletter vom 16. November 2015, N 2.

risierung individualrechtlicher Dispositionsbefugnisse in einem nachteiligen Licht erscheinen lassen.[1210]

937 Spezifisch zu thematisieren ist eine in der Praxis verbreitete Vorgehensweise. Nach dieser wird die datenschutzrechtliche Einwilligung zur Absicherung und formellen Legitimierung von Personendatenprozessen selbst dort eingeholt, wo es von Gesetzes wegen gar keiner datenschutzrechtlichen Zustimmung bedürfte. Sei es, weil die Personendatenverarbeitung gar keine Persönlichkeitsverletzung begründet, sei es, weil eine persönlichkeitsverletzende Verarbeitungshandlung durch einen gesetzlichen Rechtfertigungsgrund oder überwiegende Interessen legitimiert ist. Dem Datensubjekt wird mit einem solchen Vorgehen suggeriert, dass es über die Verarbeitung der Personendaten bestimmen würde. Allerdings wäre im Lichte der Gesetzesordnung die Personendatenverarbeitung selbst ohne seine Einwilligung zulässig. Besagtes Vorgehen ist nicht nur nach DSG, sondern auch nach DSGVO problematisch. Nach DSGVO haben Verantwortliche bei Verstössen gegen die Vorgaben der Verordnung mit weit- und tiefgreifenden Massnahmen sowie Sanktionen vonseiten der Datenschutzbehörden zu rechnen, vgl. Art. 57 f. und Art. 83 f. DSGVO.[1211] Um entsprechende Risiken zu minimieren, liegt es nahe, quasi zur Sicherheit die Einwilligung des Datensubjektes als Erlaubnistatbestand einzuholen, vgl. Art. 6 Abs. 1 lit. a DSGVO. Selbst dann, wenn die Verarbeitung durch einen anderweitigen Erlaubnistatbestand gedeckt wäre, vgl. Art. 6 lit. b–f DSGVO, und insofern nur – aber immerhin – die Transparenzvorgaben einzuhalten wären, vgl. Art. 12 DSGVO. Im Ergebnis *degeneriert in einer solchen Praxis des «cover your action» durch eine «Sicherheitseinwilligung» die datenschutzrechtliche Einwilligung zu einer inhaltslosen und bedeutungsentleerten Formalität*. Sie suggeriert eine Selbstbestimmung des Datensubjektes, die es indes von Gesetzes wegen nicht hat. Entsprechend dürfte von einer *Pseudo-Selbstbestimmung* zu sprechen sein.

938 In Bezug auf die hohe Bedeutung, die der (rechtfertigenden) Einwilligung nach DSG im schweizerischen Schrifttum zugemessen wird, ist ein weiterer Hinweis angezeigt: Die akademische Auseinandersetzung mit dem Datenschutzgesetz für den privaten Sektor war in der Schweiz lange wenig intensiv.[1212] Zwar findet in der Schweiz das Datenschutzrecht nicht zuletzt im Zuge der Inkraftsetzung und Umsetzung der DSGVO sowie der Totalrevision des DSG gesteigerte Aufmerk-

1210 Zu den Schwächen datenschutzrechtlicher Einwilligungskonstruktionen vertiefend dritter Teil, VIII. Kapitel, B.2.2. und B.5.2.

1211 Hierzu z. B. Bergt, DuD 2017, 555 ff.

1212 Der grosse Teil der Beiträge zum DSG im privaten Bereich ist Kommentarliteratur, sodann Aufsätze von Praktikerinnen und Praktikern. Wissenschaftliche Monografien zum DSG für den privaten Bereich dagegen sind Raritäten, vgl. insofern früh Peters und Aebi-Müller, unlängst spezifisch zum Profiling Heuberger.

samkeit auch vonseiten der Wissenschaft.[1213] Von einer eigentlichen Debatte und Theoriebildung mit Blick auf den Ansatz informationeller Selbstbestimmung und damit die Rolle, Funktion und Funktionstüchtigkeit von Einwilligungskonstruktionen im Datenschutzrecht kann allerdings noch nicht gesprochen werden. Bis heute stammt das Gros der Beiträge zum Datenschutzgesetz für den privaten Sektor aus der Feder der *praktizierenden Anwaltschaft* (sowie der kantonalen Datenschutzbeauftragten). Wenn auch vonseiten der Anwaltschaft bedeutsame Beiträge, namentlich Kommentierungen zum geltenden Recht, verfasst wurden, prägt dieser Ursprung das Schweizer Datenschutzrecht mit. Die praktizierende und publizierende Anwaltschaft im Bereich des Datenschutzrechts ist oft für renommierte und international tätige Wirtschaftskanzleien tätig. Hierbei sind es datenschutzrechtlich meist grosse Unternehmen in Konzernstrukturen, welche die entsprechende Expertise benötigen.[1214] Der Rückgriff auf die datenschutzrechtliche Einwilligung dient dann der Minimierung von Datenschutzverstössen mit ihren Risiken und basiert auf einer Strategie des *cover your action*. Aus der Perspektive der beratenden Anwaltschaft mag folglich die *Relevanz der Einwilligung* als Rechtfertigungsgrund faktisch im Vordergrund stehen. Umgekehrt ist davon auszugehen, dass es unzählige Personendatenverarbeitungen gibt, die persönlichkeitsverletzend sind und für die mangels anderweitigen Rechtfertigungsgrundes eine rechtfertigende Einwilligung einzuholen wäre, auf deren Einholung allerdings verzichtet wird.[1215]

939 Bezogen auf die datenschutzrechtliche Einwilligung zeigt sich damit das Problem, dass diese einerseits eingeholt wird, obschon es ihrer nicht bedürfte, und dass diese andererseits nicht eingeholt wird, obschon es ihrer bedürfte.

940 Darin erschöpfen sich indes die Herausforderungen nicht. Vielmehr stehen zudem die *Gültigkeitsvoraussetzungen* der Einwilligung im Datenschutzrecht in Anbetracht der Realität auf dem Prüfstand. Ihnen widmen sich die nachfolgenden Ausführungen. Die Beschäftigung mit der noch grundsätzlicheren Frage, inwiefern Einwilligungskonstruktionen überhaupt geeignet sind, datenschutzrechtliche Aufgaben zu adressieren und Schutzziele zu erreichen, wird im dritten Teil dieser Arbeit vertieft. Die Frage mag erstaunen, zumal sich die Anerkennung und der Ausbau von Selbstbestimmungsrechten, in denen die *Einwilligung* als Ausdruck der Autonomie des Subjektes zum Kernelement der Gesetzgebung

1213 Jünger zur Einwilligung im Datenschutzrecht, allerdings mit Akzent auf den grund- und verfassungsrechtlichen Aspekt, Fasnacht, *passim*; jüngst beachte Kasper, *passim*; Amstutz, AcP 2018, 438 ff. und NZZ vom 5. September 2018, 10.

1214 Vgl. zur unterschiedlichen Maturität mit Blick auf die Umsetzung der datenschutzrechtlichen Vorgaben durch schweizerische KMU gegenüber den Grossunternehmen Ebert/Widmer, 19.

1215 Bolliger/Féraud/Epiney/Hänni, 41; in Deutschland hat namentlich Buchner problematisiert, dass viele Personendatenverarbeitungen an den «Datensubjekten vorbei» bearbeitet werden, vgl. 130 ff.

wird,[1216] als Entwicklungstendenz für Rechtsgebiete beschreiben lässt, die sich mit den Herausforderungen neuer Technologien zu befassen haben. Sie wird als «Rezept» zur Lösung von Herausforderungen, welche die neuen Technologien mit sich bringen, präsentiert.[1217] Dahinter scheint eine Vorstellung zu wirken, wonach der Mensch und seine Würde sowie sein Subjektstatus durch die neuen Technologien ausgehöhlt werden. Dem Subjekt droht durch die undurchschaubaren und unkontrollierbaren Technologien die Degradierung zum Objekt. Zu Recht wurde allerdings – und das ist für diese Studie richtungsweisend -früh davor gewarnt, mit der Identifizierung der Technologien als «Sündenbock» von den sozialen Konflikten und Problemen abzulenken.[1218] Ebendies gilt es über das Recht zu adressieren.

941 Einwilligungskonstruktionen als rechtliche Antwort im Kontext technologiebedingter Herausforderungen können vor diesem Hintergrund als «Emanzipationsansätze» bezeichnet werden. Sie werden mit den Kategorien und Gütern der «Selbstbestimmung» und «Autonomie» assoziiert.[1219] Zwar drängt sich an dieser Stelle erneut die Vermutung auf, dass eine Reduktion auf eine Dichotomie, in der die Technologie als Herrschaftstechnologie und Instrument der Unterwerfung des Menschen beschrieben wird – mit einer Degradierung des Menschen zum Objekt –, dem Facettenreichtum der Thematik nicht gerecht wird. So erstaunt es keineswegs, dass das komplexe Verhältnis zwischen Mensch und Technik auch anderweitig umschrieben wird, beispielsweise mit Begriffen wie «hybride Assoziationen» im Kontext des Internets.[1220]

942 Gleichwohl lässt sich im Zuge der Entwicklungen des Rechts die Strategie nachweisen, auf etablierte Figuren zurückzugreifen und mit Blick auf ein Datenschutzrecht, das zutiefst im Persönlichkeitsrecht verwurzelt ist, den *Subjektstatus zu stärken und auszubauen*.[1221] Ob damit datenschutzrechtlich ein wirksames und produktives Instrument etabliert werden kann, wird jüngst hinterfragt: Insofern werden die Tauglichkeit des Instrumentes in seiner funktionellen Stossrichtung an sich wie auch die bedeutungsvolle Griffigkeit der etablierten Gültigkeits-

1216 Exemplarisch zur Qualifikation von Einwilligungsvorschriften als Elemente des informationellen Autonomieschutzes Ingold, NomosKomm-DSGVO, Art. 7 N 33.

1217 Vgl. illustrativ insofern die zahlreichen datenschutzrechtlichen Monografien zur datenschutzrechtlichen Einwilligung sowie Zeitschriftenbeiträge sowohl im schweizerischen als auch im deutschen Schrifttum; sodann die Beiträge von Barocas/Nissenbaum; Karavas, Körperverfassungsrecht, 193 ff., insb. 199 ff., für den Bereich des Biomedizinrechts.

1218 Fiedler, in: Podlech/Steinmüller (Hrsg.), 179 ff., 193.

1219 Vgl. mit Blick auf das Online Behavioral Advertisement Barocas/Nissenbaum, 1 ff.; aufschlussreich zum Selbstbestimmungsrecht Fateh-Moghadam, BJM 2018, 205 ff., 213 ff.; vgl. insofern auch Litman, Stan. L. Rev. 2000, 1283 ff., 1292 f. mit den Worten «If ownership of private property is power, however, calling privacy rights „property rights" offers the promise of magically vesting the powerless with control over their personal data».

1220 Vgl. Karavas, Neue Zeitschrift für Sozialforschung 2010, 95 ff.

1221 Burkert, 158.

voraussetzungen datenschutzrechtlicher Einwilligungen im Lichte der Realität kritisch beleuchtet.[1222] Damit erscheint es *prima facie* als nicht nachteilig, dass man in der Schweiz bislang den Weg in Richtung Ausbau resp. Etablierung eines Regimes der Selbstbestimmung, in welchem die informierte Einwilligung ein Kerninstrumentarium darstellt, nicht beschritten hat: Zwar werden mit der Totalrevision die Transparenzvorgaben gegenüber dem Datensubjekt und die Betroffenenrechte ausgebaut. Im Übrigen allerdings soll die prinzipielle Bearbeitungsfreiheit mit Schranken beibehalten werden, womit der Wille des Datensubjektes weiterhin als Widerspruchsrecht (das oft eine Utopie bleibt) sowie als rechtfertigende Einwilligung von qualifizierten Verstössen figurieren. Prinzipiell dürfen Personendatenverarbeitungen im privaten Bereich auch nach der Totalrevision des DSG ohne Einwilligung erfolgen.[1223] Sehr viel effizienter zeigt sich eine andere Strategie: die Einführung von neuen Instrumenten, die das Datenschutzrecht faktisch verwirklichen sollen. Genau diesen Weg beschreiten auch die DSGVO sowie die Totalrevision des DSG.

943 Für den Fall, dass eine Einwilligung *zwecks Rechtfertigung* persönlichkeitsverletzender – weil qualifizierter – Personendatenverarbeitungen erforderlich ist, sind ihre *Gültigkeitsvoraussetzungen* zu beachten. Die *Gültigkeitsvoraussetzungen* der Einwilligung gemäss Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG beziehen sich *nicht* auf den *Widerspruch*, wie er in Art. 12 Abs. 2 lit. b DSG oder Art. 12 Abs. 3 DSG resp. Art. 30 Abs. 2 lit. b und Art. 30 Abs. 3 nDSG niedergelegt wird. Dies ergibt bereits der Wortlaut – Einwilligung ist nicht gleich Widerspruch. Art. 4 Abs. 5 DSG resp. Art. 6 Abs. 6 und Abs. 7 nDSG befassen sich ausdrücklich mit den Modalitäten für die gültige Einwilligung. Dem Widerspruch kommt eine andere Bedeutung und Funktion zu, verkehrt dieser doch eine prinzipiell erlaubte in eine grundsätzlich verbotene Datenverarbeitung. Im DSG für den privaten Bereich wird mittels Widerspruches der gesetzliche Ausgangspunkt, wie er in genereller Weise vorgesehen wird, aufgrund des Willens des Datensubjektes für den Einzelfall modifiziert. Anders wird mit einer rechtfertigenden Einwilligung ein vom Gesetzgeber als Persönlichkeitsverletzung taxiertes Verhalten gebilligt, wobei dieses – wie gezeigt – gemäss DSG in einem qualifizierten Umgang mit Personendaten liegt. Es ist (wiederum) das Subjekt, das mit der rechtfertigenden Einwilligung eine vom Gesetzgeber als persönlichkeitsverletzend und damit prinzipiell widerrechtlich zu qualifizierende Datenverarbeitung die Widerrechtlichkeit entfallen lässt.[1224] Zugleich verzichtet es gleichsam auf das unmittel-

1222 Vertiefend dritter Teil, VIII. Kapitel, B.4.2.

1223 So auch Vasella, Jusletter vom 16. November 2015, N 2; vgl. Rosenthal, HK-DSG, Art. 12 N 25; Hussein, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.114.

1224 Vgl. Art. 28 Abs. 2 ZGB und Art. 13 DSG resp. Art. 31 nDSG.

bar an die ansonsten widerrechtliche Persönlichkeitsverletzung anknüpfende Durchsetzungsinstrumentarium.

944 Vor diesem Hintergrund ist es folgerichtig, an den *Widerspruch niedrigere* Anforderungen an dessen Gültigkeit zu formulieren als für die rechtfertigende Einwilligung in ihrer Funktion in einem Regime qualifizierter Personendatenverarbeitung (insb. gemäss Art. 12 Abs. 2 lit. a DSG resp. Art. 30 Abs. 2 lit. a nDSG, der gleichzeitig als Basisregime sowie Integritätsschutz beschrieben wurde). Immerhin scheint Art. 4 Abs. 5 DSG hinsichtlich der Widerspruchslösung – neben Treu und Glauben sowie den auf die Figur zurückgeführten Transparenz- und Informationsvorgaben – insofern einen Einfluss gezeitigt zu haben, als eine Pflicht zur Informierung über ein Widerspruchsrecht vertreten wird.[1225]

4.4.2. Gültigkeitsvoraussetzungen

945 Die rechtfertigende Einwilligung und hierbei ihre *Freiwilligkeit* sowie *Ausdrücklichkeit* hat der EDÖB namentlich in seinem Schlussbericht i. S. Postfinance thematisiert.[1226] Der EDÖB ging von einer Verletzung der allgemeinen Verarbeitungsgrundsätze der Proportionalität, Zweckbindung sowie Datenrichtigkeit aus. Zu prüfen war, ob ein Rechtfertigungsgrund i. S. v. Art. 13 DSG für die nach Art. 12 Abs. 2 lit. a DSG persönlichkeitsverletzenden Verarbeitungen angeführt werden konnte. Mangels gesetzlicher Grundlage oder überwiegenden Interesses war die Einwilligung als Rechtfertigungsgrund zu prüfen.

946 Damit die rechtfertigende Einwilligung *gültig* ist, haben mehrere Untervoraussetzungen erfüllt zu sein: Die *Urteilsfähigkeit*, die *Informiertheit* und *Freiwilligkeit* sowie *das Fehlen von Willensmängeln*. *Ausdrücklich* muss die Einwilligung einzig bei der Weitergabe von besonders schutzwürdigen Angaben oder Persönlichkeitsprofilen an Dritte sein, wohingegen, *e contrario*, andernorts die konkludente Einwilligung genügt. Dazu gehört die stillschweigende Einwilligungserklärung, wobei sich Abgrenzungsschwierigkeiten ergeben zu dem bloss passiven Verhalten, dem Nichtstun oder Schweigen, was gemeinhin nicht als Einwilligung qualifiziert werden kann.[1227] Die Gültigkeitsvoraussetzungen gemäss DSG werden schlaglichtartig beleuchtet. Die Darstellung bezieht sich auf die Version vor

1225 Kritisch Rosenthal, HK-DSG, Art. 12 N 26.

1226 EDÖB, E-Banking bei Postfinance: Datenanalyse wird freiwillig sein, Bern 2015, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/finanzwesen/e-banking-bei-postfinance--datenanalyse-wird-freiwillig-sein.html> (zuletzt besucht am 30. April 2021); jüngst ist sodann auf den Entscheid des Bundesverwaltungsgerichts i. S. Helsana+, BVGer A-3548/2018, Urteil vom 19. März 2019 hinzuweisen, der sich ebenso mit der datenschutzrechtlichen Einwilligung befasst, wobei sich Abgrenzungsfragen betr. die Anwendbarkeit der Bestimmungen des DSG für den öffentlichen oder den privaten Bereich ergeben.

1227 Vgl. Rampini, BSK-DSG, Art. 13 N 9 ff.

Totalrevision. In Bezug auf die Neuerungen zur Einwilligung nach neuem Regime ist auf die sich erst entwickelnde Lehre zu verweisen.

947 Die *Urteilsfähigkeit* bezüglich der datenschutzrechtlichen Einwilligung wurde bislang nur am Rande thematisiert.[1228] Nicht spezifisch zur Urteilsfähigkeit, stattdessen allgemein hinsichtlich der Gültigkeitsanforderungen an die Einwilligung wird vertreten, dass die Anforderungen umso höher sind, je sensibler die Angaben sind oder je schwerer eine Persönlichkeitsverletzung wiegt.[1229] Eine solche Forderung entspricht der allgemeinen Lehre zur Urteilsfähigkeit, wonach diese *relativ* ist.[1230] Diese Relativität mit Blick auf die Urteilsfähigkeit findet folglich ihren Niederschlag im Rahmen der datenschutzrechtlichen Einwilligung. Je anspruchsvoller und weitreichender eine Datenverarbeitung, für die eine Einwilligung gefordert wird, ist, desto höher sind die Vorgaben an die Urteilsfähigkeit anzusetzen. Ob eine Person urteilsfähig ist, bestimmt sich stets anhand des konkreten Rechtsaktes und der konkreten Umstände der Situation. In Anbetracht der Komplexität von Personendatenverarbeitungsprozessen und den hierbei eingesetzten Technologien stellt sich selbstredend die Frage, wie viel Urteilsvermögen realistischerweise von einer Person verlangt werden kann, um gültige Einwilligungen in persönlichkeitsverletzende Datenverarbeitungen abgeben zu können. Einwilligungstatbestände und -erklärungen dürfen weder zu detailliert noch zu oberflächlich umschrieben werden.[1231]

948 Im Rahmen der Urteilsfähigkeit als Voraussetzung der datenschutzrechtlichen Einwilligung kommt dem Thema des *Minderjährigendatenschutzes* besondere Bedeutung zu.[1232] Unter dem Begriff werden diverse Herausforderungen und Phänomene diskutiert, namentlich die Nutzung sozialer Netzwerke durch Minderjährige selbst, aber auch das Phänomen der sog. Helikopter-Eltern, die mittels Geotracking ihre Kinder stets im Auge haben, sowie die Publikation von Kinderfotos durch die Eltern.[1233] Ein paar Hinweise mögen in diesem Zusammenhang

1228 Jüngst allerdings vertiefend Fasnacht, N 305 ff., insb. N 308 sowie N 251 ff.; entsprechend ist auch Bezug auf die zivilgesetzlichen Vorgaben zur Urteilsfähigkeit zu nehmen, Art. 16 ZGB.

1229 M. w. H. Rampini, BSK-DSG, Art. 13 N 3.

1230 Für Deutschland immerhin Rogosch, 48 ff.; für die Schweiz Fasnacht, N 306 ff.; Aebi-Müller, N 223; Meier, N 836; m. w. H. zur Relativität der Urteilsfähigkeit im Zusammenhang mit der persönlichkeitsrechtlichen Einwilligung sodann Haas, N 265 ff.

1231 Vgl. Passadelis/Roth, Jusletter vom 4. April 2016, N 19 ff.

1232 Fankhauser/Fischer, in: Fankhauser/Reusser/Schwander (Hrsg.), 193 ff.; EDÖB, 19. Tätigkeitsbericht zum Jugendschutz im Internet und 16. Tätigkeitsbericht; vgl. mit Hinweis auf die Empfehlungen des Europarates CM/Rec (2018) 7 zum Thema der Kinderrechte in der digitalen Welt Husi-Stämpfli, digma 2019, 84 ff.; zum Minderjährigendatenschutz und zur Einwilligungsfähigkeit von Minderjährigen nach DSGVO und insb. Art. 8 DSGVO Krüger/Vogelgesang/Weller, Jusletter IT vom 23. Februar 2017; vgl. sodann auch Fountoulakis, in: Arnet/Eitel/Jungo/Künzle (Hrsg.), 145 ff.

1233 Vgl. insofern immerhin Fasnacht, N 609 ff.; rechtlich interessant wäre in diesem Zusammenhang auch eine Analyse zum Bezug digitaler Güter durch Jugendliche im Internet; vgl. EU-IPO, Intellectual Property and Youth, Scoreboard 2016.

genügen. Im Jahr 2019 erhielt ein Lehrmittel des Datenschutzbeauftragten des Kantons Zürichs, dessen Inhalte Kinder zwischen vier und neun Jahren für Themen der Privatsphäre sensibilisieren sollte, einen internationalen Preis.[1234] Auch der EDÖB leistet wichtige Sensibilisierungsarbeit in Bezug auf den Umgang von Kindern und Jugendlichen mit den neuen Technologien, wobei er sich auch zur Einwilligung von Minderjährigen resp. der gesetzlichen Vertreter geäussert hat, ohne allerdings Konkretisierungen bezüglich der Urteilsfähigkeit zu machen.[1235]

949 Spezifisch mit Blick auf die Urteilsfähigkeit im Zusammenhang mit der datenschutzrechtlichen Einwilligung sei auf einen Entscheid des Oberlandesgerichts Hamm hingewiesen, der Minderjährigen selbst ab fünfzehn Jahren die erforderliche Reife absprach, um die Tragweite einer Einwilligungserklärung zur Datenspeicherung und -verwendung einzuschätzen.[1236] Die DSGVO befasst sich spezifisch mit der Einwilligung zur Nutzung von Diensten der Informationsgesellschaft durch Minderjährige, Art. 8 i. V. m. Art. 4 Nr. 25 DSGVO. Zudem ist der Umgang mit Personendaten von Kindern als Kriterium der Datenschutz-Folgenabschätzung, vgl. Art. 35 DSGVO, relevant.[1237] Art. 8 Abs. 1 DSGVO setzt das Mindestalter für die selbstständige Einwilligung auf sechzehn Jahre, wobei die nationalen Rechte gemäss Abs. 2 – eine der vielen Öffnungsklauseln der DSGVO – ein geringeres Alter vorsehen können.[1238] Indem sich die Norm auf die Nutzung von Diensten der Informationsgesellschaft beschränkt und eine Öffnungsklausel vorsieht, ist ihr Wirkungsbereich beschränkt.

950 In der Schweiz ist *de lege lata* auf die allgemeinen Vorgaben zur Handlungsfähigkeit zurückzugreifen. Die Totalrevision schafft keine spezifische Regelung. Das Persönlichkeitsrecht gilt als relativ höchstpersönliches Recht; urteilsfähige Minderjährige üben es selbst aus, vgl. Art. 19c Abs. 1 ZGB.[1239] Weil das Datenschutzgesetz für den privaten Sektor an das zivilrechtliche Persönlichkeitsrecht anknüpft, können Kinder und Jugendliche für den Fall, dass sie hinsichtlich einer

1234 Kanton Zürich, Datenschutz, Zürich 2019, <https://dsb.zh.ch/internet/datenschutzbeauftragter/de/aktuell/medienmitteilungen/2019/internationale-datenschutz-auszeichnung-fuer-den-kanton-zuerich.html> (zuletzt besucht am 30. April 2021).

1235 Vgl. insofern <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/jugend-und-internet.html> (zuletzt besucht am 3. Juni 2021); EDÖB, 19. Tätigkeitsbericht, 21; Ders., 16. Tätigkeitsbericht, 33 ff.

1236 Oberlandesgericht Hamm, I-4U 85/12, vom 20. September 2012. Dem Entscheid lag folgender Sachverhalt zugrunde: Eine Krankenkasse hatte Gewinnspielkarten auf einer Messe für Schüler und Jugendliche verteilt. Auf deren Rückseite waren Felder angebracht, in welche Adresse, Name, E-Mail eingetragen werden konnten. Die Angaben sollten für Werbezwecke genutzt werden, wobei sich unter diesen Zeilen die entsprechenden Datenschutzhinweise sowie die Einwilligungszeile befand. Unter dieser befand sich der Hinweis, dass bei Kindern unter 15 Jahren die elterliche Zustimmung nötig sei.

1237 Vgl. WP 29/248 rev. 01, Data Protection Impact Assessment, 10 ff.

1238 Vgl. m. w. H. Krüger/Vogelgesang/Weller, Jusletter IT vom 23. Februar 2017, insb. N 3.

1239 Vgl. Breitschmid, HK-ZGB, Art. 19c N 1 und N 5; dagegen mit Verweis auf eine allfällige Mitwirkung der gesetzlichen Vertreter bei der Geltendmachung der Rechte Rampini, BSK-DSG, Art. 12 N 1.

konkreten Datenverarbeitung urteilsfähig sind, gültig in eine Persönlichkeitsverletzung – auch durch Datenverarbeitungen – rechtfertigend einwilligen. Vertreten wird die Ankoppelung der Urteilsfähigkeit an das Alter von 13 Jahren.[1240] Bezüglich der datenschutzrechtlichen Einwilligung Minderjähriger stellt sich, ähnlich wie bei Volljährigen, die schwierige Frage, ob die Urteilsfähigkeit für eine sinnhafte Einwilligung hinsichtlich einer Bearbeitungshandlung tatsächlich gegeben ist. Eine zusätzliche Herausforderung im Internet liegt in der Verifizierung von Alter und Urteilsfähigkeit eines Kindes. Insofern wurden in den vergangenen Jahren verschiedene Technologien entwickelt, die der Verifizierung der Identität des Nutzers, seines Alters usf. dienen, beispielsweise die Video- oder Stimmauthentifizierung.[1241]

951 Von der datenschutzrechtlichen Einwilligung, die im System des Persönlichkeitsschutzes als Ausübung eines relativ höchstpersönlichen Rechts zu taxieren ist und von urteilsfähigen Minderjährigen selbstständig erteilt werden kann, sind Fragen der Geschäfts- resp. Vertragsfähigkeit abzugrenzen.[1242] Es ist hier nicht der Ort, um beispielsweise das Geschäfts- und Vertragsmodell von Facebook im Lichte des Handlungsfähigkeitsrechts und der Nutzung durch Jugendliche zu analysieren. Für die Geschäftsfähigkeit wird grundsätzlich die volle Handlungsfähigkeit, Volljährigkeit und Urteilsfähigkeit verlangt. Ausnahmsweise genügt die beschränkte Handlungsunfähigkeit, will heissen, dass von Gesetzes wegen die Handlungsunfähigkeit punktuell durchbrochen wird, soweit Minderjährige urteilsfähig sind. Ein Beispiel ist das zulässige rechtsgeschäftliche Handeln im Rahmen des freien Kindervermögens, Art. 321 Abs. 2 ZGB, resp. des Ausbildungslohnes, Art. 323 Abs. 1 ZGB, für den Fall, dass das Kind mit Blick auf die konkrete rechtsgeschäftliche Handlung urteilsfähig ist.

952 Nach Art. 19 Abs. 2 ZGB können Minderjährige sodann Vorteile erlangen, die unentgeltlich sind. Ob die Bestimmung für Verträge zur Nutzung von Online-Dienstleistungen wie Facebook anwendbar ist? Das Konto kostet bekanntermassen kein Geld. Ist ein Vertrag gleichwohl als entgeltlich zu qualifizieren, weil eine Gegenleistung in Gestalt von Personendaten erfolgt? Vor dem Hintergrund solcher Fragen und der jüngsten datenschutzrechtlichen Verschärfungen erstaunt es

1240 Vgl. Rosenthal, Jusletter vom 16. November 2021, N 30.

1241 Unternehmen wie die Swisscom lassen den Abschluss eines Mobilabonnements nur in einem Ladenlokal und mittels Vorlegung einer ID zu. Allgemein stellt sich die Frage, wie weit die Sorgfaltspflicht bei der Verifizierung des Alters geht, ob ein Vertrauen in das Anklicken eines Kästchens, wonach die Nutzerin ein Mindestalter erlangt hat, oder ob beispielsweise das Nachsenden einer ID-Kopie verlangt wird; zur Stimmauthentifizierung, wie sie Bankkundenverkehr eingesetzt wird, Emmenegger/Reber, in: Emmenegger (Hrsg.), 162 ff.; zur Gesichtserkennung Keist, Jusletter vom 20. Mai 2019 N 10 ff., mit einer Analyse der rechtlichen Vorgaben und Schranken.

1242 Insofern ist auf die einschlägige zivil- und personenrechtliche resp. vertragsrechtliche (Kommentar-)Literatur zu verweisen.

nicht, dass Facebook öfter die Einwilligung der Eltern verlangt.[1243] Die Einwilligung der Eltern würde auch den Vorgaben von Art. 19 Abs. 1 ZGB Rechnung tragen.

953 Nach diesem Einschub zur datenschutzrechtlichen Einwilligung von Minderjährigen als Kernthema der Gültigkeitsvoraussetzung der Urteilsfähigkeit *zurück zu den weiteren Gültigkeitsvoraussetzungen*. Über die Urteilsfähigkeit hinaus braucht es zudem, damit eine datenschutzrechtliche Einwilligung gültig erteilt werden kann, grundsätzlich zweierlei: die *Informiertheit und Freiwilligkeit* der Einwilligung, vgl. Art. 4 Abs. 5 DSG und Art. 6 Abs. 6 nDSG. Neuerdings gewinnt die Ausdrücklichkeit der Einwilligungserklärung an Bedeutung, vgl. Art. 6 Abs. 7 nDSG.

954 Teilweise zu Recht wird Art. 4 Abs. 5 DSG nicht als Bearbeitungsgrundsatz qualifiziert.[1244] Art. 4 Abs. 5 DSG besagt, dass dort, wo eine Einwilligung zur Bearbeitung verlangt wird, die Datenbearbeitung nur zulässig ist, wenn die Einwilligung nach *angemessener Information und freiwillig* erteilt wird. Verlangt wird insofern das Wissen um und das Verstehen von Kernelementen der Datenverarbeitung – Zweck, Umfang, Konsequenzen – mit einem daraus resultierenden Entscheid aus freiem Willen, die Einwilligung in die fragliche Verarbeitungshandlung zu erklären.[1245]

955 Zur *Informiertheit*: Sie ist verbunden mit der Maxime, wonach eine (gemäss DSG rechtfertigende) Einwilligung der *angemessenen Informiertheit* vorherzugehen hat.[1246] Mit der *Informiertheit* der Einwilligung befasste sich das Bundesverwaltungsgericht in seinem Entscheid BVGer 2009/44. Im Entscheid ging es um die Beurteilung eines Zutrittskontrollsystems in ein Schwimmbad, das den Missbrauch von Jahreskarten verhindern sollte. Der EDÖB hatte eine Empfehlung zur schonenderen Gestaltung der Zutrittskontrolle erlassen, die indes – auch mit einem Kostenargument – nicht umgesetzt wurde. Daraufhin reichte der EDÖB Klage beim Bundesverwaltungsgericht ein. Das Bundesverwaltungsgericht äusserte sich zum Sinn und Zweck des Erfordernisses der angemessenen Information und konkretisierte dessen Vorgaben wie folgt:

> «Das Erfordernis einer angemessenen Information will erreichen, dass die betroffene Person ihre Einwilligung in Kenntnis der Sachlage gibt, das heisst, erst entscheiden muss, wenn sie sich ein Bild (auch) über die möglichen negativen Folgen ihrer Einwilligung machen konnte. Erforderlich, aber auch genügend ist letztlich, dass sich die betroffene Per-

1243 Computer Bild, Facebook: Datenschutz-Änderung für Jugendliche, Zürich 2018, <https://www.computerbild.de/artikel/cb-News-Internet-Facebook-Datenschutz-Eltern-Gesichtserkennung-21533117.html> (zuletzt besucht am 30. April 2021).

1244 Rosenthal, HK-DSG, Art. 12 Abs. 2 N 14 f.

1245 Vgl. Rampini, BSK-DSG, Art. 13 N 4.

1246 Hierzu Fasnacht, N 249 ff.; Heuberger, N 229 und N 281 ff.; Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.

> son im Klaren darüber sein kann, worin sie einwilligen soll, das heisst, was die Tragweite ihrer Entscheidung ist. Je nach Situation wird eine Aufklärung erforderlich sein, die nicht nur auf die Umstände der Datenbearbeitung, sondern auch auf ihre wichtigsten möglichen Risiken bzw. Folgen für die betroffene Person hinweist, insbesondere wenn diese schwerwiegend sind. Ob und wie weit diesbezüglich informiert werden muss, hängt letztlich aber von den konkreten Umständen ab (ROSENTHAL/JÖHRI, a. a. O., Art. 4 Abs. 5 N 72 f.).»[1247]

Eine gültige Einwilligung im Sinne der *informierten* Einwilligung bedingt, dass die betroffene Person sich zumindest ein Bild machen kann über die Auswirkungen ihrer Einwilligung resp. der daraus folgenden Datenbearbeitung, in die sie einwilligt.[1248] Die datenbearbeitenden Stellen trifft eine entsprechende Informationspflicht. 956

Insofern stellt sich nicht nur die Frage nach der rechtsgenügenden Einbettung entsprechender Informationen in AGB, sondern namentlich auch diejenige nach dem Detailgrad und der Granularität der datenschutzrechtlichen Informierung als Voraussetzung einer gültigen Einwilligung.[1249] In den Worten von Radlanski: 957

> «Sollte man diese Voraussetzung wörtlich verstehen, würde dies darauf hinauslaufen, den Betroffenen für manche Einwilligungserklärungen speziell ausbilden zu müssen: Um beispielsweise genau zu erfassen, welche Implikationen die Einwilligungserklärungen bei Inbetriebnahme eines neuen Smartphones hat, müsste man bestenfalls Informatik studiert haben, oder sich zumindest extrem detailliert mit der Materie auseinandergesetzt haben. Bei den meisten Betroffenen dürfte dies nicht der Fall sein, weswegen man durchaus von einer „Illusion der umfassenden Informiertheit" sprechen kann».[1250]

Unter Umständen entsteht eine kaum zu überbrückende Leerstelle zwischen *Informierung als Pflicht der Verarbeitenden* und *Informiertheit* als Zustand und Ergebnis aufseiten des Datensubjektes. 958

Die DSGVO sowie die Totalrevision des DSG generieren ein erhöhtes Transparenzniveau, womit ebenso ein Effekt auf die Vorgaben an die Informierung und Informiertheit der Einwilligung einhergeht.[1251] Mittlerweile hat sich eine Praxis durchgesetzt, die Transparenzerfordernisse mittels *eigenständiger Privacy-Erklärungen* zu gewährleisten. Um den Vorgaben unter dem Regime der DSGVO zu genügen, sind Einwilligungserklärungen in einem separaten Block spezifisch zu erfassen. Die *Informiertheit*, welche die Kenntnis des Datensubjektes zumindest in groben Zügen über Gegenstand, Zweck, Umfang und Konsequenzen seiner Einwilligung bedingt, begründet vonseiten der Verantwortlichen die Pflicht, die- 959

1247 BVGer 2009/44, Urteil vom 4. August 2009, Regeste 4.
1248 Vgl. Rampini, BSK-DSG, Art. 13 N 4; präzisierend Rosenthal, HK-DSG, Art. 4 N 72 f.
1249 Vertiefend zur Informiertheit und datenschutzrechtlichen Einwilligung Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.
1250 Radlanski, 16, m. w. H.
1251 Beachte insb. WP 29/259, Consent; Passadelis/Roth, Jusletter vom 4. April 2016, N 19 ff.

ses Wissen zu generieren.[1252] Die Zeiten, in denen pauschale Einwilligungserklärungen im Kleingedruckten von AGB als dem Erfordernis Rechnung tragend beurteilt wurden, gehören damit der Vergangenheit an.[1253]

960 Zur *Freiwilligkeit* der Einwilligung als weiterer Gültigkeitsvoraussetzung:[1254] In Bezug auf diese Voraussetzung sind in erster Linie negative Umschreibungen zu finden. Ungültig, weil unfreiwillig, sind Einwilligungen unbestritten zunächst, wenn diese nach Täuschung, unter Zwang oder Drohung erteilt werden.[1255] Sodann beschlagen die fehlende Informiertheit und wohl auch das Missverständnis oder die Fehlinterpretation die Freiwilligkeit einer Einwilligung.[1256] Fehlt der geforderte Grad an Verständnis über die Bearbeitung und deren Folgen, kann auch nicht freiwillig eingewilligt werden. Positiv, aber mit wenig Erkenntnisgewinn mittels Wortspalterei das Bundesverwaltungsgericht:

> «Eine Einwilligung muss freiwillig erfolgen, das heisst, Ausdruck des freien Willens der betroffenen Person sein.»[1257]

961 Aussagekräftiger dagegen die Regeste 4 von BVGer 2009/44:

> «Das Erfordernis einer angemessenen Information will erreichen, dass die betroffene Person ihre Einwilligung in Kenntnis der Sachlage gibt, das heisst, erst entscheiden muss, wenn sie sich ein Bild (auch) über die möglichen negativen Folgen ihrer Einwilligung machen konnte. Eine Einwilligung muss zudem freiwillig erfolgen. Der betroffenen Person muss „eine – mit nicht unzumutbaren Nachteilen behaftete – Handlungsalternative" zur Verfügung stehen (E. 4.2).»

962 Nach wohl herrschender Lehre, Rechtsprechung sowie den Materialien gilt eine Einwilligung dann als unfreiwillig, wenn ihre Verweigerung Nachteile mit sich bringt, die in keinem sachlichen Zusammenhang zum Bearbeitungszweck stehen oder aus anderen Gründen unverhältnismässig sind.[1258] Insb. die Konstellation, in welcher die Erteilung der Einwilligung zur Datenverarbeitung *conditio sine qua non* für den Zugang zu Dienstleistungen oder Produkten ist, hat in der Schweiz Rechtsprechung, Lehre und EDÖB beschäftigt. Hierbei setzte sich die Auffassung durch, wonach eine datenschutzrechtliche Einwilligung dann nicht als freiwillig gilt, wenn sie Voraussetzung für den Zugang zu einer Dienstleistung oder einem

1252 Rampini, BK-DSG, Art. 13 N 4.
1253 Passadelis/Roth, Jusletter vom 4. April 2016, N 22.
1254 Hierzu auch Vasella, Jusletter vom 16. November 2015, N 7 und N 14 ff.; kritisch zur datenschutzrechtlichen Freiwilligkeit der Einwilligung, auch unter Bezug auf Erfahrungen aus dem AGB-Bereich, bereits Simitis, in: Schlemmer (Hrsg.), 67 ff., 77.
1255 Rampini, BSK-DSG, Art. 13 N 4; Radlanski, 12 f.; BVGer 2009/44, Urteil vom 4. August 2009, E 4.2.
1256 Zum Konnex Vasella, Jusletter vom 16. November 2015, N 14.
1257 BVGer 2009/44, Urteil vom 4. August 2009, E 4.2.
1258 M. w. H. Vasella, Jusletter vom 16. November 2015, N 14.

Produkt ist, selbst wenn es insofern Ausweichmöglichkeiten gäbe, diese indes mit unzumutbaren Nachteilen verbunden wären.[1259]

963 Ein spezifisches Kopplungsverbot implementiert die DSGVO mit Art. 7 Abs. 4 DSGVO. Das datenschutzrechtliche Kopplungsverbot geht davon aus, dass die Erbringung einer Dienstleistung oder Erfüllung eines Vertrages nicht von einer datenschutzrechtlichen Einwilligung abhängig gemacht werden darf, die hierfür nicht erforderlich ist. Damit werden «überschiessende Einwilligungen» verhindert.[1260]

964 Kernherausforderungen der Freiwilligkeit als Gültigkeitsvoraussetzung der datenschutzrechtlichen Einwilligung bilden somit eine Machtasymmetrie sowie die Abhängigkeit von Dienstleistungen oder Produkten, die Gefährdung durch übermässige Reize oder durch sozialen Druck. Es handelt sich um Konstellationen, die allesamt in der Regel nicht die Intensität der Tatbestände des Zwanges oder der Drohung erreichen, gleichwohl die autonome Entscheidung des Subjektes beeinträchtigen können.[1261]

965 Im Rahmen der Auseinandersetzungen mit den Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung – *Urteilsfähigkeit*, *Informiertheit sowie Freiwilligkeit* – wurden Schwächen der Einwilligungsvoraussetzungen im Lichte der datenschutzrechtlichen Realität problematisiert. Gefolgert wird hieraus, dass die Einwilligungskonstruktion für verschiedene Konstellationen nicht tragfähig sei.[1262] In Kürze: Die Informiertheit lässt sich in Anbetracht der Komplexität der Verarbeitungsprozesse und Verarbeitungstechnologien faktisch kaum je erreichen.[1263] Die Freiwilligkeit wird nicht selten durch mehrere Einflüsse untergraben, allem voran infolge einer strukturellen Unterlegenheit mit der Mechanik eines «take it or leave it» oder aufgrund von übermässigen Anreizen.[1264] Folglich wird die Strategie des «notice and consent» grundlegend in Frage gestellt.[1265]

966 Gleichwohl gilt die informierte Einwilligung – wie es namentlich auch an den europäischen Rechtsentwicklungen unübersehbar ist – als ein Hauptlösungsansatz zur Bewältigung datenschutzrechtlicher Herausforderungen.[1266] Das *Selbst-*

1259 BVGer 2009/44, Urteil vom 4. August 2009, E 4.2.; m. w. H. und zugleich kritisch Vasella, Jusletter vom 16. November 2015, N 14.
1260 Vgl. Art. 7 Abs. 4 DSGVO; Ingold, Nomos-Komm DSGVO, Art. 7 N 31 f.; hierzu auch Vasella, Jusletter vom 16. November 2015, N 14; m. w. H. Heuberger, N 295.
1261 Hierzu Radlanski, 14 ff.
1262 Kritisch insb. Ders., 78 ff.; zu take it or leave it Buchner, 107 ff.; Heuberger, N 295; Barocas/Nissenbaum, 1 ff.
1263 Vgl. Rogosch, 71 ff.; Barocas/Nissenbaum, 1 ff.
1264 Grundlegend Radlanski, 78 ff.
1265 Barocas/Nissenbaum, 1 ff.; Radlanski, *passim*; kritisch unlängst auch Heuberger, *passim*; kritisch hinterfragt auch durch Passadelis, Gastkommentar NZZ vom 17. Mai 2017.
1266 Vgl. Buchner, 231 ff.; Barocas/Nissenbaum, 1 ff.; illustrativ hierfür ist der Befund, wonach sich der grosse Teil wissenschaftlicher Beiträge zum Datenschutz mit der informierten Einwilligung resp.

bestimmungsparadigma zeigt sich als logische Fortsetzung und Konsequenz eines im Persönlichkeitsschutz und damit im Subjektschutz verwurzelten Datenschutzrechts mit entsprechenden Kognitionen (Degradierung des Menschen zum Informationsobjekt qua Technologie, Emanzipationsbedarf).[1267]

967 Buchner problematisierte von wissenschaftlicher Seite den Befund, wonach Personendaten über weiteste Strecken an den Datensubjekten vorbei verarbeitet würden.[1268] Die Reaktion hierauf lässt sich durchaus als Trend beschreiben, ein subjektives Recht auf informationelle Selbstbestimmung zu stärken, auszubauen, wirksam zu machen. Es geht an dieser Stelle nicht darum, in die dogmatischen Tiefen einzugehen, zumal sich für viele Fragen erst Antworten durch Lehre und Praxis konsolidieren müssen. Allerdings riskiert eine entsprechende Betrachtungsweise, den Subjektschutz so stark in den Vordergrund zu rücken, dass die systemische Schutzdimension des Datenschutzes in den Hintergrund rückt. Wie eine Lösungsstrategie der Stärkung der Einwilligungsvorgaben als Instrumentarium zur Bewältigung datenschutzrechtlicher Herausforderungen zu evaluieren ist, wird im dritten Teil vertieft analysiert. Ebenda wird auch gezeigt, dass das *Einwilligungs- und Transparenzparadigma durch weitere Strategien paradigmatischer Natur ergänzt werden.*

968 Gleichwohl nahmen in den vergangenen Jahren Anpassungen und namentlich die Stärkung sowie Ausdifferenzierung der Vorgaben für die Gültigkeit der datenschutzrechtlichen Einwilligung (ungeachtet ihrer Positionierung im System) einen prominenten Platz in den datenschutzrechtlichen Entwicklungen ein. Sowohl die DSGVO als auch die Totalrevision des DSG heben die Anforderungen an die Gültigkeitsvoraussetzungen der Einwilligung an. Mit der Totalrevision gewinnen insb. die Informationsvorgaben, aber auch die Anforderungen an die Einwilligungserklärung und damit die Ausdrücklichkeit an Bedeutung. Die ausgebauten Vorgaben sollen die datenschutzrechtliche Einwilligung effektuieren. Damit bestätigt sich denn auch, dass in den Einwilligungskonstruktionen ein Kerninstrument zur Lösung der datenschutzrechtlichen Probleme gesehen wird.

969 Um das Bild mit Blick auf die Gültigkeitsvoraussetzungen abzurunden, ist in gebotener Kürze auf eine qualifizierende Vorgabe an die Einwilligung, die *Ausdrücklichkeit*, einzugehen (vgl. hierzu bereits oben im Rahmen der Erläuterung des Widerspruchsrechts): Qualifizierend wird nach Art. 4 Abs. 5 DSG die *Ausdrücklichkeit der Einwilligung* verlangt für die Verarbeitung von besonders schutzwürdigen Angaben und Persönlichkeitsprofilen. Art. 6 Abs. 7 nDSG ver-

Selbstbestimmung resp. dem Recht an eigenen Daten befassen; vertiefend hierzu dritter Teil, VIII. Kapitel, B.

1267 Zur gesellschaftlichen Konstruktion einer normativen Leitidee der Selbstbestimmung Krähnke, 9 ff.

1268 Vgl. Buchner, 130 ff.

langt die Ausdrücklichkeit neu für teilweise andere Konstellationen. Die nachfolgenden Ausführungen beziehen sich auf die Vorgaben vor Totalrevision.[1269]

970 Auch der Passus nach noch in Kraft stehendem Gesetz ist aus materiellrechtlicher Perspektive erklärungsbedürftig, der Gesetzeswortlaut unklar. Erneut suggeriert der Gesetzgeber ebenso für diese Konstellation, dass ein Einwilligungserfordernis, und zwar in qualifizierter Form, für die Personendatenverarbeitung von besonders schutzwürdigen Angaben und Persönlichkeitsprofilen greift. Allerdings ergibt eine systematische Auslegung, die neben Art. 4 Abs. 5 erster Satz DSG zugleich auch Art. 12 Abs. 2 lit. c DSG in die Analyse miteinbezieht, selbst für diese Konstellation kein eigenständiges Einwilligungserfordernis. Hierfür spricht an erster Stelle das dargelegte System mit dem Ausgangspunkt der prinzipiellen Verarbeitungsfreiheit. Zudem wird nach Art. 12 Abs. 2 lit. c DSG erst die Weitergabe von Personendaten und Persönlichkeitsprofilen an Dritte entgegen einem Widerspruch als Persönlichkeitsverletzung taxiert. Die dergestalt qualifizierte und damit persönlichkeitsverletzende Verarbeitungshandlung kann wiederum gerechtfertigt werden. Was folgt, ist, dass keineswegs jede Verarbeitung von Personendaten, nicht einmal diejenige von besonders schutzwürdigen Personendaten oder von Persönlichkeitsprofilen einer Einwilligung bedarf. Sodann schliesst der zweite Satz an den ersten Satz von Art. 4 Abs. 5 DSG an, wobei ersterer wie gesagt die Gültigkeitsvoraussetzungen für eine Einwilligung definiert für den Fall, dass diese (andernorts) verlangt wird. Die Auslegung, wonach eine Personendatenverarbeitung von besonders schutzwürdigen Personendaten und Persönlichkeitsprofilen der Einwilligung bedarf, hat im Gesetz keine Grundlage. Lediglich eine persönlichkeitsverletzende Verarbeitung von besonders schutzwürdigen Personendaten und Persönlichkeitsprofilen – exemplarisch diejenige, welche die allgemeinen Verarbeitungsgrundsätze nicht einhält – bedarf der Rechtfertigung, beispielsweise qua Einwilligung, die alsdann ausdrücklich zu sein hat. Immerhin mag es gerade im Rahmen der Verarbeitung von Persönlichkeitsprofilen faktisch nicht selten der Fall sein, dass diese gegen die Verarbeitungsgrundsätze verstossen. Auch Art. 4 Abs. 5 zweiter Satz DSG stellt damit erhöhte Anforderungen an die Gültigkeit der Einwilligung für den Fall, dass es sich um einen persönlichkeitsverletzenden Datenumgang mit besonders schützenswerten Angaben oder Persönlichkeitsprofilen handelt.

971 Für den Fall, dass eine persönlichkeitsverletzende Verarbeitung von besonders schutzwürdigen Personendaten oder Persönlichkeitsprofilen vorliegt und die ausdrückliche Einwilligung als Rechtfertigungsgrund figuriert, fragt sich alsdann, wann die Voraussetzung der *ausdrücklichen* Einwilligung erfüllt ist. Mit der *Ausdrücklichkeit* einer Einwilligung kann Verschiedenes gemeint sein: Zum einen

1269 Zu den Neuerungen vgl. insb. Bühlmann/Schüepp, Jusletter vom 15. März 2021; Vasella, Jusletter vom 16. November 2015.

kann es um die Art resp. Form der Kundgabe der Einwilligungserklärung gehen. Zum anderen kann sich das Adjektiv «ausdrücklich» nicht auf die Kundgabe, die Erklärung der Einwilligung, sondern auf den Inhalt der datenschutzrechtlichen Einwilligung beziehen. Problematisch in dieser Lesart sind dann Einwilligungen anhand von AGB, die sich auch, aber keineswegs nur auf die Datenverarbeitung beziehen.[1270] Epiney verschränkt die beiden Lesarten, indem sie verlangt, dass die Einwilligung nach Inhalt wie nach Form ausdrücklich zu sein hat.[1271] Nach wohl herrschender Schweizer Lehre wird «ausdrücklich» als Gegenbegriff zu stillschweigend resp. konkludent verstanden.[1272] Hält man sich vor Augen, dass zahlreiche Einwilligungen online und formulartechnisch erfolgen, wobei sich Nutzende in aller Regel passiv verhalten, sollte unter der Voraussetzung der Ausdrücklichkeit die *aktive Erklärung* verlangt werden.[1273] Ist neben dem einschlägigen Text ein leeres Kästchen angebracht und muss die Einwilligung aktiv gesetzt werden, ist von einer ausdrücklichen Einwilligung auszugehen. Nicht als ausdrücklich gelten kann indes eine Modalität, in der die Checkbox leer ist und das Leerlassen als vermutete Einwilligung gilt. Epiney ist sodann zuzustimmen, dass sich die ausdrückliche Einwilligung, sprich, die aktive Einwilligungserklärung eindeutig auf die datenschutzrechtliche Dimension und deren Inhalt beziehen muss. Sind datenschutzrechtlich mehrere Prozesse und namentlich Verarbeitungszwecke relevant, sind weiter die Erklärungen entsprechend ausdifferenziert zu gestalten und hierfür jeweils separat ausdrückliche Einwilligungen einzuholen. Mit einer so verstandenen *Ausdrücklichkeitsvorgabe* wird ein Konzept der Relativität und Ausdifferenzierung von Einwilligungsvorgaben konkretisiert. In eine solche Richtung scheint auch die Argumentation des EDÖB im Schlussbericht Postfinance zu zielen.[1274]

972 Damit die Analyse im Sinne der bisherigen Systematisierung dieser Arbeit abgerundet wird, ist zum Abschluss der Ausführungen zu den Gültigkeitsvoraussetzungen der Einwilligung (mit einer Abgrenzung zum Einwilligungserfordernis an sich) ein *struktureller Aspekt der Thematik* zu adressieren: Mit Blick auf die Anforderungen an die Gültigkeit datenschutzrechtlicher Einwilligungen wird hinsichtlich der erforderlichen Granularität von Information und Erklärungsinhalt vertreten, dass diese umso höher ist, je sensibler die Angaben resp. je

1270 In diese Richtung EDÖB, Schlussbericht vom 1. Juni 2015 i. S. PostFinance, 1 ff., 24 f.
1271 Epiney, in: Rumo-Jungo/Pichonnaz/Hürlimann-Kaup/Fountoulakis (Hrsg.), 97 ff., 103; Dies., in: Belser/Epiney/Waldmann (Hrsg.), § 9 N 19; Meier, N 899.
1272 M. w. H. Vasella, Jusletter vom 16. November 2015, N 25 ff.
1273 So auch WP 29/259, Consent, 20 f.
1274 Vgl. mit Blick auf die Ausdrücklichkeit und den Schlussbericht vertiefend Jusletter vom 16. November 2015, N 23; zur Problematik der globalen resp. «überschiessenden» Einwilligung, indes nicht spezifisch mit Blick auf die qualifizierenden Gültigkeitsvoraussetzungen der Ausdrücklichkeit der Einwilligung für den Fall von Art. 4 Abs. 5 zweiter Satz: BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, vgl. insb. E 4.8.3.

weitreichender eine Datenverarbeitung und deren Folgen sind.[1275] Eine entsprechende Relativität und Nuancierung fliesst, wie erörtert, über sämtliche Gültigkeitsvoraussetzungen ein, namentlich die Urteilsfähigkeit, die Informiertheit und Ausdrücklichkeit (sofern qualifizierend verlangt), aber auch die Freiwilligkeit. Gerade in der Anknüpfung der «Granularitätsvorgaben» resp. «Nuancierungsvorgaben», der Relativität und Staffelung bezüglich der Einwilligung lässt sich erneut ein Konzept einer abstrakten Bestimmung der Natur von Personendaten erkennen. Auch hier bilden sich Relikte der Sphärentheorie ab. Das DSG bleibt selbst an dieser Stelle, wo es um einen Mechanismus zur Integration der Entscheidungsfreiheit des Subjektes geht, einer Konstruktion verhaftet, welche das Schutzniveau gewissermassen anhand der *Natur* gewisser Angaben als «mehr oder minder sensibel» vornimmt.

973 Dass eine abstrakte Definierung der Schutzwürdigkeit dem Konzept des DSG entspricht und diese sich ebenso auf die Anforderungen im Rahmen der Einwilligung niederschlägt, wird u. a. von Vasella vertreten.[1276] Er kritisiert Ansätze, wonach die «Natur» personenbezogener Angaben nicht abstrakt zu bestimmen, stattdessen auch auf den *Verarbeitungszusammenhang abzustellen sei*, was namentlich vonseiten des EDÖB vertreten werde.[1277] Auch diese Schrift hat an mehreren Stellen einen entsprechenden Ansatz des DSG freigelegt. Etwas allgemeiner wurde wiederholt sichtbar, wie kontextuelle Bezugspunkte ebenso im DSG angelegt sind.

974 Es folgt eine Zusammenfassung der Kernerkenntnisse zum *Rechtfertigungsregime gemäss DSG*. Im Anschluss werden Einwilligungskonstruktionen aus einer erweiterten Perspektive beleuchtet. Es geht ebenda darum, die relative und kontextrelationale Bedeutung datenschutzrechtlicher Normen und die Einschlägigkeit spezifischer Differenzierungen anhand anderer Einwilligungskonstruktionen hinsichtlich des Umgangs mit Personendaten freizulegen. Hier wird sich zeigen, dass es in Bezug auf den Umgang mit Personendaten verschiedene Regelungen gibt.

5. Resümee zu den Rechtfertigungsgründen

975 Die datenschutzgesetzlichen Rechtfertigungsgründe entsprechen dem Regime, wie es im Persönlichkeitsschutz des ZGB vorgesehen wird, vgl. Art. 28 Abs. 2 ZGB und Art. 13 Abs. 1 DSG resp. Art. 31 nDSG. Die mit Blick auf die datenschutzrechtlichen Rechtfertigungsgründe lange im Zentrum der Diskussionen stehende Frage, wie die uneinheitliche Fassung des Gesetzestextes in den Art. 12

1275 Rampini, BSK-DSG, Art. 13 N 3; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 16; Botschaft DSG 2013, 2127.
1276 M. w. H. auf die weiteren Lehrmeinungen Vasella, Jusletter vom 16. November 2015, N 7.
1277 Ders., a. a. O., N 5.

Abs. 2 lit. a–c DSG zu interpretieren sei, gilt als geklärt. Für sämtliche Tatbestände ist die Möglichkeit der Rechtfertigung grundsätzlich zuzulassen; allerdings hat dies namentlich bei einem Verstoss gegen den «Integritätsschutz» gemäss Art. 12 Abs. 2 lit. a DSG mit Zurückhaltung zu erfolgen. Nach Totalrevision werden die Tatbestände der Persönlichkeitsverletzung konsequent in Art. 30 nDSG, die Rechtfertigungsgründe in Art. 31 nDSG niedergelegt. Die gebotene Zurückhaltung der Rechtfertigungsmöglichkeit in Bezug auf die wichtigsten Verarbeitungsgrundsätze, Art. 6 und Art. 8 nDSG, ist weiterhin angezeigt.

976 Wenig Anlass zu Schwierigkeiten scheinen die *gesetzlichen Rechtfertigungsgründe* zu geben. Immerhin wird das letzte Kapitel dieser Studie zeigen, dass dies ein Trugschluss ist. Für sie wurde eine *Brückenfunktion* beschrieben, indem legitimierende Gesetzestatbestände ausserhalb des DSG der Funktionstüchtigkeit und dem Schutz der Integrität jeweils spezifischer Kontexte mit ebenda zu erreichenden Zielen dienen.

977 Als neuralgisch gelten in der datenschutzrechtlichen Debatte die *überwiegenden Interessen*, die als «Supergeneralklauseln» oder Blanko-Ermächtigungsnormen zur nahezu unbeschränkten Geltendmachung verführen. In Bezug auf die überwiegenden Interessen wurde vertreten, dass ein isolierter Blick auf wirtschaftliche Interessen zu kurz greift; vielmehr ist stets zu analysieren, welche Ziele und Zwecke im Rahmen der Verarbeitungskontexte, in welche die persönlichkeitsverletzenden Verarbeitungshandlungen eingebettet sind, verfolgt werden. Der Kontextbezug ist im Gesetz mit den Enumerationen gemäss Art. 13 Abs. 2 DSG resp. Art. 31 Abs. 2 nDSG angelegt. Somit wurde dafür plädiert, die überwiegenden Interessen aus einer isolierten Perspektive individueller Interessen der Verantwortlichen zu lösen und einer kontextuellen Einbettung zuzuführen. *De lege ferenda* sind sie in eine Richtung zu strukturieren, welche die diversen Verarbeitungszusammenhänge mit den (direkten und indirekten) kontextuellen Zielen und Zwecken harmonisiert. Ein rein wirtschaftliches Interesse der Verantwortlichen, das nahezu für jede Personendatenverarbeitung aufführbar ist, kann isoliert *nur* ausnahmsweise als überwiegend gelten.

978 Folgerichtig zum Ausgangspunkt der grundsätzlichen Verarbeitungsfreiheit mit Schranken integriert das DSG für den privaten Bereich den *Willen des Datensubjektes* (neben dem Widerspruch) – insb. als *rechtfertigende Einwilligung* gegenüber qualifizierten und damit persönlichkeitsverletzenden Personendatenverarbeitungen. Die Ausführungen hierzu bestätigten, dass es fehlgeht, das System des DSG für den privaten Bereich als eines der informationellen Selbstbestimmung zu qualifizieren, wie es in seinem Gehalt vom Bundesverfassungsgericht in dessen Volkszählungsurteil geprägt wurde. Art. 4 Abs. 5 DSG statuiert kein eigenständiges Einwilligungserfordernis, stattdessen die Gültigkeitsvorgaben für die Einwilligung, sofern diese gefordert wird. Dasselbe gilt nach Totalrevision für Art. 6

Abs. 6 und Abs. 7 nDSG. Allgemein ist in der Stärkung der Transparenzvorgaben und der Einwilligungsvorgaben ein Lösungsansatz zu verorten, welcher die jüngsten datenschutzrechtlichen Entwicklungen mitprägt.

979 Dargestellt wurden die *einzelnen Gültigkeitsvoraussetzungen* der rechtfertigenden Einwilligung. Insofern wurde vor Augen geführt, dass die *Tauglichkeit* von Einwilligungskonstruktionen zur Lösung datenschutzrechtlicher Herausforderungen mit ihren Gültigkeitsvorgaben (Urteilsfähigkeit, Informiertheit und Freiwilligkeit, qualifizierend ggf. Ausdrücklichkeit) im Lichte der datenschutzrechtlichen Realität in jüngster Zeit ebenso *kritisch* thematisiert wird. Für die datenschutzrechtliche Einwilligung, die im DSG primär als Rechtfertigungsgrund figuriert, wurde zudem gezeigt, inwiefern auch hier das DSG in erster Linie von einer abstrakten Qualifizierung von Personendaten – quasi anhand ihrer Natur – als besonders schutzwürdig oder sensibel ausgeht, worin sich erneut die Verhaftung in der Sphärentheorie spiegelt. Das Datensubjekt, die Person und Persönlichkeit, wird bis heute als ein *einheitliches Subjekt perzipiert*, wobei ihm Personendaten quasi abstrakt qualifiziert und objekthaft zugeordnet werden anhand der um die Person gelegten konzentrischen Kreise.[1278] Der datenschutzgesetzlich geschützte Autonomieraum zeigt sich zumindest auf den ersten Blick als wenig ausdifferenziert. Erweitert man die Betrachtung über das DSG hinaus, werden die *ausdifferenzierten Autonomiebereiche resp. abgestuften Schutzpositionen in Bezug auf den Willen im Umgang mit Personendaten* sichtbar.

6. Diversifizierte Autonomien, plurale Verarbeitungskontexte

6.1. Bezugsrahmen

980 Nachgewiesen wurde, dass das DSG für den privaten Bereich kein Regime der informationellen Selbstbestimmung verankert (isoliert oder alternativ zu anderen Erlaubnistatbeständen), aus welchem ein prinzipielles Verarbeitungsverbot abgeleitet wird und die Einwilligung entsprechend einen Erlaubnistatbestand für die nicht qualifizierte Personendatenverarbeitung darstellt.[1279] Das Konzept des DSG lässt sich aufgrund des Ausgangspunktes der Freiheit der Personendatenverarbeitung mit Schranken am trefflichsten als Konzept des *Integritätsschutzes* be-

1278 Ein interessantes Erklärungsmuster könnte bei Page, 27, aufgespürt werden: Der Autor weist auf die Unterscheidung zwischen der individuellen Person, Selbstbestimmung sowie der sozialen Person hin. Wenn im Privatheitsschutz und Datenschutzrecht das Individuum mit seiner Autonomie in den Vordergrund gerückt wird sowie die gesamte Bedrohungslage für das Recht in der Technik verdichtet wird, dann rückt fast zwingend die Relevanz des Menschen, eingebunden in seine sozialen Realitäten und damit auch agierend in verschiedenen sozialen Rollen, in den Hintergrund.

1279 Zur Lehre und Rechtsprechung, die nicht unwesentlich zur Verwirrung mit Blick auf die Qualifizierung des Regimes des DSG für den privaten Bereich beigetragen haben, vertiefend dritter Teil, VII. Kapitel, A.

schreiben. In diesem wird der Wille des Subjektes als Ausdruck eines Autonomieschutzes zurückgestuft. Er figuriert lediglich als Widerspruch resp. rechtfertigende Einwilligung (gegenüber qualifizierten und damit persönlichkeitsverletzenden Personendatenverarbeitungen). Ein Recht an eigenen Daten im Sinne eines Herrschaftsrechts des Datensubjektes findet damit im Gesetz keine Verbürgung.[1280]

981 Ebendieser Befund wird nachfolgend weiter untermauert. Zwei Themen werden hierzu aufgegriffen: Erstens geht es um die Konstruktion und Gestaltung des *zivilrechtlichen Rechts am eigenen Bild*. Zweitens werden die für den Kontext des *Biomedizinrechts* spezialgesetzlich vorgesehenen Einwilligungskonstruktionen zum Umgang mit Personendaten dargestellt.

982 Mit dieser Betrachtung der erweiterten Landschaft von Einwilligungskonstruktionen im Zusammenhang mit Personendaten wird gezeigt, inwiefern das Recht den Willen des Datensubjektes zur Regulierung von Personendatenverarbeitungen differenziert einsetzt. Hinsichtlich der Ordnung des DSG lassen sich daraus weitere Erkenntnisse zu Ziel und Funktion nicht nur der Einwilligung des Datensubjektes generieren, sondern darüber hinausgehend für das *Datenschutzrecht – das mehr ist als das DSG – an sich*.

983 Gezeigt werden soll, dass es ein «einheitliches» Datensubjekt mit einer «einheitlichen Autonomie und Selbstbestimmung» nicht gibt. Vielmehr präsentiert sich das Datensubjekt vor dem Hintergrund verschiedener Verarbeitungszusammenhänge und unterschiedlicher Bereiche in *unterschiedlichen Rollen mit differenzierten Autonomieräumen*. Das Schweizer Recht ist gemäss einer integrativen Betrachtung der Rechtslandschaft, die sich mit dem Umgang mit Personendaten befasst, weit davon entfernt, dem Datensubjekt eine einheitlich strukturierte Entscheidungsbefugnis hinsichtlich des Umgangs mit «seinen» Personendaten einzuräumen.

6.2. Das Recht am eigenen Bild – gerichtlich anerkanntes Sonderregime

984 Die rechtliche Ausdifferenzierung der Autonomiegrade hinsichtlich des Umgangs mit Personendaten wird – *erstens* – sichtbar, wenn die Betrachtung der Normierung im DSG um diejenige des sog. *Rechts am eigenen Bild* ergänzt wird.[1281]

1280 Zur Diskussion auch unter dem Titel eines Eigentums an Personendaten u. a. Thouvenin, SJZ 2017, 21 ff.

1281 Vertiefend hierzu Bächli, *passim*; jüngst namentlich in Bezug auf die Publikation des Bildnisses von Kindern durch ihre Eltern Fankhauser/Fischer, in: Fankhauser/Reusser/Schwander, 193 ff.; Vogt/Wiget, in: Arter/Jörg (Hrsg.), 129 ff., insb. 142 ff.; zum Bildnis resp. Portrait vgl. auch den geschichtswissenschaftlichen Beitrag von Mayer, 11 ff.; interessant mit Blick auf den rechtlichen Bildnisschutz der Beitrag der Historikerin Dommann, in: Joly/Visman/Weitin (Hrsg.), 249 ff.; zum Recht am eigenen Bild im System des deutschen allgemeinen Persönlichkeitsrechts vgl. Helle, 45 ff., 47 mit dem Hinweis, dass das Schutzobjekt dieses besonderen Persönlichkeitsrechts ein Selbstbestimmungsrecht des Abgebildeten darstellt; zum Recht am eigenen Bild und weiteren Per-

Die Erstellung, Verbreitung und Speicherung des Abbildes eines Menschen ist unbestritten eine Bearbeitung von Personenangaben gemäss DSG, wobei sich das Bundesgericht in den letzten Jahren wiederholt mit dem rechtlichen Schutz des Bildnisses auch im Kontext der neuen Informationsverarbeitungstechnologien zu befassen hatte, beispielsweise in seinem Entscheid zu «Google Street View»;[1282] zudem war es mit dem Thema der Video-Observation in verschiedenen Kontexten beschäftigt. Es geht an dieser Stelle darum, die Grundstruktur des Rechts am eigenen Bild in seinem Kontrast zur allgemeinen Ordnung des DSG darzulegen. Basierend auf der bundesgerichtlichen Rechtsprechung gilt für das Recht am eigenen Bild eine spezifische Ordnung. Sie ist historisch mitbedingt: Das Abbild des Menschen in Gestalt des Portraits, die Fotografie und eventuelle Reproduktionen sowie die resultierenden rechtlichen Herausforderungen im Umgang mit Bild- und Videomaterial sind älter als (digitale) Personendatenverarbeitungen, wie man sie mit dem DSG adressieren wollte. 985

Das Abbild(en), das Bildnis des «Menschen», das gewissermassen die Person eins zu eins repräsentiert, kann als Ursituation der Personendatenverarbeitung bezeichnet werden. Weil die Person gewissermassen «kopiert» wird, findet das Bildnis wie keine andere «Personenangabe» eine Assoziation mit dem Menschen, der Person als «Ganzes». Kontrastreich insofern die informationelle Fragmentierung des Menschen, wie sie durch die digitalen Technologien erfolgt. Der rechtliche Bildnisschutz wird bis heute auf Art. 28 ZGB abgestützt. Insofern hat sich eine besondere Schutzwürdigkeit herausgebildet, die mit dem «Näheverhältnis» des Abbildes zu seiner Person zu erklären ist. 986

Im historischen Entscheid «Hodler auf dem Totenbett», BGE 70 II 127, wehrte sich die Witwe von Hodler gegen die Ausstellung eines Gemäldes von Schürch, einem Schüler – dem Lieblingsschüler – von Hodler. Das Bild stellt Hodler auf dem Totenbett dar. Die Witwe ging gegen den Galeristen Kaspar vor und verlangte, dass das Bild mangels Zustimmung der Familie nicht gezeigt werde. Die Witwe berief sich in ihrer Klage – mangels anerkannten postmortalen Persönlichkeitsschutzes – auf die Verletzung ihrer eigenen Pietätsgefühle sowie ihrer psychischen und emotionalen Integrität. Zudem störte sie sich daran, dass man mit dem intimen Abbild auch noch Geld verdienen wollte. Das Bundesgericht hatte in der Folge die eigentumsrechtliche Position des Galeristen am Bild sowie die Interessen der Öffentlichkeit an Kunst und Kulturgütern gegenüber den Interessen der Witwe abzuwägen. Es beurteilte diejenigen der Witwe als überwie- 987

sönlichkeitsmerkmalen, insb. mit Blick auf ihre kommerzielle Nutzung und das Right to Publicity, Bergmann, Loyola of Los Angeles ELR 1999, 479 ff., 484 ff.; zum Recht am eigenen Bild auch Ladeur, ZUM 2000, 879 ff.; Seemann, 136 ff., handelt das Recht am eigenen Bild, gemeinsam mit dem Recht am eigenen Namen, unter dem Titel der Publizitätsrechte im deutschen Recht ab; Lüthy, 74 ff.; Lévy, 27 ff., auch zur Verwertungskomponente, 291 ff.

1282 Vgl. BGE 138 II 346, insb. E 6.

gend. Es entbehrt nicht einer gewissen Ironie des Schicksals, dass just die Ehefrau des Künstlers sich mit Erfolg gegen etwas zur Wehr setzte, was ebendieser zu Lebzeiten getan hatte und ihn auch berühmt gemacht hatte: Hodler war es, der minutiös und erschütternd den Zerfall seiner Geliebten Valentine Godé-Darrel dargestellt hatte. Dieser intime, verstörende Zyklus, der mit der Darstellung von Valentine auf dem Totenbett endet, gilt als (s)ein Meisterwerk.[1283]

988 Jahrzehnte später hielt BGE 127 III 481 fest, dass niemand ohne seine Zustimmung abgebildet werden dürfe, sei es durch Zeichnung, Gemälde, Fotografie, Film oder ähnliche Verfahren. Das dergestalt anerkannte Recht am eigenen Bild galt als Konkretisierung des Persönlichkeitsrechts, Art. 28 Abs. 1 ZGB.[1284]

989 Mit dem Recht am eigenen Bild befasste sich das Bundesgericht weiter im Google-Street-View-Entscheid, BGE 138 II 364: Der EDÖB hatte gegen Google geklagt und verlangt, dass Bilder des Dienstes Google Street View nur veröffentlicht werden dürfen, wenn Gesichter und Autokennzeichen vollständig unkenntlich gemacht worden seien. Inhaltlich gelte das Recht am eigenen Bild, so das Bundesgericht in E 8.2. unter Zitierung von Bächli, als *Selbstbestimmungsrecht*. Ebendieses schütze vor der widerrechtlichen Verkörperung des eigenen Erscheinungsbildes. Einen ersten Teilgehalt bilde der Abwehranspruch gegen gezieltes, auf Identifikation und Ausforschung gerichtetes Erstellen von Fotos etc. Der zweite Teilgehalt bestünde in einem Recht auf Selbstbestimmung des Menschen hinsichtlich der Veröffentlichung des eigenen Bildes, insb. des Porträts, und seiner Verwendung in kommerzieller oder politischer Werbung.

990 Obschon es sich beim Abbild einer Person um eine Personenangabe handelt, *übersteuert das Recht am eigenen Bild die Regelung gemäss DSG*. Über die etablierte bundesgerichtliche Rechtsprechung zum Recht am eigenen Bild wird für das Bildnis der Person der entgegengesetzte Ausgangspunkt zum Regime des DSG im privaten Bereich anerkannt. Das Recht am eigenen Bild geht von einem Grundsatz des Verarbeitungsverbotes mit Erlaubnisvorbehalt aus. Jede Verarbeitungshandlung (und nicht erst qualifizierte Verarbeitungshandlungen) mit Blick auf das Bildnis – das Erstellen, Speichern, Weiterleiten oder Veröffentlichen – ist prinzipiell verboten, es sei denn, es läge ein Legitimationsgrund, namentlich die Einwilligung, vor.

991 Ungeachtet dessen, dass das Bildnis eines Menschen, sein Abbild, ein personenbezogenes Datum im Sinne des DSG ist – das hat BGE 127 III 481 festgehalten –,

1283 Ein Maler vor Liebe und Tod. Ferdinand Hodler und Valentine Godé-Darel. Ein Werkzyklus. Kunsthaus Zürich; Kunstverein St. Gallen; Villa Stuck, München; Kunstmuseum Bern, 1976/1977.

1284 Vgl. zur Einwilligung im Rahmen des Rechts am eigenen Bild BGE 136 III 401, E 5 und E 6; zum Right to Publicity und der Bedeutung der Einwilligung auch für die kommerzielle Nutzung des Abbildes Bergmann, Loyola of Los Angeles ELR 1999, 479 ff., 488; vgl. auch Seemann, 66 ff.; Lévy, 112.

gilt eine gerichtlich etablierte und vom gesetzlichen Regime abweichende *Sonderordnung resp. Spezialregelung*. Das grundsätzliche Verarbeitungsverbot mit Erlaubnisvorbehalt im Rahmen des Rechts am eigenen Bild nach schweizerischer Judikatur, das Gesetz derogierendes Recht ist somit strukturell näher an der Konzeptionierung gemäss Art. 6 DSGVO.

992 Gleichzeitig erhärtet diese (gerichtlich etablierte) Spezialregelung zum Bildnis, dass die Schweiz in ihrem allgemeinen Datenschutzrecht, wie es das DSG als Querschnittsgesetz liefert, für den privaten Bereich mit der grundsätzlichen Verarbeitungsfreiheit mit Schranken *kein* Regime der Selbstbestimmung vorsieht. Das Recht am eigenen Bild mit seiner Konkretisierung durch das Bundesgericht repräsentiert ein gegenüber der allgemeinen Ordnung des DSG für den privaten Bereich spezifisches Regelungssystem. Dass mit dem Recht am eigenen Bild ein grundsätzliches Verarbeitungsverbot mit Erlaubnistatbestand und aufgewerteter Relevanz der Einwilligung anerkannt wird, ist kognitiv nachvollziehbar: Das Bildnis ist keine fragmentierte Informationseinheit, stattdessen fängt es eine Person gesamthaft ein und schafft ein «Antlitz der analogen Welt». Das Abbild der Person, das diese wie eine Kopie repräsentiert, ist ihr so «nah», dass nicht erst qualifizierte Bearbeitungen, sondern jede Verarbeitungshandlung verboten ist, es sei denn, es läge ein Erlaubnistatbestand vor. Das Recht am eigenen Bild mit seiner bundesgerichtlichen Konkretisierung kann mit Fug und Recht als Selbstbestimmungsrecht bezeichnet werden.

993 Anzufügen bleibt, dass mit der Teilrevision des Urheberrechtsgesetzes, die am 27. September 2019 verabschiedet wurde, der Bildnisschutz neu geregelt wird. Die Revision will das Urheberrecht an das Zeitalter der Digitalisierung heranführen.[1285] Insofern ist auf einen neu weit gefassten Bildnisschutz hinzuweisen, demgemäss Fotografien, sofern selbst angefertigt, urheberrechtlich geschützt werden.[1286] Die Regelung hat Bedeutung für den Umgang mit sog. Selfies.

6.3. Gesetzliche Spezialnormen – Einwilligung im Biomedizinrecht

994 Bezüglich der *Diversifizierung von Autonomiepositionen in Bezug auf Personendaten und damit datenschutzrechtliche Autonomiepositionen* sind – *zweitens* – vom DSG abweichende, spezifische gesetzliche Einwilligungskonstruktionen einschlägig. Sie finden sich im Zivil- und Privatrecht, insb. im ZGB resp. OR sowie in Spezialgesetzgebungen. Solche Erlasse und Normen legiferieren *kontext-*

1285 Vgl. für eine Übersicht IGE, Die eidgenössischen Räte heissen die Teilrevision URG gut, Bern 2019, <https://www.ige.ch/de/recht-und-politik/immaterialgueterrecht-national/urheberrecht/revision-des-urheberrechts/parlamentarische-beratung.html#c66462> (zuletzt besucht am 30. April 2021); Parlament, Urheberrechtsgesetz, Änderung, Bern 2019, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20170069 (zuletzt besucht am 30. April 2021).

1286 Kritisch zu einem «irrlichtenden Bildnisschutz» Schmidt-Gabain, NZZ vom 26. Januar 2018.

oder bereichsspezifisch in Ergänzung zum resp. Abweichung vom DSG, auch in Bezug auf die Bedeutung der Einwilligung des Datensubjektes. Der Umgang mit Personendaten wird in mehreren Erlassen ausserhalb des DSG adressiert. Exemplarisch zu nennen sind die familieninformationsrechtlichen Bestimmungen gemäss ZGB, insb. im Adoptionsrecht.

995 Im (weiten) Feld des (Bio-)Medizinrechts finden sich in verschiedenen Spezialgesetzen zahlreiche informations- und datenschutzrechtliche Vorgaben.[1287] Verfassungsrechtlich relevant ist in diesem Zusammenhang insb. Art. 119 Abs. 2 lit. f BV, der hinsichtlich Untersuchung, Registrierung oder Offenbarung des Erbgutes einer Person deren vorgängige Zustimmung fordert. Eine elaborierte und eigenständige Ordnung zur Verarbeitung von Personendaten («Gesundheitsdaten») verankern das Humanforschungsgesetz (HFG)[1288] und das Bundesgesetz über genetische Untersuchungen beim Menschen (GUMG).[1289]

996 Das Humanforschungsgesetz befasst sich mit der Forschung am Menschen, vgl. Art. 2 lit. a–c HFG. In diesem Kontext regelt es ebenso den Umgang mit gesundheitsbezogenen Angaben, vgl. Art. 1 lit. e HFG. Das HFG liefert folglich insofern eine *lex specialis* bezüglich DSG. Die Ordnung des HFG ist nuanciert. Das Gesetz differenziert danach, ob es um die Forschung mit gesundheitsbezogenen Personendaten geht oder ob gesundheitsbezogene Personendaten für Forschungsprojekte *weiterverwendet* werden.[1290] An diese Kategorisierung schliesst ein differenziertes Einwilligungssystem an. Der Gesetzgeber definiert strengere Anforderungen für die zuerst genannte Konstellation, weil er diese als risikoträchtiger beurteilt. Werden dagegen bereits erhobene gesundheitsbezogene Personendaten zu *Forschungszwecken* weiterverwendet, sei das Gefahrenpotential geringer. Ebendies erlaube eine pragmatischere Lösung.[1291] Die Forschung mit gesundheitsbezogenen Personendaten gilt als Forschung am Menschen und wird im 2. Kapitel des HFG geregelt: Ebendiese Forschung bedinge die Erhebung der entsprechenden personenbezogenen Gesundheitsdaten, was einen stärkeren Eingriff in die Rechte der betroffenen Person darstelle. Entsprechend ist nach Art. 16 Abs. 1 HFG die Forschung mit gesundheitsbezogenen Personendaten (die nicht weiterverwendet, stattdessen erhoben werden) grundsätzlich nur zulässig, wenn die Person nach

1287 Vgl. zum Bioinformationsrecht Gruber, *passim*.

1288 SR 810.30; hierzu jüngst grundlegend Karavas, Körperverfassungsrecht, 211 ff.; vgl. auch Art. 119 Abs. 2 lit. f BV.

1289 SR 810.12; zur fehlenden Legaldefinition von Gesundheitsdaten und zu den einschlägigen Normen vgl. auch do Canto, sic! 2020, 177 ff., 179 f.; vgl. sodann die Beschreibung der Datenströme mit Blick auf Gesundheitsdaten im Zusammenhang mit der Gesundheitsversorgung durch Spitäler Gogniat, Jusletter vom 20. Juni 2016, N 16.

1290 Zum Ganzen vertiefend und kritisch Karavas, Körperverfassungsrecht, 154 ff.; vgl. zur Relevanz der Unterscheidung der verschiedenen Kontexte auch Simitis, in: Brem/Druey/Kramer/Schwander (Hrsg.), 469 ff., 491 f.

1291 Botschaft vom 21. Oktober 2009 zum Bundesgesetz über die Forschung am Menschen, BBI 2009 8082; kritisch hierzu Karavas, Körperverfassungsrecht, 219 ff.

hinreichender Aufklärung in das *konkrete Forschungsprojekt* eingewilligt hat. Die Anforderungen an die Informiertheit der Einwilligung resp. die reziproken Aufklärungspflichten werden in Art. 16 Abs. 2 lit. a–e HFG detailliert konkretisiert. Die Einwilligung hat prinzipiell schriftlich zu erfolgen; die Gültigkeit verlangt nach Art. 16 Abs. 3 HFG zudem die Einhaltung einer Bedenkfrist zwischen Aufklärung und Einwilligung.[1292] Anders wird die *Weiterverwendung* von gesundheitsbezogenen Personendaten im 4. Kapitel des HFG geregelt. Auch hier lässt sich ein differenziertes Regime feststellen. Nach Art. 17 HFG bedarf es der Einwilligung der betroffenen Person resp. des Hinweises auf ein Widerspruchsrecht im Zeitpunkt der Erhebung, sofern in diesem Moment feststeht, dass die Information später dem Forschungszweck zugeführt wird. Ein «Versäumnis» kann geheilt werden, sofern gemäss Art. 17 HFG die Einwilligung spätestens vor der Weiterverwendung gemäss Art. 32 bzw. Art. 33 HFG eingeholt wird.[1293]

997 Ebenda, in den Art. 32 f. HFG, finden sich nuancierte Modalitäten der Einwilligung, je nach Art der Daten und des Datenumgangs: Differenzierungskriterien sind die Kategorisierungen von genetischen Daten versus gesundheitsbezogenen Daten sowie die Bearbeitung in unverschlüsselter, verschlüsselter oder anonymisierter Form. Art. 32 HFG befasst sich mit den *genetischen Daten* (sowie dem biologischen Material): Eine Weiterverwendung der genetischen Daten in *unverschlüsselter Form* bedarf nach Art. 32 Abs. 1 HFG eine Einwilligung nach hinreichender Aufklärung der betroffenen Person resp. der gesetzlichen Vertretung oder der nächsten Angehörigen über das geplante und konkrete Forschungsprojekt. Nach Art. 32 Abs. 2 HFG genügt eine Generaleinwilligung, sofern die Weiterverwendung genetischer Angaben in *verschlüsselter Form* vorgesehen ist. Werden genetische Daten in *anonymisierter* Form weiterverwendet, genügt der Hinweis auf ein Widerspruchsrecht, vgl. Art. 32 Abs. 3 HFG; eine formularmässige Informierung, beispielsweise mittels einer Patienteninformationsbroschüre des Spitals, soll zulässig sein.[1294] Die Weiterverwendung von *nicht-genetischen Gesundheitsdaten* wird nach Art. 33 HFG unter ein minder strenges Zustimmungsregime gestellt: Eine Generaleinwilligung ist bei der Weiterverwendung solcher Daten in *unverschlüsselter Form einzuholen*, Art. 33 Abs. 1 HFG, wohingegen die Informierung über das Widerspruchsrecht bei der Weiterverwendung in *verschlüsselter Form statuiert wird*, Art. 33 Abs. 2 HFG; eine Weiterverwendung in anonymisierter Form wird voraussetzungslos zugelassen.

1292 Weitere erhöhte Voraussetzungen an die Aufklärung und Einwilligung werden spezifisch für sog. «besonders verletzbare Personen», beispielsweise Kinder, schwangere Frauen oder Personen im Freiheitsentzug, formuliert, vgl. Art. 7 Abs. 1 i. V. m. Art. 16 Abs. 1, Art. 26 und Art. 28 Abs. 1 HFG.

1293 M. w. H. Karavas, Körperverfassungsrecht, 153 f.

1294 Botschaft Humanforschungsgesetz 2009, 8045 ff., 8122; zum Ganzen Karavas, Körperverfassungsrecht, 155.

998 Das HFG sieht entsprechend ein abgestuftes und differenziertes Regelungskonzept vor im Kontext der Forschung und der Weitergabe von gesundheitsbezogenen resp. genetischen Angaben zu Forschungszwecken.[1295] Es geht an dieser Stelle nicht darum, eine Bewertung dieses Systems abzugeben. Vielmehr taugt dieser Blick auf die datenschutzrechtlichen Bestimmungen im HFG dazu, *dreierlei* (weiter) freizulegen und zu verdeutlichen:

999 *Erstens* lässt sich anhand der Einwilligungsvorgaben im Bereich der Forschung mit gesundheitsbezogenen genetischen und nicht-genetischen Daten des HFG bestätigen, dass das allgemeine System des DSG für den privaten Bereich gerade *keines der informationellen Selbstbestimmung* ist. Während das HFG die Einwilligung grundsätzlich als Voraussetzung zulässiger Verarbeitung verlangt – oft mit qualifizierten formellen wie informationellen Anforderungen –, genügt der Widerspruch nur ausnahmsweise. Damit liegt diesem auch datenschutzrechtlich einschlägigen, bereichsspezifischen Spezialgesetz ein prinzipielles Verarbeitungsverbot als Basisannahme zugrunde. Anders funktioniert dagegen, wie gezeigt, das System im DSG für den privaten Bereich.

1000 *Zweitens* wird mit dieser gegenüber der allgemeinen Ordnung des DSG hoch ausdifferenzierten Normierung des Umgangs mit Personendaten im Forschungskontext nach HFG dokumentiert, dass das Schweizer Datenschutzrecht – trotz der Querschnittsgesetzgebung mit dem DSG – einen *sektor- und bereichsspezifischen Ansatz* kennt.[1296] Dass das Datenschutzrecht der Schweiz – trotz der persönlichkeitsrechtlichen Anknüpfung des DSG – *systemspezifische Erwägungen* als datenschutzrechtlich einschlägiges Gestaltungselement anerkennt, wurde an diversen weiteren Stellen herausgeschält, z. B. im Rahmen der Darstellung des Dualismus im DSG, des Rechtmässigkeitsprinzips sowie des Zweckbindungsgrundsatzes, der Rechtfertigungsgründe qua Gesetz oder überwiegenden Interessen.

1001 Dass die Differenzierung je nach einbettenden *Verarbeitungszusammenhängen* datenschutzrechtlich als einschlägig anerkannt wird, erhärtet sich mittels der Gegenüberstellung des DSG mit dem HFG sowie der Regelung innerhalb des HFG selbst. Spezifisch für den *Forschungskontext* wird ein gegenüber dem DSG eigenständiges Regelungsregime im Umgang mit gesundheitsbezogenen und genetischen Personendaten verankert. Innerhalb des HFG wird zudem erneut differenziert: Werden gesundheitsbezogene Daten *zwecks* Forschung erhoben, gilt

1295 Botschaft Humanforschungsgesetz 2009, 8045 ff., 8083.

1296 Eindrücklich sichtbar wurden diese Korrelationen jüngst in BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2019, wobei sich die Erwägungen nicht nur mit den allgemeinen Verarbeitungsgrundsätzen, sondern auch den Einwilligungsvorgaben befassen. Ein Kernelement der Entscheidung ist indes in den bereichsspezifischen Erwägungen des Gerichts zu verorten, wobei nicht nur die Analyse, ob das öffentliche oder private DSG anwendbar ist, sondern auch die Relevanz der versicherungsrechtlichen Spezialgesetzgebung in ihrer Korrelation zum Datenschutzrecht deutlich wird.

dies als Forschung am Menschen. Hieran knüpfen spezifisch Verarbeitungsvorgaben an.[1297] Handelt es sich hingegen um die Weiterverwendung von gesundheitsbezogenen Daten, greift ein anderes Regime. Exemplarisch soll insofern die folgende Konstellation vorgestellt werden: Im Rahmen einer ärztlichen Untersuchung, beispielsweise einer Brustkrebs-Vorsorgeuntersuchung bei einer Frau mit familiärer Prädisposition, werden auch Personendaten erhoben. Diese Personenangaben werden entsprechend ursprünglich im Gesundheitsbereich und medizinischen Sektor erhoben; mit ihnen wird ursprünglich ein gesundheitsbezogenes Ziel verfolgt. Sollen nun die im Rahmen einer Untersuchung erlangten Gesundheitsdaten oder genetischen Angaben zur Forschung weiterverwendet werden, werden sie in einen anderen Kontext transferiert.[1298] Über das Beispiel, das auch das Regelungsregime veranschaulicht, wird in der gesetzgeberischen Konzeptionierung abermals die *dynamische Dimension des Datenschutzrechts* deutlich: Es geht um die Regelung des *Transfers* von Personendaten aus einem Kontext, dem Gesundheitskontext, in einen anderen Kontext, den Forschungskontext. In der ersten Konstellation dagegen zirkulieren die Personendaten innerhalb eines einzigen Kontextes. Im HFG wird folglich datenschutzrechtlich ein Ansatz gewählt, der sich der *rechtlichen Gestaltung von Datenflüssen innerhalb eines Kontextes, aber auch zwischen zwei Kontexten («weiterverwenden») widmet*. Dieser jüngere Rechtserlass, welcher der Bewältigung technologischer resp. bio- und informationstechnologischer Herausforderungen dient, lassen sich Anhaltspunkte für die Weiterentwicklung des Datenschutzrechts finden. Die Betrachtung des HFG zeigt, inwiefern die Verwurzelung in einer Subjekt-Objekt-Basierung, wie sie genuin im DSG verwurzelt ist, gelockert wird. Das DSG mit seiner persönlichkeitsrechtlichen Anknüpfung und den quasi objekthaften Kategorien von abstrakt charakterisierten «gewöhnlichen» resp. «besonders schutzwürdigen» Personendaten wird ergänzt. Das HFG präsentiert trotz seiner rechtlichen Anknüpfung an das Individuum und dessen Selbstbestimmung die Einschlägigkeit von Kontexten sowie die Bedingungen von Personendatentransfers, mithin von Datenflüssen im Umgang mit Personendaten und damit im Datenschutzrecht. Allerdings: Die im HFG gewählte Bewertung dürfte kritisch diskutiert werden. Es geht um die Schlussfolgerung, wonach die Bearbeitung von Personendaten *innerhalb* des Forschungskontextes die problematischere Konstellation sei als diejenige, in der Personendaten beispielsweise im Gesundheitskontext erhoben und dann in den Forschungskontext übergeleitet werden.[1299] Der Transfer von Personendaten von einem Kontext in einen anderen Kontext ist *prima vista* die eigentliche datenschutzrechtliche Herausforderung.

1297 Vertiefend hierzu Karavas, Körperverfassungsrecht, 152 ff., 210 ff.
1298 Hierzu Ders., a. a. O., 153 ff.
1299 Ders., a. a. O., 195 ff.

1002 Damit sind weitere Belege gefunden, welche die in dieser Schrift vertretene These bestätigen: Eine Kernaufgabe des Datenschutzrechts stellt die Gestaltung des *Deltas* der Datenflüsse oder der *Knotenpunkte* dar.[1300] Kritisch zeigt sich die Situation, in welcher ein Datenstrom *aus einem Kontext in einen anderen Kontext* übergeleitet wird. Diese Betrachtungsweise konterkariert diejenige, die das Datensubjekt und Personendaten als Quasi-Objekte fokussiert. Im Laufe dieser Studie wird noch robuster erhärtet werden, dass der datenschutzrechtliche Regelungsauftrag auch darin zu verorten ist, sich der *Gestaltung der Grenzverläufe und der Flussläufe zwischen verschiedenen Bereichen* anzunehmen. Mehrere im Laufe dieser Arbeit analysierte Normen und Regelungskonstruktionen innerhalb des DSG, aber auch eine einbettende Betrachtung seines Regimes in der Gesamtlandschaft von datenschutzrechtlichen Normen und Erlassen haben entsprechende bereits im geltenden Recht angelegte Elemente freigelegt. Die Fixierung auf die «persönlichkeitsrechtliche, subjektivrechtliche Anknüpfung», wie sie im DSG als sog. Querschnittsgesetz implementiert wird, lässt eine solche datenschutzrechtliche Regelungsaufgabe aus dem Blick fallen.[1301]

1003 Die Relevanz lässt sich anhand eines zweiten Erlasses veranschaulichen, seinerseits angesiedelt im *Bereich von Recht und neuen Technologien*.[1302] Das GUMG, das einer Revision unterzogen wurde, deren Ergebnisse Ende 2020 vorlagen, unterstellt den Umgang mit genetischen Informationen einer spezifischen Normierung. Auch in und über das GUMG wird eine konzeptionelle und systemische Herangehensweise angelegt. Genetische Untersuchungen haben faktisch stark an Bedeutung gewonnen. Heute werden sie nicht nur im Rahmen von Abstammungsabklärungen, sondern auch für pränatale Tests sowie zur Bestimmung von Krankheitsveranlagungen (z. B. die Mutation im BRCA1/2-Gen) eingesetzt. Auf den Erkenntnissen basierend erfolgt eine individualisierte medizinische Behandlung.[1303] Genetische Testungen, die Erkrankungsrisiken einer Person dokumentieren, sind nicht nur für das Individuum und den medizinischen Bereich, den Gesundheitssektor, aufschlussreich. Das GUMG adressiert die facettenreichen Inter-

1300 Ladeur, Vortrag, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021).

1301 Insofern lässt sich eine Parallele zu den familienrechtlichen Entwicklungen und Herausforderungen nachzeichnen: Solange das Familienrecht sich dem Schutz der ehelichen Einheitsfamilie verschreibt, stellt sich die Frage, was die Regelungsaufgabe des Familienrechts ist, nicht resp. scheint sie beantwortet zu sein. Allerdings wurde diese Frage jüngst aufgeworfen, wobei verschiedene Ansätze und Konzepte insofern präsentiert werden: Hierzu richtungsweisend insb. die zahlreichen Beiträge von Schwenzer.

1302 Zum sich wandelnden Recht in Einbettung zu sozialen und technologischen Entwicklungen vgl. die Beiträge in Becker/Hilty/Stöckli/Würtenberger (Hrsg.), Festschrift für Manfred Rehbinder, München 2002.

1303 Vgl. zur Bedeutung von genetischen Informationen im Zusammenhang mit psychiatrischen Erkrankungen mit den hieraus resultierenden datenschutzrechtlichen Bedenken Nagenborg/El-Faddagh, IRIE 2006, 40 ff.; zu Daten als Medizin resp. im Gesundheitsbereich Baeriswyl, digma 2014, 52 ff.

essen, indem es die genetischen Untersuchungen gemäss Art. 1 Abs. 1 GUMG für den medizinischen Bereich (lit. a), den arbeitsrechtlichen Bereich (lit. b), den Versicherungsbereich (lit. c) und den Haftpflichtbereich (lit. d) unterscheidet. Es sieht ein differenziertes Einwilligungsregime vor.[1304]

Die genetische Untersuchung im *Versicherungsbereich* beispielsweise wird im fünften Abschnitt des GUMG geregelt: Art. 26 GUMG verbietet Versicherungsgebern, für den Abschluss eines Vertrages die Vornahme genetischer Untersuchungen zu verlangen. Für spezifische Versicherungsleistungen greift nach Art. 27 GUMG ein Nachforschungsverbot. Mit anderen Worten: Für die Grundversicherung dürfen Ergebnisse vorhandener genetischer Untersuchungen nicht verlangt werden. Im Übrigen dürfen die mit der Durchführung eines Gentests beauftragten Ärztinnen und Ärzte gemäss Art. 28 Abs. 1 lit. a und lit. b GUMG unter zwei Voraussetzungen vorhandene Ergebnisse der Versicherung mitteilen. Insofern ist zunächst für den Privatversicherungsbereich das VVG einschlägig, wobei Art. 6 VVG eine Anzeigepflicht des Versicherungsnehmers vorsieht. Liegen Ergebnisse vorhandener genetischer Untersuchungen vor, die für die versicherte Person ein erhöhtes Krankheitsrisiko und damit für die Versicherung ein akzentuiertes wirtschaftliches Risiko indizieren, und kommt der Versicherungsnehmer seiner Anzeigepflicht nach, ist die Versicherung grundsätzlich berechtigt, sich von ihren Vertragsverpflichtungen zu befreien. Während im Bereich der sozialen Grundversicherung allgemeine *Einwilligungsverbote* zur Transmission entsprechender Ergebnisse anerkannt sind, gilt dies nicht für den Bereich der privaten Versicherung.[1305] Insofern wird – getreu der persönlichkeitsrechtlichen Verwurzelung – jüngst die «Freiwilligkeit» einer Einwilligung des Datensubjektes hinterfragt. Die dahinterliegende Grundsatzfrage, ob eine entsprechende Wertung in Anbetracht der *systemischen Dimension* des Datenschutzes mit seiner Aufgabe, die Integrität jeweils verschiedener gesellschaftlicher Bereiche zu gewährleisten, angemessen ist, wird dagegen nicht gestellt. Auch anhand des GUMG wurde sichtbar, dass dieses – selbst wenn es ebenso nicht unwesentlich an den Willen des Datensubjektes anknüpft – datenschutzrechtlich die Einschlägigkeit kontextbezogener Kriterien anerkennt. Hieran anknüpfend schafft es ein informationsrechtlich nuanciertes Normgefüge. 1004

Lassen sich über diesen Befund hinaus, namentlich aus der Erkenntnis, wonach der Wille des Subjektes unter Anerkennung bereichsspezifischer Differenzierungen in facettenreicher, nuancierter und abgestufter Weise in das Datenschutzrecht der Schweiz – das weit mehr ist als das DSG – integriert wird, allgemeinere Schlussfolgerungen hinsichtlich der Funktion der datenschutzrechtlichen Einwilligung gewinnen? Karavas arbeitet in seiner Habilitationsschrift für den 1005

1304 Fasnacht, N 573.
1305 Vgl. hierzu Ders., N 551 ff. und zum GUMG N 570 ff.

biomedizinrechtlichen Bereich heraus, dass sich die *Funktion der informierten Einwilligung* keineswegs auf die Gewährleistung eines verfassungsrechtlich verbürgten Selbstbestimmungsrechts, das der Sicherung der freien Willensbildung und freien Willensbetätigung diene, beschränke.[1306] Indem das Rechtsinstitut auf der anderen Seite Pflichten, beispielsweise der Forscherinnen und Forscher, definiere, strukturiere es ebenso Beziehungen der involvierten Personen. Damit wird dem Rechtsinstitut der informierten Einwilligung im Bereich des Biomedizinrechts konstitutionelle Wirkung zugemessen.[1307] Zudem gilt die informierte Einwilligung als *Governance*-Instrument sowie als weit verbreitetes und etabliertes *organizational recipe* im Bereich der biomedizinischen Forschung.[1308] Folglich qualifiziert Karavas die informierte Einwilligung im weiten Feld des Biomedizinrechts aus einer funktionellen sowie kontextuellen Perspektive heraus als *Kompatibilisierungsinstrument*: Der Einwilligung wird in diesem Sinne die Funktion zugemessen, verschiedene Bereiche – z. B. den Gesundheitssektor und den Forschungsbereich – mit ihren unterschiedlichen Handlungslogiken und Erwartungen sowie ihre Schnittstellen zu harmonisieren. Allerdings hinterfragt der Autor sogleich die Tauglichkeit der informierten Einwilligung zur Lösung von Kollisionen zwischen Gesellschaftsbereichen resp. Kontexten. Seiner Ansicht nach lassen sich Spannungsfelder und Kollisionen gerade wegen ihrer kollektiven Dimension durch die informierte Einwilligung des Einzelnen nicht sinnvoll adressieren.[1309]

1006 Dass die Figur der Selbstbestimmung nicht das einzig relevante Erwägungselement ist, findet sich für das Datenschutzrecht in der Argumentation des Bundesverfassungsgerichts in seinem Volkszählungsurteil. Das Bundesverfassungsgericht richtete den Fokus auch auf die *kontextuelle Dimension* und namentlich auf die *notwendige Trennung resp. Abgrenzung der Statistik vom Vollzug mit dessen facettenreichen Teilbereichen*. Um einen Transfer oder Informationsfluss von Personendaten, die zum Zweck der Volkszählung erhoben wurden, in andere Bereiche des Verwaltungsvollzuges zu verhindern, beschränkte sich das Bundesverfassungsgericht nicht darauf, die Bedeutung des Grundrechts auf informationelle Selbstbestimmung, das prinzipielle Verarbeitungsverbot mit Schranken, die Relevanz des Zweckbindungsgrundsatzes und das Statistikgeheimnis zu thematisieren. Vielmehr wurden *flankierende personelle und organisatorische Massnahmen* verlangt. Beispielhaft zu nennen ist die Forderung, wonach die Zähler nicht in ihrem unmittelbaren räumlichen Einsatzgebiet tätig werden sollen. Es sei zu verhindern, dass sie aufgrund ihres ursprünglichen fachlichen Wirkungsfeldes nur ungenügende Neutralität aufweisen.[1310] Das Bundesverfassungsgericht

1306 Karavas, Körperverfassungsrecht, 195 ff., insb. 222 ff.
1307 Ders., a. a. O., 197.
1308 Hierzu m. w. H. Ders., 197 f.
1309 Ders., 228 f.
1310 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 220.

formuliert einen hoch *ausdifferenzierten und facettenreichen Katalog an materiellen, namentlich aber auch organisatorischen sowie formellen Vorgaben*, um damit die Trennung von Statistik und Verwaltungsvollzug zu gewährleisten. Ein Kernargument liegt darin, dass nur das *Vertrauen in diese Trennung* und damit die Gewährleistung, wonach Personendaten, die im Kontext der Statistik erhoben wurden, nicht anderen Bereichen und Behörden (z. B. Steuerbehörden oder Migrationsbehörden) zwecks konkreten Verwaltungsvollzugs zugeführt werden, sicherstelle, dass die Bürgerinnen und Bürger die Erhebungsfragen korrekt und vollständig beantworten würden. Auf ebendiese korrekten und vollständigen Angaben sei eine repräsentative statische Erhebung, welche die damit verfolgten staatlichen Ziele effizient erreichen soll, angewiesen. Zwangsmassnahmen dagegen könnten die Kooperation der Bürgerinnen und Bürger insofern gerade nicht gewährleisten. Die vom Bundesverfassungsgericht formulierten Datenschutzvorgaben zielen damit in grundlegender Weise auf den Schutz der Funktionstüchtigkeit und Integrität der Volkszählung ab.

6.4. Resümee – Nuancierte Autonomiegrade

Gezeigt wurde, dass das Schweizer Recht in Bezug auf den Umgang mit Personendaten in verschiedenen datenschutzrechtlich einschlägigen Erlassen variable Modalitäten für den Einsatz von Einwilligungs- resp. Widerspruchslösungen vorsieht.[1311] Eine Gesamtbetrachtung führt zu dem Schluss, dass im Umgang mit Personendaten keine einheitliche «Selbstbestimmung» verbürgt wird. Insofern wurde zum einen das durch eine stabile bundesgerichtliche Rechtsprechung etablierte Regime zum Recht am eigenen Bild dargestellt. Zum anderen fand eine Betrachtung von HFG und GUMG statt, wobei sich in diesen Erlassen nuancierte Einwilligungskonstruktionen zeigten. Diese einbettende und vergleichende Betrachtung diverser und diversifizierter Konstruktionen zur Inklusion des Willens des Datensubjektes hat bestätigt, dass das *DSG selbst kein Recht auf informationelle Selbstbestimmung* implementiert, mit einem Gehalt, wie es mit dem Volkszählungsurteil des Bundesverfassungsgerichts gemeint und assoziiert wird. 1007

Als ein Recht auf informationelle Selbstbestimmung – das eine solche Titulierung zu Recht tragen würde – lässt sich demgegenüber das *Recht am eigenen Bild* charakterisieren. Bei den Verarbeitungshandlungen im Zusammenhang mit dem Abbild einer Person handelt es sich unbestritten um Personendaten. Das Recht am eigenen Bild etabliert ein eigentliches Sonderrecht im Vergleich zum DSG. Der im Wesentlichen über Art. 28 ZGB anerkannte Inhalt des Rechts am eigenen Bild 1008

1311 Die Nuancierung von Einwilligungskonstruktionen lässt sich gesetzlich wie anhand der bundesgerichtlichen Rechtsprechung nachzeichnen; exemplarisch ist BGE 136 II 401.

lässt sich deshalb als Selbstbestimmungsrecht bezeichnen, weil Verarbeitungshandlungen im Umgang mit dem Abbild einer Person prinzipiell untersagt sind. Sie bedürfen eines Erlaubnistatbestandes, namentlich der Einwilligung des Subjektes. Ganz anders sind im DSG für den privaten Bereich Personendatenverarbeitungen grundsätzlich erlaubt. Verboten ist nur der qualifizierte Umgang mit Personendaten (insb. Verletzung der Verarbeitungsgrundsätze, Verarbeitung entgegen dem Widerspruch, Weitergabe von Persönlichkeitsprofilen und besonders schutzwürdigen Angaben an Dritte).

1009 Auch die Analyse der Einwilligungsvorgaben in *Spezialgesetzen wie dem HFG sowie dem GUMG* führte vor Augen, dass das schweizerische Datenschutzrecht *keine einheitliche Autonomie* des Datensubjektes über sämtliche Handlungsfelder hinweg implementiert. Vielmehr wird durch Normen und Erlasse mit datenschutzrechtlichen Bestimmungen ausserhalb des DSG *kontextspezifisch* nuanciert geregelt. Der Bereich des (Bio-)Medizinrechts ist als dasjenige Gebiet zu bezeichnen, in welchem der sog. Selbstbestimmung und damit dem Einwilligungserfordernis seit jeher eine prominente Rolle zugewiesen wurde.

1010 Das HFG schafft ein spezialgesetzliches Regime in Bezug auf den Umgang mit gesundheitsbezogenen Angaben im Forschungskontext. Es verankert ein hochdifferenziertes Gefüge, dessen Strukturierung kontextspezifisch geleitet ist. Das HFG unterscheidet die Einwilligungserfordernisse anhand einer Basisdifferenzierung danach, ob die Verarbeitung gesundheitsbezogener Personendaten originär zwecks Forschung erfolgt, also ob die Angaben zu Forschungszwecken erhoben werden oder ob diese weiterverwendet werden bzw. ob gesundheitsbezogene Personendaten aus einem anderen Kontext stammen, in dessen Rahmen sie primär erhoben wurden. Sichtbar wird anhand des HFG, dass datenschutzrechtlich kontextbezogen reguliert wird – in dieser Arbeit als *systemische und akzessorische Dimension des Datenschutzrechts* bezeichnet. Das Augenmerk der Regelung richtet sich auf *Datenflüsse* – in dieser Arbeit *dynamische Dimension* des Datenschutzrechts genannt. Die entsprechenden Ansätze finden sich, spezifisch für genetische Informationen, im Regelungsregime gemäss GUMG bestätigt. Sowohl HFG als auch GUMG sehen im Vergleich zum DSG eine differente und differenzierte Gestaltung der Einwilligungsvorgaben für den Umgang mit Personendaten vor. Beide Erlasse weisen der Einwilligung eine im Vergleich zum DSG stärkere Position zu.

1011 Folglich ist ein einheitliches und uniformes «informationelles Selbstbestimmungsrecht» dem schweizerischen Datenschutzrecht fremd. Dies heisst ebenso, dass es «das» Datensubjekt im Sinne eines «informationellen Einheitssubjekts» nicht gibt. Vielmehr präsentiert sich die Person und das Datensubjekt resp. Informationssubjekt facettenreich, mit pluralen informationellen Teilrollen resp. -persönlichkeiten. Seine Autonomiegrade sind je nach einschlägigem Recht und damit

relevantem gesellschaftlichem Bereich resp. Kontext unterschiedlich. Die Autonomieräume, die dem Datensubjekt durch Regelungen ausserhalb des DSG eingeräumt werden, sind facettenreich, die Positionierung der Einwilligung in den verschiedenen Feldern ist ausdifferenziert. Freigelegt wurde damit, dass die «Person», die Persönlichkeit, das Datensubjekt sich als bereichsspezifisch konkretisiertes Datensubjekt mit entsprechend variablen Autonomieräumen resp. -graden beschreiben lässt. Vordergründig zeigt sich allerdings das geltende Datenschutzrecht in Gestalt des DSG mit einer wirkungsdominanten Annahme – derjenigen eines kontext- und rollenblinden Datensubjektes, ein gewissermassen indifferentes Einheitssubjekt.

1012 Die Ausführungen zu den Tatbestandselementen der Persönlichkeitsverletzung gemäss DSG haben eine konsequente Anlehnung an die für das Persönlichkeitsrecht etablierte Figur der «qualifizierten» Verletzungshandlung für den privaten Bereich nachgewiesen. Dieser subjektiv-, abwehr- und deliktsrechtlichen Konzeption des DSG für den privaten Bereich folgt nun eine *Tour d'Horizon* über die *Umsetzungs- und Durchsetzungsinstrumente*. Damit wird dieser Abschnitt über die persönlichkeitsrechtliche Basierung des DSG für den privaten Bereich abgerundet. Gleichzeitig wird in den dritten Teil dieser Arbeit übergeleitet, der den Herausforderungen des aktuellen Datenschutzrechts nachgeht: Während der zweite Teil zeigte, dass sich die Funktionsweise des DSG anhand dreier Strukturmerkmale beschreiben lässt – Dualismus zwischen öffentlichem und privatem Bereich, generalklauselartige allgemeine Verarbeitungsvorgaben sowie persönlichkeitsrechtliche Anknüpfung und damit individual-, abwehr- sowie deliktsrechtliche Ausrichtung des DSG für den privaten Bereich –, wird im dritten Teil dieser Arbeit vorab auf die *Wirksamkeit und faktische Griffigkeit dieses Instrumentariums in der Praxis* eingegangen. Der dritte Teil wendet sich einer Kernproblematik des Datenschutzrechts und hierbei namentlich des DSG zu, dem sog. *Vollzugsdefizit*. Nach einer Auseinandersetzung mit den Fortschritten und Entwicklungen, die mit den jüngsten datenschutzrechtlichen Neuerungswellen einhergehen, wird ein Vorschlag zur Gestaltung eines wirksame(re)n Datenschutzrechts *de lege ferenda* vorgelegt.

C. Folgerung und Überleitung – Um- und Durchsetzung

1013 Die *Verwirklichung des Datenschutzrechts* hängt nicht unwesentlich auch von der Gestaltung des Umsetzungs- und Durchsetzungsinstrumentariums und der insofern gewählten Ansätze ab. Hierbei hat die *persönlichkeitsrechtliche Anknüpfung und Ausrichtung des DSG* für den privaten Bereich *de lege lata* massgeblichen Einfluss auf die Konzeptionierung der *Umsetzungs- und Durchsetzungs-*

instrumente. Die DSGVO sowie die Totalrevision des DSG sehen in diesem Feld durchgreifende Neuerungen vor. Der Massnahmen- und Sanktionenkatalog wurde markant ausgebaut sowie verschärft. Anlass zu dieser Verschärfung und zum Ausbau der möglichen behördlichen Anordnungen gab ein ernüchternder Befund, der in Bezug auf das bisherige Datenschutzrecht gemacht wurde. Für Deutschland in den Worten von Buchner:

> «In kaum einem Rechtsgebiet liegen Anspruch und Wirklichkeit so weit auseinander wie im Datenschutzrecht.»[1312]

1014 Auch für die Schweiz wird ein *Vollzugsdefizit* datenschutzrechtlicher Normierung beschrieben.[1313] Mit dem Begriff «Vollzugsdefizit» ist Verschiedenes gemeint. Zunächst geht es um die ungenügende Einhaltung der datenschutzgesetzlichen Vorgaben durch die Verarbeitenden. Es musste festgestellt werden, dass das datenschutzrechtskonforme Verhalten der Verarbeitenden eher bescheiden ist.[1314] Mehrere neue Instrumente der Totalrevision sollen hier ansetzen. Insbesondere das Verarbeitungsverzeichnis und die Datenschutz-Folgenabschätzung zielen darauf ab, eine faktische Effektuierung zu liefern. In Bezug auf die ungenügende Einhaltung des DSG vor Totalrevision ist sodann auf das Rechtsdurchsetzungsinstrumentarium einzugehen, das die persönlichkeitsrechtliche Anknüpfung rezipiert. Es geht hier zum einen um die Betroffenenrechte wie das Auskunftsrecht sowie zum anderen um die Rechtsbehelfe, die der betroffenen Person an die Hand gegeben werden, um gegen eine Persönlichkeitsverletzung durch private Verarbeitende gerichtlich vorzugehen, vgl. Art. 15 DSG und Art. 32 nDSG. Der individualrechtliche Rechtsschutz steht weder vor noch nach Totalrevision isoliert da. Er wird flankiert durch verwaltungsrechtliche sowie strafrechtliche Instrumente. Vor der Totalrevision des DSG müssen die den «zivilrechtlichen Datenschutz» ergänzenden Instrumente als schwach gestaltet beurteilt werden. Der bislang stark auf der Schulter der Datensubjekte ruhende Rechtsschutz wird mit Totalrevision ergänzt durch erweiterte Kompetenzen des EDÖB und verschärfte strafrechtliche Sanktionen, die durch die kantonalen Behörden verfügt werden, vgl. Art. 49 ff. nDSG und Art. 60 ff. nDSG.

1015 Bislang wurden die Betroffenenrechte, deren Verbürgung eng mit der individual- und persönlichkeitsrechtlichen Anknüpfung des DSG zusammenhängt, in der

1312 So der einleitende Satz von Buchner, 1; ähnlich Simitis, Symposium, 1 ff., 1; früh bereits ebenso Bull, Computer, 353; zudem Sachs, 19.

1313 Vgl. Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f., 23; indikativ hierfür Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.1; Bolliger/Féraud/Epiney/Hänni, 68; unlängst insb. auch Ebert/Widmer, 19; von einem gewissen Vollzugsdefizit sprechen Vasella/Sievers, digma 2017, 44 ff., 48 f.; in der schwachen Effektivität der Datenschutzerlasse in Europa wurde ein weiterer Grund verortet, weshalb in den USA bislang auf eine das Datenschutzrecht umfassende Datenschutzgesetzgebung verzichtet wurde, vgl. Mayer-Schönberger, Delete, 165.

1314 Vgl. Bolliger/Féraud/Epiney/Hänni, 30 ff.; Ebert/Widmer, 10 ff.

Praxis selten in Anspruch genommen. Zudem greifen die gerichtlichen Durchsetzungsinstrumentarien, die ebenso konsequent an den Persönlichkeitsschutz angelehnt sind, bloss rudimentär resp. punktuell.[1315]

Solange das Datenschutzgesetz für den privaten Bereich in der Struktur des delikts- und abwehrrechtlich gedachten Persönlichkeitsschutzes angelegt ist, ist es folgerichtig, die *Verletzungshandlung* gegenüber dem Individuum, dem Datensubjekt, in das Zentrum der Aufmerksamkeit zu stellen und die «Verteidigung» des Datenschutzes dem Datensubjekt über das Arsenal der zivilrechtlichen Rechtsbehelfe zuzuweisen. Eine persönlichkeitsrechtlich fixierte Datenschutzgesetzgebung allerdings wirft die Frage auf, ob das *DSG mit seinen Strukturmerkmalen an sich geeignet ist, einen wirksamen Datenschutz zu gewährleisten*. Die insofern zu führende Diskussion ist diejenige über Schutzzweck und -objekt datenschutzrechtlicher resp. datenschutzgesetzlicher Normierung. Bis hierher wurden in dieser Arbeit mehrere Indizien herausgearbeitet, die dafürsprechen, den Datenschutz nicht isoliert dem Persönlichkeitsschutz zu verpflichten, stattdessen darüber hinausgehend systemische Schutzerwägungen als einschlägig zu inkludieren.[1316] 1016

An dieser Stelle geht es vorab allerdings um das Durchsetzungsinstrumentarium, wie es das aktuelle DSG vorsieht. *De lege lata* bilden – formell und theoretisch betrachtet – zunächst die den *Datensubjekten eingeräumten Rechte*, die sog. *Betroffenenrechte*, eine tragende Säule zur Verwirklichung des Datenschutzrechts.[1317] 1017

Hierbei ist zunächst das Auskunftsrecht gemäss Art. 8 DSG zu nennen. Das Auskunftsrecht beschränkt sich auf Personendaten, die sich in Datensammlungen befinden. Zudem formulieren Art. 9 f. DSG Gründe zur Verweigerung resp. Einschränkung der spiegelbildlichen Auskunftspflicht. Das Auskunftsrecht, so wird es gesagt, soll es der «betroffenen Person erleichtern, ihre datenschutzrechtlichen Ansprüche durchzusetzen, indem es ihr ermöglicht, Kenntnis davon zu erhalten, wer überhaupt Daten über sie bearbeitet».[1318] Theoretisch betrachtet kommt dem 1018

1315 Vgl. Bolliger/Féraud/Epiney/Hänni, 38; Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.10 ff., insb. N 7.20 f.; interessant in diesem Zusammenhang der Befund von Ebert/Widmer, 16, wonach nur 35 Prozent der befragten Unternehmen einen Prozess zur Abwicklung von Auskunftsbegehren etabliert haben.

1316 Ein Recht auf informationellen Systemschutz als neuer Ansatz für ein «wirksames Datenschutzrecht», das über den Subjektschutz hinausgeht, diesen gleichwohl inkludiert, wird – nach einer kritischen Auseinandersetzung mit den derzeit präsentierten Lösungsansätzen zur Adressierung aktueller datenschutzrechtlicher Herausforderungen – im dritten Teil, IX. Kapitel elaboriert; der Begriff des Systemschutzes wird im datenschutzrechtlichen Kontext von Hoffmann-Riem, AöR 1998, 513 ff., 534 ff. verwendet, wobei ebenda nicht dieselbe Schutzkonzeption gemeint wird, wie sie in dieser Arbeit präsentiert wird; bereits Mallmann, 67 ff. statuierte, dass Privatheit eine Reihe existenzieller Funktionen für die Gesellschaft und den einzelnen erfülle.

1317 Vertiefend hierzu Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5.

1318 Vgl. BBl 1988 II 414 ff., 452.

Auskunftsrecht in einem Regime, wie es die Schweiz *de lege lata* im DSG für den privaten Bereich aufgrund des Ausgangspunktes der prinzipiellen Verarbeitungsfreiheit mit Schranken und des Fehlens einer allgemeinen aktiven Informationspflicht vorsieht, besondere Bedeutung zu. Dem Auskunftsrecht wird Präventiv- wie Kontrollfunktion zugewiesen.[1319] Insofern wird vertreten, dass unrechtmässige Datenverarbeitungen resp. persönlichkeitsverletzende Verarbeitungshandlungen in aller Regel erst über die Wahrnehmung des Auskunftsrechts von den Betroffenen in Erfahrung gebracht würden, weshalb diesem Recht hohe Relevanz zugemessen wird.[1320] Dies reflektierend sieht das DSG für den Fall der Verletzung des Auskunftsrechts geeignete Instrumente vor, vgl. Art. 15 Abs. 4 DSG; sodann wird gemäss Art. 34 Abs. 1 lit. a DSG auf Antrag mit Busse bestraft, wer eine falsche oder unvollständige Auskunft erteilt. Zwar werden Auskunftsrechte in der Realität ausgeübt, allerdings muss die Bedeutung des Auskunftsrechts in Anbetracht des Ausmasses von Personendatenverarbeitungen gleichwohl als marginal bezeichnet werden. Es sind ernsthafte Zweifel daran anzubringen, im Auskunftsrecht des einzelnen Datensubjektes einen wirkungsstarken Mechanismus zu verorten, um die Einhaltung der Vorgaben des DSG zu verwirklichen.

1019 Wie erwähnt bringen die jüngsten datenschutzrechtlichen Entwicklungen neue Elemente und Ausrichtungen dergestalt, dass in erster Linie die Verantwortlichen in die Pflicht genommen werden, die Einhaltung der datenschutzrechtlichen Vorgaben umzusetzen und zu dokumentieren. Das Auskunftsrecht wird zwar beibehalten, die Last der «Umsetzungs- und Prüfungs- sowie Beweispflicht» wird indes verlagert. Das Auskunftsrecht selbst ist nach Totalrevision im 4. Kapitel unter dem Titel «Rechte der betroffenen Person» in Art. 25 ff. nDSG verbürgt. Weitere Ansprüche der Datensubjekte finden sich an anderen Stellen, so in Art. 32 nDSG. Zudem sind Informationspflichten gegenüber dem Datensubjekt zu beachten, vgl. Art. 19 ff. nDSG.

1020 Die *zivilrechtlichen Ansprüche* verbürgt Art. 15 Abs. 1 DSG resp. Art. 32 nDSG. Es handelt sich hier um die Klagebehelfe, die allgemein im Rahmen des Regimes der Persönlichkeitsverletzung gemäss Art. 28 ff. ZGB anerkannt sind. Im Rahmen des *zivilgerichtlichen Rechtsschutzes* sind die Klagen auf Unterlassung und Beseitigung, vgl. auch Art. 28a Abs. 1 Ziff. 1 und Ziff. 2, aber auch die Feststellungsklage, vgl. Art. 28a Abs. 1 Ziff. 3, eröffnet; daran anknüpfend die Klagen auf Schadenersatz, Genugtuung und Gewinnherausgabe.[1321] Für vertiefende Ausführungen zu den entsprechenden Ansprüchen und Klagen sei auf die einschlägige

1319 Vgl. m. w. H. Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5 N 5.4.
1320 Vgl. Ders., a. a. O., § 5 N 5.85.
1321 Zu diesen Grundansprüchen vgl. Pedrazzini, in: Schweizer (Hrsg.), 81 ff., 82 ff., und 88 f., wo der Autor bereits früh auf den starken Ausbau der privatrechtlichen Durchsetzungsinstrumente qua DSG hinwies, allerdings Zweifel daran äusserte, ob sich diese in der Realität bewähren würden.

Kommentarliteratur verwiesen. Datenschutzgesetzliche Spezifika liefert Art. 15 Abs. 1 und Abs. 3 DSG mit den Ansprüchen auf eine Bearbeitungssperre sowie Sperre der Bekanntgabe, auf Berichtigung der Personendaten sowie auf Vernichtung resp. Löschung von Personendaten. Art. 15 Abs. 2 DSG sieht zudem das Instrument des Bestreitungsvermerkes vor. In der Totalrevision finden sich vergleichbare Ansprüche in Art. 32 Abs. 1, Abs. 3 und Abs. 4 nDSG. Unbestritten sollte sein, dass alle Ansprüche vorab auch aussergerichtlich geltend gemacht werden können.

Für datenverarbeitende Unternehmen stellen die zivilrechtlichen Ansprüche der Datensubjekte formell, nicht aber in der Realität ein Risiko dar, da sie sowohl aussergerichtlich als auch gerichtlich kaum je durchgesetzt werden. Mit einer zivilrechtlichen Klage wegen Persönlichkeitsverletzung durch Personendatenverarbeitung hat in der Schweiz kaum jemand ernsthaft zu rechnen.[1322] Zudem ist zu attestieren, dass selbst eine individualrechtlich geführte Klage wegen Persönlichkeitsverletzung durch Personendatenverarbeitungen stets eine auf den Einzelfall gerichtete Beurteilung mit sich bringt. Das abwehrrechtlich strukturierte und im Persönlichkeitsrecht verwurzelte Durchsetzungsregime des Datenschutzrechts hat entsprechend kaum (bzw. keinerlei) für die Einhaltung motivierende resp. abschreckende Wirkung. Die *individualrechtliche und selbstverteidigte Privatsphäre* weist beträchtliche Schwachstellen auf. 1021

Der Vollständigkeit halber sei daher im Rahmen des zivilrechtlichen Rechtsschutzes auf Art. 89 Abs. 1 und Abs. 2 ZPO hingewiesen. Damit wird über das allgemeine zivilprozessuale Regime eine Verbandsklage auch für den Bereich des zivilrechtlichen Datenschutzes anerkannt.[1323] Zudem besteht die Möglichkeit, gerichtlich vorsorgliche Massnahmen zu verlangen, Art. 261 ff. ZPO.[1324] 1022

In diesem persönlichkeitsrechtlichen Klagenarsenal erschöpft sich das zivilrechtliche Durchsetzungsregime nicht. Vielmehr würden gemäss Rosenthal die *vertragsrechtlichen Sanktionierungen* in der Praxis als effektiver und wichtiger beurteilt.[1325] Zudem kann eine betroffene Person einen Strafantrag gemäss Art. 34 Abs. 1 DSG einreichen oder dem EDÖB eine Meldung erstatten, womit zu den 1023

1322 Vgl. Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.20; vertiefend zur Rechtsprechung nachfolgend dritter Teil, VII. Kapitel, A.2.; zur fehlenden Rechtsdurchsetzung nicht nur in der Schweiz vgl. Burghardt/Böhm/Buchmann/Kuhling/Sivridis, in: Sivridis/Patrikakis/Burghardt et al. (Hrsg.), die von einer Nichtreaktion auf Auskunftsbegehren in rund 30 Prozent der Fälle berichten, 3 ff.

1323 Vgl. zum Vorentwurf der Revision der ZPO mit Blick auf den Ausbau der Verbandsklage und die Einführung eines Gruppenvergleichs Ceregato, Jusletter vom 10. September 2018, N 7 ff.; dagegen wurde die Einführung einer Verbandsklage im Rahmen der Verabschiedung des DSG abgelehnt, BBl 1988 II 414 ff., 465; zur Revision der ZPO mit ihrer Stärkung des kollektiven Rechtsschutzes auch Domanig, Jusletter vom 17. Juni 2019, N 5 ff.

1324 Rampini, BSK-DSG, Art. 15 N 33.

1325 So Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.22.

verwaltungsrechtlichen sowie strafrechtlichen Sanktionen bei Datenschutzverstössen übergeleitet wird.

1024 Auf die *verwaltungsrechtlichen Massnahmen* des EDÖB für den privaten Bereich, Art. 29 DSG, wurde bereits im Kapitel über den Dualismus eingegangen. Seine Kompetenzen sind – systemkonform – für den privaten Bereich insb. vor der Totalrevision nur beschränkt.[1326] Der EDÖB kann über seine Informations-, Aufklärungs- und Beratungsfunktion – in deren Rahmen insb. auch seine Leitfäden von Interesse sind[1327] – im Anschluss an eine Sachverhaltsabklärung, die er allerdings nur bei sog. Systemfehlern durchzuführen befugt ist, vgl. Art. 29 Abs. 1 DSG, eine Empfehlung erlassen. Kommt der Adressat dieser nicht nach, kann der EDÖB die Angelegenheit dem Verwaltungsgericht vorlegen.[1328] Entscheidungen vom Bundesverwaltungsgericht sind alsdann vom Bundesgericht überprüfbar. Hierbei ist zu verzeichnen, dass der EDÖB gerade in den letzten Jahren seine Interventionen intensiviert hat. Indem er seine Empfehlungen konsequenter durchsetzt, sind auch einige namhafte Urteile vonseiten des Bundesverwaltungsgerichts und Bundesgerichts ergangen.[1329] Ebendiese Urteile werden folgend genauer beleuchtet, wobei bereits an dieser Stelle festzuhalten ist, dass es Urteile von grundlegender Bedeutung sind, nicht zuletzt, indem sie datenschutzrechtliche Herausforderungen weit über einen verengten Blick auf das Individuum hinaus beleuchten. Hier deutet sich auch für die Schweiz der Bedeutungsgewinn und Bedeutungswandel im Datenschutzrecht an. Die Kompetenzen des EDÖB werden mit der Totalrevision neu gestaltet, vgl. Art. 49 ff. nDSG.[1330]

1025 Ergänzend ist festzuhalten, dass nicht nur der EDÖB datenschutzrechtlich eine Aufsichtsfunktion wahrnimmt. Vielmehr ist auf branchen- und sektorspezifische Regulierungen und Organisationen hinzuweisen. Allem voran zu nennen sind der Finanzmarktsektor sowie der Versicherungsbereich und hierbei die FINMA, welche in ihrer aufsichtsrechtlichen Funktion ebenso die Einhaltung datenschutzrechtlicher Vorgaben im Auge hat. So wird die Datenschutzrechtskonformität im Rahmen des Rundschreibens «operationelle Risiken» thematisiert. Die Möglichkeit aufsichtsrechtlicher Massnahmen vonseiten der FINMA im Kontext des Datenschutzes werde in der Praxis ernst genommen.[1331] Mit Blick auf die Einhaltung

1326 Vgl. zweiter Teil, IV. Kapitel, B.3.3.
1327 Abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden.html> (zuletzt besucht am 3. September 2021).
1328 Jüngst geschehen in der Angelegenheit BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018; Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.61, wonach es sich um ein Verwaltungsverfahren handle, das indes im Wesentlichen den Grundsätzen des Zivilprozesses folge; das Verfahren könne als eine Art Popularklage bezeichnet werden.
1329 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018.
1330 Hierzu Rosenthal, Jusletter vom 16. November 2020, N 181 ff.
1331 So Ders., in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.22; zur bankaufsichtsrechtlichen Relevanz des Datenschutzrechts, insb. des DSG, auch Meier, in: Emmenegger (Hrsg.), 1 ff.

datenschutzrechtlicher Vorgaben sowie deren Überprüfung präsentiert sich der Bankensektor mit einer gegenüber anderen Bereichen höheren Reife, was traditionell damit zu erklären ist, dass in der Branche seit jeher und ebenso im Zuge der jüngsten Fintech-Entwicklungen stark auf die Vertrauensbeziehung zwischen Finanzinstitut und Kunde gesetzt wird, in deren Zentrum das (mittlerweile kleine) traditionelle Schweizer Bank(kunden)geheimnis steht, vgl. Art. 47 BankG. Letzteres leitet zu den strafrechtlichen Sanktionierungen von Datenschutzverstössen über.

1026 Im DSG finden sich *nur ganz punktuell strafrechtliche Sanktionierungsmöglichkeiten*, vgl. Art. 34 f. DSG.[1332] Von hoher Relevanz sind die Strafbestimmungen des StGB, die namentlich für den Geheimnisschutz vorgesehen sind, vgl. Art. 162 StGB; zudem ist im Zusammenhang mit Sanktionierungen im Kontext von Datenverarbeitungen auf Art. 179–179^{novies} hinzuweisen. Sodann finden sich Strafbestimmungen im Fernmeldegesetz, vgl. Art. 49 ff. FMG. Zu beachten ist die Strafandrohung gemäss Art. 23 Abs. 1 UWG mit seinem in Art. 3 Abs. 1 lit. o UWG niedergelegten Spam-Verbot sowie gemäss Art. 3 Abs. 1 lit. u UWG. Der Hinweis von Rosenthal im Zuge seiner Darstellung des Sanktionierungssystems bei Datenschutzverstössen, wonach die im UWG und StGB zu findenden Bestimmungen nicht als Normen des Datenschutzes wahrgenommen werden,[1333] dokumentiert, dass eine kontextuelle Sicht des Datenschutzrechts in der Schweiz (noch) nicht etabliert ist. Die Totalrevision baut die datenschutzgesetzlichen Strafbestimmungen markant aus, vgl. Art. 60 ff. nDSG.[1334]

1027 Mit der Totalrevision wird der *bisherige Akzent des DSG auf die Persönlichkeitsverletzung und die individualrechtliche Geltendmachung von Datenschutzrechtsverstössen markant ergänzt*. Bis zu ihrer Umsetzung bleibt die retrospektive und repressive sowie subjektivrechtliche Sichtweise prägend. Sie entspricht der Anknüpfung des Datenschutzrechts in einem defensivrechtlich sowie deliktsrechtlich angelegten Persönlichkeitsrecht, vgl. Art. 1 DSG. Dass hierin eine Mitursache für die ungenügende Wirksamkeit des Datenschutzrechts und spezifisch des Datenschutzgesetzes liegt, wird im VII. Kapitel des dritten Teils vertieft werden. Im VIII. Kapitel des dritten Teils wird kursorisch gezeigt, inwiefern die jüngsten datenschutzrechtlichen Neuerungen an diesem Schwachpunkt ansetzen.

1332 Hierzu vertiefend Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.36 ff.
1333 Ders., a. a. O., § 7 N 7.56.
1334 Hierzu Ders., Jusletter vom 16. November 2020, N 191 ff.

Dritter Teil: Vom Recht auf informationellen Subjektschutz zum Recht auf informationellen Systemschutz

Im vorangehenden *zweiten Teil wurden in den Kapiteln IV–VI drei Strukturmerkmale* des DSG beschrieben. Damit wurden gleichzeitig die *Wirkungsweisen* des DSG herausgearbeitet. Nunmehr geht es darum, die *Wirksamkeit des Regimes* und namentlich die (faktischen) Herausforderungen, mit denen das Rechtsinstrumentarium konfrontiert ist, zu analysieren. 1028

Das DSG wurde und wird in verschiedener Hinsicht auf eine harte Probe gestellt. Die Totalrevision ist damit nicht nur vor den Entwicklungen in der EU und der DSGVO zu sehen, sondern ebenso vor diesem Hintergrund. Für diese Untersuchung sind *zwei Problemfelder*, die sich unter dem DSG vor Totalrevision zeigten, von besonderem Interesse. 1029

Das *erste Thema* lässt sich mit der Frage umreissen, inwiefern das *Regelungskonzept in der Realität Wirksamkeit* entfaltet. Damit wird auch die Relevanz, die dem Datenschutz, dem Datenschutzrecht und namentlich dem DSG zugemessen wird, sichtbar. Zudem findet eine Auseinandersetzung mit der Frage statt, ob das DSG die Ziele, deren Schutz sich das DSG verschreibt, zu erreichen vermag. Damit verbunden ist die Identifizierung allfälliger Schwachpunkte des Regelungskonzeptes und das Verständnis seiner Herausforderungen. Auf einer solchen Basis lassen sich alsdann Lösungsansätze ableiten. Dieser dritte Teil befasst sich folglich mit Fragen der Effektivität und Effektuierung datenschutzrechtlicher Regulierung. 1030

Damit zusammenhängend führt ein nächster Schritt zum *zweiten Problemfeld*. Für dieses stellt sich die Frage, ob die vom DSG definierten und anerkannten Schutzzwecke sowie die gewählten Strukturmerkmale die datenschutzrechtlichen Herausforderungen und Ziele überhaupt «korrekt» wiederzugeben vermögen. Umgekehrt fragt sich, ob unter Umständen in grundlegender Weise die drei Strukturmerkmale des DSG, wie sie im vorangehenden zweiten Teil herausgearbeitet wurden, überdacht werden sollten.[1335] 1031

Dieser *dritte und letzte Teil* geht diesen Fragekomplexen wie folgt nach: Das VII. Kapitel analysiert die Wirksamkeit des DSG, seine (bislang ungenügende) Bedeutung sowie die faktischen Herausforderungen, denen das geltende Recht begegnet. Das VIII. Kapitel präsentiert die Entwicklungslinien, die als Antwort auf bislang und gemeinhin identifizierte Defizite vorgeschlagen wurden. Die präsentierten Lösungsansätze sollen zugleich kritisch beleuchtet werden. Zur Spra- 1032

1335 In besonders eindrücklicher Weise wird die Fragestellung mit dem in der Abschlussphase dieser Schrift erschienenen Urteil des Bundesverwaltungsgerichts, BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2019, illustriert.

che kommen namentlich auch die Neuerungen, die im Zuge der Totalrevision des DSG vorgesehen werden. Weil diese nicht unwesentlich von der DSGVO angestossen wurden, wird auch auf die Trends, die dieses neue Datenschutzregime bringt, eingegangen. Im IX. Kapitel wird ein eigener Lösungsansatz präsentiert, der für einen *Perspektivenwechsel* plädiert. Ebendieser ist, wie es im Zuge des bisherigen Verlaufs der Studie durchschien, zumindest punktuell und subkutan bereits im aktuellen Datenschutz und dessen Recht angelegt. Diese Studie tritt indes – das Ziel eines effizienten Datenschutzrechts vor Augen habend – für einen konsequenten Perspektivenwechsel resp. einen erweiterten Fokus ein.

VII. Kapitel: Datenschutzrecht auf dem Prüfstand

«While sounding good in theory, the right to privacy has proven hard to apply in practice.»[1336]

A. Bedeutungszuweisungen

Die folgenden Zeilen widmen sich der Frage, welche *Bedeutung dem Datenschutzrecht* zugemessen wird. Insofern erfolgt vorab eine Analyse zur faktischen Verwirklichung des DSG und der insofern präsentierten Einschätzungen. Daran anschliessend wird evaluiert, welche Impulse der Rechtsprechung für die Bedeutung des DSG entnommen werden können. Anschliessend soll anhand eines Blickes auf die politische Debatte sowie die mediale Landschaft der gesellschaftliche Stellenwert, der dem Datenschutz zugemessen wird, eingefangen werden. Die Darstellung wird mit der Totalrevision zwar nicht obsolet, dürfte allerdings etwas von ihrer Relevanz verlieren. 1033

Zunächst wird ein Befund freigelegt, der sich mit dem Begriff des sog. *Vollzugsdefizits* charakterisieren lässt. Die Vorgaben des DSG bleiben in der Realität sowie Unternehmens- wie Behördenpraxis über weite Strecken tote Buchstaben. Das Gesetz existiert in erster Linie auf dem Papier. In der Realität und faktisch wird das DSG nur ungenügend eingehalten, wobei Verstösse gegen seine Vorgaben in aller Regel weiter ohne Konsequenzen bleiben. Das DSG hat faktisch bisher wenig Wirksamkeit gezeitigt. Als ursächlich für dieses Defizit wird gemeinhin der rasante technische Fortschritt verantwortlich gemacht. Auch die Achtlosigkeit der Datensubjekte wird ins Feld geführt. Das Erklärungsmuster für die Wirkungsschwächen aktueller Datenschutzregelungen ist allerdings – wie zu zeigen sein wird – vielschichtiger. Um die Schwachstellen der etablierten Regelungsmechaniken präziser zu benennen, was Voraussetzung für einen Weg in Richtung einer wirkungseffizienten Datenschutzregulierung ist, werden *zwei Kernherausforderungen* detaillierter dargelegt: *Erstens* geht es um die *Kernkapazitäten der modernen Verarbeitungstechnologien*, *zweitens* um das Phänomen der *Vermarktung personenbezogener Angaben*. Werden vor ihrem Hintergrund die Leitideen und Funktionsmechanismen des DSG sowie die Dogmatik des Persönlichkeitsschutzes gemäss Art. 28 ZGB (an die sich das DSG für den privaten Sektor konsequent anlehnt, vgl. zweiter Teil, VI. Kapitel) reflektiert, so zeigen sich diese bereits theoretisch betrachtet als nur beschränkt geeignet, die beschriebenen Entwicklungstrends angemessen zu adressieren. 1034

1336 Richards, Vand. L. Rev. 2010, 1295 ff., 1296.

1. Evaluationen zur faktischen Wirksamkeit des DSG

1035 Auch hierzulande lässt sich für das datenschutzrechtliche Querschnittsgesetz von einem *Vollzugsdefizit* sprechen.[1337] Dieses bezieht sich auf das Gesetz im Gesamten, aber auch auf spezifische Instrumente resp. Strukturelemente. Namentlich das Zusammenspiel der drei im vorangehenden Teil beschriebenen strukturierenden Ansätze trägt dazu bei, dass das Gesetz gerade im privaten Bereich faktisch über weite Strecken ins Leere geht. Die im zweiten Teil dieser Studie herausgearbeiteten der Strukturmerkmale bleiben mit der Totalrevision des DSG, die 2023 und damit lange nach dem Verfassen dieser Schrift in Kraft tritt, erhalten. Allerdings werden sie in substanzieller Weise ergänzt, womit sie zumindest teilweise eine neue Bedeutung erlangen. Weil die drei Strukturmerkmale dem DSG auch künftig charakteristische Züge verleihen, bleibt die Debatte zur Wirksamkeit des DSG in seiner Gestalt vor Totalrevision aufschlussreich.

1036 Schon in einer der Kommissionssitzungen, in denen man sich mit der Ausarbeitung eines Entwurfes für ein eidgenössisches Datenschutzgesetz befasste, erlaubte sich ein Kommissionsmitglied, das geplante Gesetz als «zahnlosen Tiger» zu bezeichnen. Diese Einschätzung, die ohne jegliche Erfahrungswerte basierend auf einen existierenden Erlass gefällt wurde, stattdessen einzig aufgrund einer theoretischen Analyse der gesetzgeberischen Entscheidungen erfolgte, ist bemerkenswert – nicht nur, weil der Kommissionspräsident Pedrazzini, der federführend bei der Verfassung des Entwurfes war, daraufhin – so wird es berichtet – die Contenance verlor.[1338]

1037 Nach der erstmaligen Verabschiedung des DSG verlief die Debatte bezüglich seiner Wirksamkeit vorab in eher leisen und zurückhaltenden Tönen.[1339] Zum einen war bereits der Vorlage zum ersten DSG ein ausgewogener und zweckmässiger Charakter attribuiert worden.[1340] Zum anderen wurde eingeräumt, dass – nicht zuletzt wegen der generalklauselartigen Prägung des Datenschutzgesetzes – vieles ausserhalb der «Macht» des Gesetzes liege:

1337 Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f., 23; indikativ Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.1; Bolliger/Féraud/Epiney/Hänni, 68; unlängst insb. auch Ebert/Widmer, 19; von einem gewissen Vollzugsdefizit sprechen Vasella/Sievers, digma 2017, 44 ff., 48 f.; Wermelinger/Schweri, Jusletter vom 3. März 2008, N 64 statuieren, dass die Schweiz bezüglich Datenschutz kein Musterschüler sei; zur Forderung, wonach das Datenschutzrecht sich an seiner Wirksamkeit orientieren muss, Rudin, in: Sutter-Somm/Hafner/Schmid/Seelmann (Hrsg.), 415 ff., 437 ff.

1338 Vgl. Belser, in: Datenschutz-Forum Schweiz (Hrsg.), Fn 1.

1339 Zum mühseligen gesetzgeberischen Prozess und den Hindernissen, denen insb. die Normierung für den privaten Bereich ausgesetzt war, zweiter Teil, IV. Kapitel.

1340 Daehler, NZZ vom 1. Juni 1993, 21, der Argumente für und gegen das Datenschutzgesetz aufführt.

> «Zusammengedampft um die Hälfte […] hängt aber sehr vieles davon ab, was auf Verordnungsstufe geschieht und wie der Vollzug letztlich gehandhabt wird.»[1341]

DANIOTH wies auf diese Herausforderung hin, liess indes eine hoffnungsvolle Einschätzung zur Produktivität des DSG in seiner Anwendung durchscheinen: 1038

> «Das Datenschutzgesetz echt schweizerischer Prägung weist nur noch die Hälfte der Artikel des früheren Vernehmlassungsentwurfes auf und enthält eine bedeutend geringere Regelungsdichte als die meisten Gesetze anderer Länder. Es verzichtet auf übertriebene Detaillierung und Kasuistik und lässt damit der vernünftigen Interpretation und Rechtsentwicklung genügend Raum […]. Wir Bürger und Behörden haben es in der Hand, was wir in der Praxis aus diesem Gesetz machen wollen […].»[1342]

«Echt schweizerischer Prägung» will heissen: pragmatisch, zurückhaltend und für den privaten Sektor konsequent «den Glanz des Kleinodes schweizerischer Zivilgesetzgebung», Art. 28 ZGB, reflektierend.[1343] Das DSG wurde nach seiner Inkraftsetzung somit durchaus wohlwollend aufgenommen. Exemplarisch beurteilte der damalige Luzerner Datenschutzbeauftragte das DSG als gelungenes Regelwerk zur Wahrung der Schutzzwecke, das widerstreitende Interessen hinreichend austariere.[1344] Als «elegante Lösung» gelobt wurde die für das Zivilrecht vorgesehene Regelung, nach welcher bloss exemplarisch Voraussetzungen genannt würden, unter denen eine Datenbearbeitung zu einer Persönlichkeitsverletzung führe.[1345] 1039

FORSTMOSER zieht zehn Jahre nach dem Inkrafttreten des DSG eine positive Bilanz: Politik und Gesetzgeber – einen solchen Anschein mache es zumindest – hätten das Datenschutzproblem im Griff.[1346] Gerade die Weichenstellung, den öffentlichen und den privaten Bereich einem jeweils unterschiedlichen Regime zu unterstellen, habe sich bewährt. Anders dagegen befindet SCHWEIZER im Jahr 2003, dass das DSG den «gesellschaftlichen und ökonomischen Wert des informationellen Persönlichkeitsschutzes nur beschränkt vermitteln konnte».[1347] BAERISWYL, der kantonale Datenschutzbeauftragte Zürichs, fordert im gleichen Jahr eine grundlegende Überdenkung der Strukturen und Instrumente des Datenschutzgesetzes und seiner Schwachstellen.[1348] 1040

Vonseiten der «Datenbankbesitzer», der Privatwirtschaft und insb. der Kreditauskunfteien wurde die Implementation des DSG als reibungslos beurteilt. Ge- 1041

1341 KÜCHLER, AB 88.032, 13. März 1990, 129.
1342 DANIOTH, AB 88.032, 13. März 1990, 128.
1343 Ebendies und namentlich die Quantität der Bestimmungen an sich sind unbestritten nicht geeignet, um eine Aussage zur «Güte» des Gesetzes zu machen.
1344 BRÜNDLER, SJZ 1993, 129 ff., 133.
1345 DERS., a. a. O., 129 ff., 129.
1346 FORSTMOSER, digma 2003, 50 ff., 55; dass die datenverarbeitenden Stellen den Datenschutz dagegen nicht im Griff haben, wird erst einige Jahre später deutlich gemacht werden.
1347 SCHWEIZER, digma 2003, 58 ff.
1348 BAERISWYL, digma 2003, 48 ff., 49; kritisch auch insb. mit Blick auf den öffentlich-rechtlichen Bereich RUDIN, BJM 1998, 113 ff.

mäss B & D, einem der grössten Kreditauskunft-Unternehmen, hat das DSG, abgesehen von der Registrierungspflicht, keine oder kaum Konsequenzen gezeitigt.[1349]

1042 Die Rechtsprechung zur Datenschutzgesetzgebung zeigte sich – anders als in Deutschland – in den ersten fünfzehn Jahren nach Inkrafttreten des DSG unspektakulär. Es blieb bei einer weitgehend am Einzelfall ausgerichteten Judikatur, die dem Datenschutzrecht wenig Kontur verlieh.

1043 Die Bilanz fiel damit, so ein erster Blick auf die Erfahrungen mit dem DSG in seinem ersten Dezennium, durchzogen aus.[1350]

1044 Nach weiteren Jahren Erfahrung mit dem DSG wird die vorab wohlwollende Rezeption des DSG zusehends von kritischen Beiträgen abgelöst.[1351] Es stellt sich eine gewisse Ernüchterung ein. Bildhaft bissig beschreibt Brunner einen datenschutzrechtlichen Ohnmachtszustand in virtuellen Welten, indem er den Datenschutz als Musketier mit rostiger Flinte vergleicht.[1352]

1045 Das 20-jährige Bestehen des eidgenössischen Datenschutzgesetzes nahm der Bundesrat zum Anlass, das DSG einer Evaluation zu unterziehen.[1353] Dabei war

> «Ziel der Evaluation […], das Datenschutzgesetz auf seine Wirksamkeit hin zu überprüfen. Nicht Gegenstand der Evaluation waren die im Zuge der Reformen des Datenschutzgesetzes per 1. Januar 2008 und 1. Dezember 2010 eingeführten neuen Bestimmungen, weil hierzu noch zu wenige Erfahrungen vorliegen.»[1354]

1046 Mit der Evaluation wollte man eine Basis zur Fortentwicklung des Schweizer Datenschutzrechts schaffen. Sie erschien im Lichte des «rasanten technischen Fortschrittes» sowie der anrollenden datenschutzrechtlichen Revisionswelle aus der EU angezeigt. Zugleich sollte mit dem Evaluationsbericht auf die Postulate Hodgers sowie Grabers reagiert werden.[1355] Der Auftrag zur Gesamtevaluation ging an das Büro Vatter AG, das Institut für Europarecht der Universität Freiburg sowie das Umfrageinstitut Demoscope AG.[1356] Als Ergebnis liegt neben dem Schlussbericht der mit der Evaluation Betrauten der Bericht des Bundesrates zu ebendiesem Bericht vor. Letzterer stellt eine «Interpretation» des Schlussberichts

1349 Vgl. den Artikel «Persönlichkeitsschutz contra Gläubigerschutz; Datenschutzaspekte von Kreditinformationssystemen», NZZ vom 4. Januar 1995, 23.
1350 Vgl. zur Rechtsprechung dritter Teil, VII. Kapitel, A.2.
1351 Baeriswyl, digma 2003, 48 ff.; Huber, recht 2006, 205 ff.; vgl. Brunner, Jusletter vom 4. April 2011, N 1 ff.; Drechsler, AJP 2007, 1471 ff.; vgl. sodann die Evaluationen durch Bolliger/Féraud/Epiney/Hänni, *passim* sowie Ebert/Widmer, *passim* sowie BR, Schlussbericht Evaluation 2011–1952, 335 ff.
1352 Brunner, Jusletter vom 4. April 2011, N 1 ff.
1353 BR, Schlussbericht Evaluation 2011–1952, 335 ff.; Bolliger/Féraud/Epiney/Hänni, *passim*.
1354 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 339.
1355 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 340 f.
1356 Bolliger/Féraud/Epiney/Hänni, 4.

dar.[1357] Im bundesrätlichen Bericht liest man zurückhaltend positiv, vermittelnd diplomatisch und gleichzeitig ausweichend desillusionierend:

> «Das Datenschutzgesetz erzielt insgesamt zweifellos eine gewisse Wirksamkeit. Insofern sind die ursprünglichen Erwartungen an das Datenschutzgesetz, soweit diese überhaupt feststellbar sind, zumindest teilweise erfüllt worden.»[1358]

Basierend auf dem Befund der ungenügenden Griffigkeit des DSG in der Realität wurde direkt die Frage aufgeworfen, ob der «Schutz des Privaten» überhaupt noch ein schutzwürdiges Interesse sei. Insofern auch der Schlussbericht zur Evaluation des DSG: 1047

> «Während im Vorfeld der Verabschiedung des Gesetzes durch die eidgenössischen Räte der „Fichenskandal" ein dominierendes politisches Thema war, stellt sich heute im Zeitalter des Internets und weltweiter Kommunikationsmöglichkeiten die Frage, inwiefern der Datenschutz überhaupt noch einem Bedürfnis der Bevölkerung entspricht, und inwieweit er als störendes Hindernis des freien Informationsflusses wahrgenommen wird.»[1359]

Ein mutmasslich entfallender Bedarf am Datenschutz wird durch eine zusätzliche Behauptung flankiert: Nur diejenigen, die etwas zu verstecken hätten, wollten Privatheit.[1360] Eine solche Schlussfolgerung drängt sich auf für ein Datenschutzrecht, das konsequent dem Individualrechtsschutz verpflichtet ist und in welchem das Datensubjekt – so wird es zumindest beschrieben – nur wenig für die Rechtseinhaltung und -durchsetzung tut. Sie übersieht allerdings nicht nur die Basisstruktur des DSG sowie die datenschutzrechtlichen Realitäten, sondern auch die datenschutzrechtlichen Herausforderungen. Ihnen widmet sich dieses Kapitel vertieft. Bereits die bisherigen Ausführungen haben Indizien zu Tage geführt, wonach das attestierte Vollzugsdefizit des DSG nicht unwesentlich in seinen Ansätzen und Instrumenten selbst zu verorten ist. Namentlich die individualrechtliche Konzeptionierung scheint zu kurz zu greifen.[1361] 1048

1357 In die Evaluation integriert wurden namentlich die Untersuchung der nationalrätlichen Geschäftsprüfungskommission zum Datenschutz in der Bundesverwaltung (GPK-N 2003; Bundesrat/BBl 2004: 1431–1436), die Analyse der Eidgenössischen Finanzkontrolle beim EDÖB (EFK 2007) sowie eine Untersuchung zum Datenaustausch zwischen Behörden (vgl. Bolliger/Féraud/Epiney/Hänni); spezifisch der Frage nach dem Umgang der Datensubjekte mit ihren persönlichen Daten, ihrer Haltung zum Datenschutz sowie zu ihren Kenntnissen und Erfahrungen bezüglich des DSG widmete sich sodann die Umfrage von Privatim 2009.

1358 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 345.

1359 Bolliger/Féraud/Epiney/Hänni, 45; gewieft folgert Zuckerberg aus dem in den USA mit ihrer punktuellen datenschutzrechtlichen Regulierung gezogenen Befund, wonach Datenschutz nicht griffig funktioniere: Privacy is no longer a social rule, im Guardian vom 11. Januar 2010, abrufbar unter: <https://www.theguardian.com/international> (zuletzt besucht am 30. April 2021.

1360 Vgl. Nissenbaum, 76, die diese Behauptung sogleich entkräftet mit dem Beispiel, wonach Ausscheidungen vom grössten Teil der Menschen am «stillen Örtchen» in Diskretion erledigt werden, obschon es sich hierbei nicht um etwas Verbotenes, sondern das «Natürlichste» der Welt handelt; kritisch auch Bull, Computer, 11.

1361 Für die Schweiz früh Rudin, digma 2001, 126 ff., 126.

1049 Im Rahmen der Evaluation des Datenschutzgesetzes sind die relativierend-beschwichtigenden Worte augenfällig. So habe das DSG

> «im Bereich der Herausforderungen, die bereits zum Zeitpunkt seines Inkrafttretens bestanden, eine spürbare Schutzwirkung erzielt. Die grosse Mehrheit der öffentlichen und privaten Datenbearbeitenden ist einigermassen sensibilisiert für den Datenschutz und beachtet in pragmatischer Art und Weise die Bestimmungen des Datenschutzgesetzes.»[1362]

1050 Die Beurteilungen betreffend die Einhaltung und Wirksamkeit des DSG im öffentlichen und privaten Bereich divergieren.[1363] Einen Wirksamkeitsfortschritt attestierte man früh für den öffentlichen Sektor, während die frühere Richtlinie von 1981 über die Bearbeitung von Personendaten in der Bundesverwaltung quasi toter Buchstabe geblieben sei.[1364] Im Evaluationsbericht wird davon ausgegangen, dass im öffentlichen Bereich das Legalitätsprinzip, mithin das Verarbeitungsverbot mit Erlaubnistatbeständen, einer uferlosen Bearbeitung Grenzen setze.[1365] Das Vertrauen in die Polizei beispielsweise hinsichtlich des Umgangs mit Personendaten sei folglich höher als in private Unternehmen.[1366] Bundesorgane würden den Datenschutz eher besser berücksichtigen als Private.[1367]

1051 Die grössten Probleme werden damit im *Privatbereich* verortet, was von einer jüngst erschienenen empirischen Studie bestätigt zu werden scheint.[1368] Die Einschätzung eines Interviewpartners der Evaluation fällt ernüchternd aus, wenn es heisst, dass es in der Schweiz

> «kein Unternehmen gäbe, das das DSG vollständig einhalte. Es gäbe aber sehr viele Firmen, die sich bemühen, vorschriftskonform zu handeln, selbst wenn die Gefahr gering sei, bei einer Verletzung sanktioniert zu werden. Für grössere Unternehmen, die in der Öffentlichkeit stünden, sei die Normkonformität bedeutsamer. Anreize zur Beachtung des Datenschutzrechts für Unternehmen seien eher das Image- und Investitionsrisiko.»[1369]

1052 Ein Kernproblem wird im *Fehlen von konkreten Handlungsanleitungen* verortet.[1370] Damit sind insb. die generalklauselartigen Bearbeitungsgrundsätze angesprochen.[1371] Problematisiert wird im Evaluationsbericht die Nichteinhaltung der

1362 Nissenbaum, 336 und 342.
1363 Zum Dualismus zweiter Teil, IV. Kapitel.
1364 «Offenbar ist es weitgehend bei der Fleissarbeit des Dienstes für Datenschutz geblieben. Sonst aber blieben die Richtlinien weitgehend toter Buchstabe, und zwar sowohl bei den Beamten, die sie hätten anwenden sollen, wie auch bei den Behörden, dem Bundesrat und unserem Parlament – vor allem auch bei der Geschäftsprüfungskommission –, die sie hätten kontrollieren sollen. Denn wären sie gehandhabt worden, hätten viele der unrichtigen, heute überholten und unangepassten, oft für andere Zwecke erhobenen Daten und Fichen längst vernichtet werden müssen», AB 88.032, 13. März 1990, 126.
1365 Bolliger/Féraud/Epiney/Hänni, 34 und 38.
1366 Dies., 53.
1367 Dies., 37.
1368 Dies., 35; Ebner/Widmer, 5 ff.
1369 Bolliger/Féraud/Epiney/Hänni, 38, 192.
1370 Dies., 41.
1371 Zu den generalklauselartigen Bearbeitungsgrundsätzen zweiter Teil, V. Kapitel.

Bearbeitungsgrundsätze der Erkennbarkeit, aber auch der Zweckbindung sowie Verhältnismässigkeit.[1372] Entgegen dem Verhältnismässigkeitsgrundsatz würden zudem Daten auf Vorrat gesammelt.[1373] Missbräuche blieben in aller Regel unentdeckt.[1374] Die nicht regelkonformen und unbeschränkten Personendatenverarbeitungen werden oftmals mit den Chancen zur Effizienz- und Profitsteigerung begründet.[1375] Der Einhaltung der Vorgaben des DSG abträglich sei sodann die geringe Wahrscheinlichkeit einer Sanktion.[1376] Das Durchsetzungsrisiko wird als niedrig eingestuft, zumal die Durchsetzungsmechanismen als zu schwach gelten: Die Rechtsdurchsetzung wird aufgrund der Anknüpfung im Persönlichkeitsrecht an erster Stelle auf die Schultern des Subjektes gelegt, wobei der Gang an das Gericht meist eine zu hohe Hürde sei. Hierzu sowie allgemein zum Erkennbarkeitsgrundsatz heisst es:

> «Schliesslich gilt es auf einen Umstand hinzuweisen, der sich im Zuge der technologischen Herausforderungen ergibt (vgl. Kapitel 3): Datenbearbeitungen sind aufgrund der verfügbaren technischen Möglichkeiten verschiedentlich für die Betroffenen nicht mehr erkennbar. Die Frage nach den Missbrauchserfahrungen in der Bevölkerung lässt vermuten, dass es sich häufig um eher klassische Situationen handelt, wenn Betroffene einen Missbrauch vermuten. In die gleiche Richtung deutet auch die qualitative Analyse der Gerichtsurteile im folgenden Kapitel. Somit muss zumindest berücksichtigt werden, dass ein Teil von Persönlichkeitsverletzungen für die Betroffenen – selbst wenn sie sehr sensibilisiert sind – gar nicht erkennbar ist. Dieses Argument lässt sich grundsätzlich auch für klassische Konstellationen anführen, es dürfte aber angesichts des technischen Wandels zunehmend an Bedeutung gewinnen.»[1377]

Die vorab aussergerichtlich geltend zu machenden *Betroffenenrechte*, die der Umsetzung, Durchsetzung und Einhaltung des Datenschutzrechts Nachachtung verschaffen sollen, stehen in Einklang mit der subjektivrechtlichen und – für den privaten Bereich – persönlichkeitsrechtlichen Basierung des Datenschutzgesetzes. Das Auskunftsrecht nach DSG, Art. 8 DSG, ist beschränkt und *de lege lata* nur gegenüber Inhabern von Datensammlungen verbürgt. Es hat gleichermassen Präventiv- wie Kontrollfunktion. Es findet in der Informationspflicht gemäss Art. 14 und Art. 18a DSG sein Pendant.[1378] Mit der Totalrevision sind die Art. 19 ff. und Art. 25 ff. nDSG einschlägig, welche die Transparenzvorgaben ausbauen. Mit der Einräumung des – vergleichbar mit dem Gegendarstellungsrecht des ZGB – zunächst aussergerichtlich geltend zu machenden Auskunftsrechts wird zum Ausdruck gebracht, dass der Erkennbarkeitsgrundsatz sowie die Informationspflicht nicht als hinreichend wirkungsvolle Garanten gesehen werden, um datenschutz- 1053

1372 Bolliger/Féraud/Epiney/Hänni, 7 ff., 29 ff.
1373 Hannich/Jenni/Beerli/Mandl, in: ZHAW (Hrsg.), 29 ff.
1374 Bolliger/Féraud/Epiney/Hänni, 38.
1375 Dies., 52 und 91.
1376 Dies., 19; Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.1.
1377 Bolliger/Féraud/Epiney/Hänni, I.
1378 Vertiefend Widmer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 5 N 5.2. ff.

rechtliche Transparenz zu gewährleisten. Das Auskunftsrecht muss in diesem Sinne als flankierendes Korrektiv verbürgt werden, das zugleich dem Subjekt zumindest formell eine aktive Rolle im Datenverarbeitungsgeschehen verschaffen will. Zwar wird das Auskunftsrecht in der Praxis durchaus geltend gemacht. In Anbetracht der quantitativen und qualitativen Bedeutung von Personendatenverarbeitungen kann dieses gleichwohl nicht als effizientes Kontrollinstrument mit Blick auf die Gesetzeskonformität von Personendatenverarbeitungen qualifiziert werden. Ebenso wenig ist für die Schweiz erhoben, ob Auskunftsansprüche ähnlich oft ignoriert werden, wie es in einer Studie für Deutschland nachgewiesen wurde.[1379] Immerhin wurde das Auskunftsrecht, wie der Blick auf die Judikatur zeigen wird, durchaus auch schon gerichtlich durchgesetzt. Dass in der Folge eines Auskunftsanspruches eine nicht im Einklang mit datenschutzgesetzlichen Vorgaben stehende Verarbeitungshandlung gerichtlich angefochten wird, kommt gleichwohl kaum je vor.[1380] Die weiteren Betroffenenrechte sind ebenso wenig auf die gerichtliche Geltendmachung beschränkt, wie es Art. 15 DSG resp. Art. 32 nDSG vermeinen lassen könnte. Vielmehr können auch diese Ansprüche vorab unmittelbar gegenüber den verarbeitenden Stellen geltend gemacht werden. Dass das Gesetz diese Rechte nur innerhalb der klageweisen Durchsetzungsbehelfe verankert, mag mit ein Grund sein, dass ebendiese in der Realität kaum je geltend gemacht werden – auch nicht aussergerichtlich.[1381] Die derzeit im Schweizer DSG implementierten individualrechtlichen Ansprüche sind, *zusammengefasst*, zu kurze «Spiesse» für die Durchsetzung des DSG.[1382]

1054 Vor diesem Hintergrund sind auch Vorstösse z. B. von Privatim, der Konferenz schweizerischer Datenschutzbeauftragter, zu lesen. Wiederholt wurde von dieser Organisation für einen Ausbau organisatorischer und prozeduraler Instrumente im Interesse des Datenschutzes plädiert und die Ausstattung vorhandener behördlicher Stellen mit mehr und angemessenen Ressourcen gefordert.[1383] Die Totalrevision liefert gewisse Instrumente und damit wohl auch Fortschritte.

1055 An dieser Stelle ist an auf einem bemerkenswerten Befund einzugehen: Menschen erklären bis heute, dass ihnen die Einhaltung des Datenschutzrechts wichtig

1379 Vgl. Burghardt/Böhm/Buchmann/Kuhling/Sivridis, in: Sivridis/Patrikakis/Burghardt et al. (Hrsg.), die von einer Nichtreaktion auf Auskunftsbegehren in rund 30 Prozent der Fälle berichten, 3 ff., 9.

1380 Vgl. Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.20 f.

1381 Bolliger/Féraud/Epiney/Hänni, II.

1382 Dies., II und III.

1383 Privatim, Resolution vom 18. Dezember 2019, abrufbar unter: <https://www.privatim.ch/wp-content/uploads/2019/12/privatim_Resolution_Ressourcen_v1_0_20191218.pdf> (zuletzt besucht am 30. April 2021); vgl. auch Dies., Medienmitteilung vom 2. September 2010, abrufbar unter: <https://www.privatim.ch/wp-content/uploads/2017/06/2010_Unabhaengige_Datenschutzaufsicht_im_Staatsschutz.pdf> (zuletzt besucht am 30. April 2021).

sei («they care»).[1384] Allerdings gilt das ihnen als eingeräumte Instrumentarium für die Durchsetzung des Datenschutzrechts als ungenügend. Diese Erkenntnisse führten auch zu einer Forderung, wonach ein wirksamer Datenschutz resp. ein griffiges Datenschutzrecht zu entwickeln sind. Die Neuerungswellen, wie sie mit dem DSGVO und der Totalrevision des DSG einhergehen, bestätigen dies. Eine im Rahmen der ersten Teilrevision des DSG getätigte Aussage dürfte damit heute widerlegt sein:

> «Es wird somit davon ausgegangen, dass die betroffene Person selbst die ihr zustehenden Rechte ausüben kann, wenn sie über die Datenbeschaffung informiert ist, und dass bezüglich der Kontrollfunktion des Datenschutzbeauftragten keine weitergehenden Massnahmen erforderlich sind.»[1385]

Dass ein Regelungsregime, das auf generalklauselartigen Grundsätzen fusst, die 1056
im privaten Bereich die entscheidende Schranke der Verarbeitungsfreiheit definieren, und dass die individualrechtliche Durchsetzung Schwachstellen aufweist, wurde bereits im Rahmen der Verabschiedung des DSG erkannt. Entsprechend wurde «flankierend» die Funktion des ED(Ö)B eingeführt.

Im Evaluationsbericht jedoch wird attestiert, dass der EDÖB nicht über genü- 1057
gend Ressourcen verfüge und die Sanktionen im DSG zu schwach seien.[1386] Vor diesem Hintergrund erstaunt es nicht, dass gerade in der Schweiz die mit der DSGVO weit- und tiefgreifenden Sanktionen sowie Massnahmen der Behörden prominent thematisiert werden.[1387] Für die meisten Unternehmen in der Schweiz, die einzig unter das DSG fallen, reiche es dagegen aus,

> «mit dem allgemeinen Strom zu schwimmen und keine gravierenden Datenschutzverletzungen zuzulassen. Oft würden unternehmerische Strategien entwickelt und Entscheidungen gefällt, die dem Datenschutz nicht immer zuträglich seien.»[1388]

Betreffend die Bedeutung der Funktion des EDÖB für die Einhaltung des DSG ist 1058
eine Aussage des EDÖB selbst zitierwürdig:

1384 Bolliger/Féraud/Epiney/Hänni, II; vgl. auch Nissenbaum, 186 ff.; BR, Schlussbericht Evaluation 2011–1952, 335 ff., 342; dies gilt auch für das Internet, wobei viele Menschen ihre Personendaten zur Verfügung stellen, sofern sie einen adäquaten Gegenwert hierfür erhalten; m. w. H. Waidner/Karjoth, digma 2004, 18 ff., 20; als Privacy-Paradox umschrieben, weil einerseits die Sorge um den Schutz eigener Personen betont wird, andererseits Personendaten grosszügig preisgegeben werden, m. w. H. Auf der Mauer/Fehr-Bossard, in: Thouvenin/Weber (Hrsg.), ITSL 2017, 23 ff., 28 f.; früh schon Bibas, Harv. J.L. & Pub. Pol'y 1994, 591 ff., 597 f.; Eckhardt/Fattebert/Keel/Meyer, 5 scheint es so, als ob die Bedeutung der Privatsphäre für viele Menschen abnehme. Das Nutzungsverhalten der Menschen von neuen Technologien führt nicht selten zu einer solchen Folgerung, die allerdings zu kurz greift: Es ist empirisch dokumentiert, dass der Datenschutz als wichtiges Anliegen benannt wird; sie wollen indes ebenso die neuen Technologien nutzen. Beiden Elementen hat das Recht Rechnung zu tragen; vgl. auch die Befunde bei Dörflinger, 83 ff.

1385 Botschaft DSG 2003, 2101 ff., 2108.

1386 Vgl. Bolliger/Féraud/Epiney/Hänni, 5, 38 f., 139 ff., 153 ff.

1387 Vgl. Exemplarisch Müller, NZZ vom 14. Juli 2017, abrufbar unter: <https://www.nzz.ch/wirtschaft/folgen-der-neuen-datenschutz-grundverordnung-eu-datenschutzverordnung-tangiert-auch-die-schweiz-ld.1306009> (zuletzt besucht am 30. April 2021).

1388 Bolliger/Féraud/Epiney/Hänni, 37.

> «[M]ehrere private Bearbeiter gaben an, sich gut zu überlegen, mit welchen Fragen und Problemstellungen sie sich an den EDÖB wenden, um nicht „schlafende Hunde" zu wecken.»[1389]

1059 Dem EDÖB als Wächter über das DSG (vor Totalrevision) wird gemäss eigener Aussage und Einschätzung ein gewisser Respekt gezollt. Über die Empfehlungskompetenz im privaten Bereich hinaus nimmt der EDÖB eine wichtige Funktion im Rahmen der Sensibilisierung und Informierung ein – seine Homepage bietet eine gut ausgebaute Informationsplattform, auf der sich regelmässig Presseberichte zum Thema, Hinweise auf Entscheide usf. finden; zudem nimmt der EDÖB regelmässig in den Medien Stellung zum Thema.[1390] Die Informations-, Weiterbildungs- und Schulungsmöglichkeiten im Bereich des Datenschutzes gelten gleichwohl als zu schmal. In der Schweiz gibt es bislang eher wenige Datenschutzexpertinnen und -experten. Die dem EDÖB zugebilligten Ressourcen beschränken die Amtsausübung zusätzlich auf einen engen Rahmen. Die ungenügenden Ressourcen bilden eine Kernproblematisierung bezüglich der Effizienz und Durchschlagskraft des EDÖB und dahinterstehend des DSG.[1391] Der EDÖB (resp. seine Handlungsoptionen) sei für die Unternehmen zu wenig furchteinflössend, um diese dazu zwingen zu können, sich an die gesetzlichen Regeln zu halten.[1392]

1060 Dennoch ergingen von seiner Seite in den letzten Jahren einige bedeutsame Empfehlungen, wobei der EDÖB diesen, sofern erforderlich, über den Gerichtsweg Nachachtung zu verleihen versucht(e).[1393] Im Nachgang an eine unter bisherigem DSG vom EDÖB erlassene Empfehlung ist nicht immer der Gang an das Bundesverwaltungsgericht notwendig. Dies zeigt die «Intervention» des EDÖB gegenüber der Valora: Ende 2016 erschienen mehrere Berichte in Publikumsmedien, denen zufolge Valora in ihren Kioskfilialen Mobilfunkdaten ihrer Kunden erfasse und für personifizierte Werbung nutzen wolle. Der EDÖB nahm daraufhin in dieser Angelegenheit Abklärungen vor. Valora legte dem EDÖB in einer schriftlichen Stellungnahme dar, dass sie keine personenbezogenen Daten bearbeite, stattdessen aggregierte Daten einzig zu statistischen Zwecken auswerte. Das Unternehmen erklärte sich zudem bereit, auf seiner Website detaillierter über das Projekt zu informieren. Gestützt darauf sah der EDÖB keinen weiteren Hand-

1389 Bolliger/Féraud/Epiney/Hänni, 137.
1390 Zum Beispiel der amtierende EDÖB Lobsiger in der NZZ vom 25. Mai 2018 oder im Interview, NZZ vom 29. Juli 2019; neu wird der EDÖB über das ordentliche Verwaltungsverfahren auch Verfügungen erlassen können, vgl. Rosenthal, Jusletter vom 16. November 2020, N 181 ff.
1391 Vgl. auch BR, Schlussbericht Evaluation 2011–1952, 335 ff., 339 ff.
1392 Bolliger/Féraud/Epiney/Hänni, 163.
1393 Unlängst BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018; weiter zu nennen sind BGE 138 II 346 – Street View, Urteil vom 31. Mai 2012; BGE 136 II 508 – Logistep, Urteil vom 8. September 2010; vertiefend zur Rechtsprechung dritter Teil, VII. Kapitel, A.2.

lungsbedarf und schloss das Verfahren gegen Valora ab.[1394] Anders die Situation im jüngsten Fall einer App der Helsana Zusatzversicherungs-AG, die den Empfehlungen des EDÖB nicht folgen wollte. Letztlich kam es zu einem Urteil des Bundesverwaltungsgerichts.[1395] Dieser Trend der effizienteren Rechtsdurchsetzung dürfte sich mit der Totalrevision des DSG fortsetzen. Auch der EDÖB dürfte dem datenschutzrechtlichen Bedeutungswandel Nachachtung verschaffen. Mit anderen Worten ist mit einer gesteigerten Behördenaktivität zu rechnen, vgl. hierbei Art. 49 ff. nDSG und zu den strafrechtlichen Sanktionen, die von kantonalen Behörden verhängt werden, Art. 60 ff. nDSG.

Das Hauptrisiko für die Datenverarbeitenden bleibt de lege lata in der Schweiz – sofern sie nicht in den Anwendungsbereich der DSGVO aufgrund von Art. 3 DSGVO fallen – in einer «*schlechten Presse*».[1396] Einer Einschätzung im CRM-Bericht 2012, der sich mit datenschutzrechtlichen Belangen im Kontext von Customer Relationship Management befasst und meint, dass die Medien «immer kreativere» Beispiele von Kriminalität aufgrund von Datenmissbrauch an die Öffentlichkeit tragen und damit zwangsläufig Angst und Misstrauen verbreiten, ist nicht beizupflichten.[1397] Die Rolle der *Medien vis-à-vis* dem Datenschutz, so wird zu zeigen sein, ist mehr als diejenige des Unruhestifters und Angstmachers. Paradoxerweise gibt der Bericht selbst wenig Anlass zur Beruhigung, weder was seinen Duktus noch seinen Inhalt anbelangt. Er führt aus: 1061

> «Verheerend sieht es bei einem Drittel der Schweizer Unternehmen aus. Sie verzichten gänzlich auf die Information ihrer Kunden (bzgl. Datenerfassung).»[1398]

Im Evaluationsbericht wird auf die fehlende Sensibilität und die Zurückhaltung der Datenbearbeitenden bei der *Annahme eigener Verantwortlichkeiten und ihrer eigenen Rolle* hingewiesen.[1399] Dass die Einhaltung des DSG in seiner noch geltenden Fassung von den verarbeitenden Stellen *nicht* als primär eigene Verantwortung im Sinne einer Compliance- oder Governance-Aufgabe verstanden wird, ist eine Konsequenz eines Datenschutzgesetzes zu sehen, das auf die Verletzungshandlung der Persönlichkeit, vgl. Art. 12 f. DSG, fokussiert. Damit geht eine subjektiv- und abwehrrechtlich gedachte Durchsetzungsmechanik einher. Art. 30 ff. nDSG greifen konzeptionell Art. 12 ff. DSG auf. Gleichwohl werden mit der Totalrevision markante Kontrapunkte durch die Einführung faktischer Umsetzungs- 1062

1394 Vgl. Daten:recht, Informationen des EDÖB zum Personentracking; Verfahren gegen Valora abgeschlossen, Zürich 2017, <https://datenrecht.ch/informationen-des-edoeb-zum-personentracking-verfahren-gegen-valora-eingestellt/> (zuletzt besucht am 30. April 2021).

1395 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018.

1396 Zum medialen Rauschen als Hauptwirkung des Datenschutzrechts Vesting, in Ladeur (Hrsg.), 155 ff., 182.

1397 Hannich/Jenni/Beerli/Mandl, in: ZHAW (Hrsg.), 43.

1398 So vertreten von Dies., a. a. O., 44.

1399 Bolliger/Féraud/Epiney/Hänni, 13; indikativ auch Ebert/Widmer, 3 ff.

instrumente sowie ausgebaute wie verschärfte Behördenkompetenzen geschaffen. Sie werden im VIII. Kapitel dieses dritten Teils dargestellt.

1063 Vor dem Hintergrund dieser Darstellung ist der aus der Evaluation gezogene Befund vonseiten des Bundesrates, wonach sich das Datenschutzgesetz «grundsätzlich bewähre», bemerkenswert.[1400] Das Wort «grundsätzlich» dürfte sich auch auf seine Strukturmerkmale beziehen, wie sie im zweiten Teil herausgearbeitet wurden. Weder über den pointierten Dualismus mit entgegengesetzten Ausgangspunkten noch die entscheidenden Schranken in Gestalt von generalklauselartigen Verarbeitungsvorgaben noch die persönlichkeits-, individual-, delikts- und abwehrrechtliche Anknüpfung des DSG im privaten Bereich wurde grundlegend debattiert. Allerdings muss für das DSG im privaten Bereich von beträchtlichen Defiziten hinsichtlich seiner faktischen Einhaltung und Durchsetzung ausgegangen werden. Unbestritten dürfte sein, dass die drei Grundprinzipien hierfür mitursächlich sind. Nachdem eine beschränkte Wirksamkeit des DSG für den privaten Bereich in der Realität beschrieben wurde, soll nunmehr analysiert werden, inwiefern das Datenschutzgesetz und allgemeiner das Datenschutzrecht durch die Lehre und Rechtsprechung effektuiert wird. Es geht damit zugleich um die Frage, welche Bedeutung dem Datenschutzgesetz und -recht in der Schweiz zugemessen wird.

2. Effektuierung durch Lehre und Rechtsprechung

2.1. Tour d'Horizon

1064 Bilden Generalklauseln den Kern der Handlungsanleitungen an die Bearbeitenden, kommt der *Konkretisierung* ebendieser für die Effektuierung des Datenschutzrechts in der Praxis entscheidende Relevanz zu. Konkretisierung und Auslegung erfolgen über die Lehre und Rechtsprechung, vgl. Art. 1 ZGB. Relevant sind die Ausführungen namentlich im zweiten Teil, IV. Kapitel.

1065 An dieser Stelle geht es darum, die dem Datenschutzrecht und dem DSG im Schrifttum zugemessene Bedeutung zu umreissen. Die Lehre zum Datenschutzrecht und Datenschutzgesetz ausserhalb der medialen Behandlung ist fest in der Hand der *Praktikerinnen und Praktiker*, namentlich der Anwaltschaft. Mehrere Rechtsanwältinnen und Rechtsanwälte haben das Thema jüngst stark besetzt. Sodann publizieren nicht nur der Eidgenössische Datenschutzbeauftragte, sondern auch die kantonalen Datenschutzbeauftragten regelmässig zum Datenschutzrecht und spezifisch zum DSG. Sichtet man das Schrifttum zum Datenschutzgesetz, ist zudem gewissermassen in Entsprechung zum gesetzgeberisch

1400 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 339 ff., 347.

gewählten Dualismus mit seinem markant höheren Schutzniveau für den öffentlichen Bereich eine verstärkte Konzentration auf ebendiesen Bereich festzustellen. Das DSG für den privaten Bereich hat von wissenschaftlicher Seite her viele Jahre nur beschränkte Aufmerksamkeit auf sich gezogen. Eine erste und für lange Zeit alleinstehende wissenschaftliche Studie zum Datenschutzgesetz im privaten Sektor legte im Jahr 1994 PETER mit seiner Zürcher Dissertation vor.[1401] Neueren Datums ist die Dissertation von HEUBERGER zum Profiling im DSG.[1402] Jüngst erschienen sodann eine beachtliche Doktorthesis von KASPER.[1403] Wissenschaftliche Monografien wie Dissertationen oder Habilitationen spezifisch zum *Datenschutzgesetz* als Kernerlass datenschutzrechtlicher Normierung bleiben Raritäten.[1404] Einen Beitrag für die wissenschaftliche Aufbereitung des Themenfeldes sollte das Forschungsprogramm NFP 75 «Big Data» bringen. Mit dem Inkrafttreten der DSGVO, aber auch der Ausarbeitung einer Totalrevision des DSG ist ein sich steigerndes Interesse in der Lehre zu verzeichnen.

Zudem wurde das Thema in den letzten Jahren stärker institutionell verankert, indem Forschungsstellen und Kompetenzzentren gegründet,[1405] informationsrechtliche Lehrstühle aufgebaut, Schriftenreihen[1406] und Zeitschriften[1407] etabliert wurden und das Thema in die Curricula auf der Stufe der Masterstudiengänge vermehrt integriert wird.[1408] 1066

Eine Sichtung der Lehre bestätigt, dass sich das Datenschutzrecht nicht im DSG und seinem Dualismus erschöpft. Vielmehr beschäftigt man sich für den privaten Bereich mit spezifischen Kontexten, Branchen und Sektoren, die oft spezialgesetzlich erfasst werden. An erster Stelle in der Schweiz stehen hierbei 1067

1401 PETER, Das Datenschutzgesetz im Privatbereich. Unter besonderer Berücksichtigung seiner motivationalen Grundlage, Diss. Zürich 1994.
1402 HEUBERGER, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, Diss. Luzern 2020.
1403 KASPER, People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, Diss. St. Gallen 2021.
1404 Immerhin ist auf die Basler Dissertation von GLASS hinzuweisen, die indes einen öffentlich-rechtlichen Fokus wählt; sodann spezifisch zur datenschutzrechtlichen Einwilligung die Dissertation von FASNACHT; beachte sodann die Doktorarbeiten von BUCHER aus dem Jahr 2010 zu Spyware sowie HÄUSERMANN aus dem Jahr 2009 zur Vertraulichkeit als Schranke von Informationsansprüchen; hinzuweisen ist sodann auf die bereits zitierte Habilitationsschrift von AEBI-MÜLLER sowie die Dissertation von STÄMPFLI zum Schengener Informationssystem und das Recht auf informationelle Selbstbestimmung.
1405 Vgl. ebendiese an den Universitäten St. Gallen, Zürich sowie Fribourg.
1406 Vgl. z. B. «Studien zu Information, Kommunikation, Medien und Recht, Beiträge der Forschungsstelle für Informationsrecht an der Universität St. Gallen».
1407 Zeitschrift für Datenrecht und Informationssicherheit, digma, sowie die sic!
1408 Vgl. z. B. an der Universität Luzern die Vorlesung Datenschutzrecht sowie PFAFFINGER, Rechte an Daten, Universität Luzern.

der Telekommunikationsbereich[1409], der Finanzsektor[1410], der arbeitsrechtliche und versicherungsrechtliche Bereich.[1411] Sodann ist festzustellen, dass sich wissenschaftliche Beiträge oft auf spezifische subjektive Rechte konzentrieren, so zum Recht am eigenen Bild oder Wort, aber auch zu Einsichts- und Auskunftsrechten.[1412] Anders als in der Schweiz wird dem allgemeinen Datenschutzrecht, in dessen Zentrum die allgemeine Datenschutzgesetzgebung steht, namentlich in Deutschland wissenschaftlich hohe Bedeutung zugemessen.

1068 Ebenso gilt es, den Stellenwert, der dem DSG vonseiten der *Rechtsprechung* zugemessen wird, präziser zu untersuchen. Insofern interessiert, ob die Behördenpraxis dem Datenschutzrecht und insb. dem DSG Wirksamkeit verleiht. Es geht dabei nicht nur um eine quantitative Frage und damit darum, wie häufig die Einhaltung des DSG behördlich überprüft wird. Es geht auch um einen qualitativen Aspekt mit der Frage nach einer Strukturierungskraft der rechtsanwendenden Behörden für das Regime des DSG in seiner geltenden Fassung. Zudem soll untersucht werden, ob sich in der Judikatur Anstösse finden, welche wissenschaftlich für die Weiterentwicklung des Datenschutzrechts produktiv gemacht werden können.

1069 Anlass für den Untersuchungsgegenstand der datenschutzrechtlichen Rechtsprechung in der Schweiz gibt die Erkenntnis, dass in Deutschland das Bundesverfassungsgericht die Entwicklung des Datenschutzrechts massgeblich geprägt hat. Die Volkszählungsentscheidung des Bundesverfassungsgerichts habe deutlich gemacht, dass mit dem Datenschutzrecht nicht zu spielen sei.[1413] Mit seinem Urteil setzte das Bundesverfassungsgericht nicht nur ein Zeichen, welchen Stellenwert es dem Datenschutzrecht an sich zuweist, wobei es auch ein Grundrecht auf informationelle Selbstbestimmung und damit die individualrechtliche Position stärkte. Zugleich ist in dem Entscheid – wie im Zuge dieser Arbeit gezeigt wurde – eine Sichtweise angelegt, die richtungsweisend für die Gestaltung eines künftigen Datenschutzrechts erscheint: Die Argumentation des Bundesverfassungs-

1409 Bondallaz, La protection des personnes et de leurs données dans les communications, Diss. Fribourg 2007.

1410 Martin, Datenschutz im Bank- und Kreditbereich, Eine Studie zu einem Schweizer Datenschutzgesetz unter Berücksichtigung ausländischer Erfahrungen, insb. In der BRD und in den USA, Diss. Zürich 1987; Schucan, Datenbanken und Persönlichkeitsschutz, Diss. Zürich 1977.

1411 Pärli, Datenaustausch zwischen Arbeitgeber und Versicherung. Probleme der Bearbeitung von Gesundheitsdaten bei der Begründung des privatrechtlichen Arbeitsverhältnisses, Diss. Bern 2003; Kasper, People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, Diss. St. Gallen 2021.

1412 Hierzu z. B. Bächli, *passim*; Glaus, *passim*; Greter, *passim*; vgl. den Fokus auf das subjektive Recht an Information Meyer-Schönberger, in: Schweizer/Burkert/Gasser (Hrsg.), 853 ff., 864 ff.

1413 Simitis, Interview vom 30. September 2009, abrufbar unter: <https://www.datenschutzzentrum.de/artikel/940-Interview-mit-Prof.-Dr.-Dr.h.c.-Spiros-Simitis.html> (zuletzt besucht am 20. September 2021).

gerichts macht die Notwendigkeit, die dynamische wie systemische Dimension im und für den Datenschutz anzuerkennen, zu einem tragenden Element.[1414]

Nachfolgend wird die *schweizerische Rechtsprechung zum DSG* – nicht abschliessend und vollständig – dargestellt, um Entwicklungslinien hinsichtlich seiner Bedeutungsinhalte herauszuarbeiten. Analysiert wird, wie die Schweizer Gerichte der Bedeutsamkeit des Datenschutzrechts Nachachtung verschaffen und wieweit sie konkretisierende Vorgaben entwickeln, um die durch die offene Gesetzgebung verknappte Strukturierungswirkung durch die Praxis zu gewährleisten. Zudem wird reflektiert, inwiefern aus der Behördenpraxis Impulse für die Neugestaltung des Datenschutzrechts gewonnen werden. Die datenschutzrechtliche Judikatur der Schweiz ist quantitativ gering. Datensubjekte lassen datenschutzrechtliche Praktiken kaum je zivilgerichtlich auf ihre Gesetzeskonformität überprüfen.[1415] Diese Tatsache ist gleichzeitig Ausdruck wie Ursache für das datenschutzgesetzliche Vollzugsdefizit. Ein Normensystem, das primär mit Generalklauseln operiert und mit diesen die entscheidende Schranke für die prinzipielle Verarbeitungsfreiheit setzt, ist auf eine konsolidierende Rechtsprechung (und Lehre) dringend angewiesen. Das gewählte Regime wurde, wie gezeigt, namentlich damit legitimiert, dass die Offenheit der Normen angesichts der sich rasant entwickelnden Technologien das richtige Instrumentarium sei, wobei es an der Praxis läge, diese im Fluss stehende Strukturierungswirkung vorzunehmen. Allerdings wurden von der Rechtsprechung nur beschränkt Leitplanken gesetzt. Die datenschutzrechtlich bedeutsamsten gerichtlichen Impulse für das Datenschutzrecht im privaten Bereich gehen von den Entscheidungen aus, die aus der Durchsetzung einer Empfehlung des EDÖB bei sog. Systemfehlern hervorgehen. Wird eine von ihm erlassene Empfehlung ignoriert, kann der EDÖB an das Bundesverwaltungsgericht und in der Folge an das Bundesgericht gelangen. Kaum grundlegende Bedeutung haben zivilgerichtliche Entscheidungen infolge von Klagen wegen Persönlichkeitsverletzungen durch Personendatenverarbeitungen gemäss DSG im privaten Bereich.[1416] Datensubjekte wählen bei mutmasslichen Datenschutzverletzungen – wenn überhaupt – den Weg über die Medien oder den EDÖB. Wie sich die Situation nach Totalrevision entwickelt, ist aktuell offen. 1070

1414 Vgl. BverfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 230; vertiefend zweiter Teil, V. Kapitel, B.4.

1415 Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.10 ff.

1416 Vgl. immerhin BGE 127 III 481 sowie jüngst die Urteile aus dem Banksektor im Zusammenhang mit der Lieferung von Personendaten an ausländische Steuerbehörden, insb. in die USA, z. B. betr. Bankmitarbeiterdaten der Leitentscheid BGE 144 II 29; BGer 4A_73/2017 vom 26. Juli 2017; vertiefend Opel, in: Emmenegger (Hrsg.), 85 ff.; zur Datenlieferung und Steueramtshilfe aus der Sicht der ESTV Hug, in: Emmenegger (Hrsg.), 104 ff.; aufschlussreich mit Blick auf die datenschutzrechtlichen Verantwortlichkeiten von Banken im Verkehr mit ihren Dienstleistern nach DSG und DSGVO in ebendiesem Band auch Vasella/Epprecht, in: Emmenegger (Hrsg.), 127 ff.

2.2. Kernbefunde und Trends in der Rechtsprechung zum DSG

1071 Die folgende Darstellung beginnt mit einem Blick auf die Praxis zum öffentlichen Bereich, wobei der *verfassungsrechtliche Datenschutz* im Rahmen der Drittwirkungslehre sowie der Auslegung der Generalklauseln auch für das Datenschutzrecht im privaten Bereich Relevanz entfalten kann. Allerdings zeigt sich, dass infolge der inkongruenten Rechtsprechung der Inhalt verfassungsrechtlicher Vorgaben im Bereich des Datenschutzes nicht abschliessend geklärt ist.[1417] Es schliesst eine Beschäftigung mit der Rechtsprechung zum DSG im privaten Bereich an im Versuch, Schlaglichter zu setzen, die für das geltende Datenschutzrecht, aber auch für seine Fortentwicklung relevant sein können.[1418] Es geht bei der Vorstellung der Urteile nicht darum, diese einer erschöpfenden Analyse der datenschutzrechtlichen Vorgaben *de lege lata* zuzuführen. Ebenso wenig sollen die Entscheide im Sinne einer Urteilsbesprechung dargestellt werden. Der Fokus liegt vielmehr auf der Frage der Effektuierung, wobei zugleich eine produktive Lektüre darauf ausgerichtet ist, in den Urteilen Indizien für eine paradigmatische Weiterentwicklung des Datenschutzrechts aufzuspüren.

2.2.1. Für den öffentlichen Bereich

1072 Die Rechtsprechung aus dem *öffentlichen Bereich* steht in ihren Anfängen unter den Eindrücken der Fichenaffäre. Kurz vor und rund um den Zeitpunkt des Inkrafttretens des DSG befassten sich mehrere Urteile mit dem (Akten-)*Einsichtsrecht* – herkömmlich aus dem Anspruch auf Wahrung des rechtlichen Gehörs sowie der persönlichen Freiheit abgeleitet –, an welches in der Folge Formulierungen oder Schutzideen einer «informationellen Selbstbestimmung» gekoppelt werden.[1419] Es ist dieses spezifische Betroffenenrecht auf Akteneinsicht, das später mit dem datenschutzgesetzlichen Auskunftsrecht verbürgt wird – weil es dem Subjekt einen aktiven Anspruch einräumt, zu wissen, wer welche Personendaten über es bearbeitet. Ein solcher Anspruch scheint mit einem Recht auf informationelle Selbstbestimmung assoziiert zu werden. Darin, dass für die Schweiz oft unreflektiert ein «Recht auf informationelle Selbstbestimmung», das in seinem Inhalt indes nicht kongruent definiert wird und nur wenig mit dem vom Bun-

1417 Vgl. Belser, in: Epiney/Fasnacht/Blaser, 19 ff.; Fasnacht, N 96 ff.

1418 Eine Rechtsprechungsübersicht über die Jahre 2012 und 2013 findet sich insb. bei Métille, in: Epiney/Fasnacht/Blaser (Hrsg.), 113 ff.

1419 In diese Richtung vgl. BBl 1988 II 414 ff., 453 und 475; vgl. BGE 113 Ia 1, E 4.b.; BGE 112 la 97; BGE 110 la 85; BGE 103 la 492; BGE 100 la 10; in BGE 120 II 118, E 3.a.; wird festgestellt, dass ein Recht auf informationelle Selbstbestimmung von Lehre und Rechtsprechung anerkannt sei, wobei es als Teil des Akteneinsichtsrecht beschrieben wird; vgl. auch Waldmeier, 9; m. w. H. zur Rolle des Akteneinsichtsrechts zur Anerkennung und Entwicklung von Informationsrechten im Kontext des Adoptions- und damit Familienrechts, Pfaffinger, N 126.

desverfassungsgericht geprägten Recht auf informationelle Selbstbestimmung gemein hat, behauptet wird, liegt ein Hauptproblem für die Erfassung und damit Effektuierung sowie Fortentwicklung des schweizerischen Regimes. Die Urteile aus der Schweiz zum öffentlichen Bereich beziehen sich regelmässig auf Register resp. Sammlungen von Personendaten, die klassischerweise der «Geheim- resp. Privatsphäre» zugeordnet werden, und insofern geltend gemachte Auskunftsrechte. Es ging also nicht um irgendwelche Personendaten, in deren Bestände den Beschwerdeführenden Einsicht gewährleistet werden sollte, stattdessen um Daten, die – in Anlehnung an das Konzept der Sphären und der Einteilung von Daten als geheim oder privat – als besonders schützenswert galten.

1073 In *BGer vom 12. Januar 1990, SemJud 112 (1990), 561 ff.* heisst es: «Toute personne doit pouvoir garder la maitrise des informations qui la concernent.» Gleichwohl ist dies nicht das Urteil, das als Grundlage für die Proklamierung eines Rechts auf informationelle Selbstbestimmung dient.

1074 Vielmehr wird bei der Feststellung, wonach die Schweiz «wohl» ein Recht auf informationelle Selbstbestimmung anerkenne, *BGE 113 I 1* aufgegriffen.[1420] Das höchste Schweizer Gericht hatte sich in jenem Entscheid mit der Zulässigkeit eines verweigerten Akteneinsichtsgesuches ausserhalb eines Verfahrens zu befassen. Dem Urteil lag folgender Sachverhalt zugrunde: Ein Mann war in einem Lokal festgenommen worden, das als Treffpunkt für Homosexuelle galt. Ebendort war es zu zahlreichen Diebstählen gekommen. Verhaftet wurde besagter Mann, weil er sich nicht ausweisen konnte. Nachdem seine Identität festgestellt werden konnte und sich in der Folge kein hinreichender Tatverdacht gegen ihn ergab, entliess man ihn. Kurz darauf verlangte der Betroffene Einsicht in ihn erfassende behördliche Registrierungen – ohne Erfolg. Daraufhin beschritt er den Prozessweg. In letzter Instanz beurteilte das Bundesgericht die Ablehnung des Einsichtsgesuches als Verstoss gegen den damals einschlägigen Art. 4 BV und das *rechtliche Gehör.* Der Entscheid selbst stützte sich nicht auf ein «Recht auf informationelle Selbstbestimmung». Stattdessen nahm er Bezug auf den sphärentheoretischen Ansatz. Er wies auf das Unbehagen des Bürgers hin, der seine *Privatsphäre* als beeinträchtigt empfinde, wenn Verwaltungsbehörden Personendaten über längere Zeit hinweg aufbewahren und unter Umständen anderweitige Verwaltungsstellen zu diesen Daten auf unbestimmte Zeit Zugang haben.[1421]

1075 An dieser Stelle zeigt sich eine ähnliche Argumentation, wie sie sich im Volkszählungsurteil des Bundesverfassungsgerichts findet: Als problematisch gilt, wenn in einem bestimmten Verwendungszusammenhang erhobene Personendaten anderen Verarbeitungszwecken und ggf. weiteren Verwaltungsstellen (unbeschränkt)

1420 Breitenmoser/Schweizer, St-GallerKomm.-BV, Art. 13 N 64 und N 72 mit Hinweis auf die ausdrückliche Anerkennung in BGE 120 II 118, E 3.a.

1421 BGE 113 I 1, E 4.b.aa.

zugänglich gemacht werden. Damit scheint auch in einem schweizerischen Entscheid die Perspektive durch, wonach eine Aufgabe des Datenschutzrechts darin liegt, Verarbeitungsbereiche und -zusammenhänge angemessen abzugrenzen. Obschon der Entscheid stark in einer sphärisch angelegten Konzeption angelegt ist, wonach bestimmte Angaben «geheim resp. intim» und damit schutzwürdig seien und in Bezug auf die Homosexualität mögliche Vorurteile mitschwingen, wird in diesem Urteil die Beachtlichkeit der dynamischen wie systemischen Dimension des Datenschutzrechts adressiert und der (potentielle) Fluss von Personendaten aus einem bestimmten Verwendungszusammenhang in einen anderen kritisch beurteilt. Gleichwohl rücken diese Schutzaspekte, ähnlich wie im Volkszählungsurteil, auf welches das Urteil referiert, infolge eines subjektivistischen Fokus eher in den Hintergrund:

> «Gerade der vorliegende Fall zeigt indessen den engen Bezug der Registrierung zum Grundrecht der persönlichen Freiheit: Soweit der Beschwerdeführer aus dem Umstand, dass er an einem Ort kontrolliert worden ist, an dem sich angeblich häufig Homosexuelle aufhalten sollen, allenfalls mit dem Kreis von Homosexuellen in Verbindung gebracht werden sollte, kann der Registereintrag für ihn von nicht geringer Tragweite sein und ihn aus diesem Grunde allenfalls davon abhalten, sich völlig frei zu bewegen. Diesen Gedanken hat denn auch das Bundesverfassungsgericht in seinem sog. Zensus-Urteil angesichts der modernen Datenbearbeitungsmöglichkeiten unterstrichen (BVerfGE 65 Nr. 1 S. 41 ff. E. 1a = EuGRZ 1983 S. 577 ff., insbesondere S. 588).»[1422]

1076 BGE 113 I 1 greift damit auf eine *cause célèbre* des Bundesverfassungsgerichts zurück und weist namentlich auf die Beeinträchtigung der freien Entfaltung des Menschen hin, wenn dieser unsicher sei, wer was von ihm wisse. Allerdings erfolgt die Referenz in jenem Entscheid noch ohne einen expliziten Bezug auf das vom Bundesverfassungsgericht allgemein anerkannte Recht auf informationelle Selbstbestimmung. Soweit sich das Bundesgericht indes auf den Zusammenhang zwischen Selbstbestimmung und Beeinträchtigung der freien Entfaltung aufgrund des ungenügenden Durchblicks über den Wissensstand Dritter über einen selbst bezieht, greift es gleichwohl einen Kerngedanken des Bundesverfassungsgerichts auf. Und: Die Anerkennung eines Rechts auf Akteneinsicht leistete einen Beitrag, dem eigentlich Unheimlichen des Orwellschen Staates, nämlich der Intransparenz staatlicher Macht, zumindest die Spitze zu nehmen.

1077 Anzufügen ist, dass das Bundesgerichtsurteil dem früheren *Mikrozensusurteil*[1423] näher steht als dem späteren Volkszählungsurteil des Bundesverfassungsgerichts: Denn mit der Registrierung der sexuellen Orientierung geht es um eine klassische Kategorie der sog. «besonders schützenswerten Daten». Um den Schutz von Personenangaben mit «Geheimnischarakter» ging es im Mikrozensus-Urteil.[1424]

1422 BGE 113 I 1, E 4.b.aa.
1423 Vgl. BVerfG 27, 1 – Mikrozensus, Urteil vom 16. Juni 1969.
1424 Vgl. BVerfG 27, 1 – Mikrozensus, Urteil vom 16. Juni 1969, E 36.

Anders im Volkszählungsurteil, wo klargestellt wird, dass es «belanglose» Daten nicht gibt.[1425] Erst der Volkszählungsentscheid betont, dass sich der Schutz des Menschen in einer technisierten Datenverarbeitungsumgebung auf *sämtliche Daten* zu erstrecken hat und nicht nur auf Personendaten mit einer bestimmten «Natur». Weil es sich in BGE 113 I 1 um Angaben aus dem sog. Intimbereich handelt und deren Erfassung eine freie Entscheidung und Selbstbestimmung über die Lebensführung beeinträchtigen würde, steht BGE 113 I 1 in der Linie des *Mikrozensus*-Entscheides. Es geht um den Schutz im Zusammenhang mit der Verarbeitung von Personendaten, die traditionell dem qualifizierten Nahbereich der Person, dem Bereich der Intimsphäre zugeordnet werden. Das Mikrozensus-Urteil beschränkte ein Selbstbestimmungsrecht auf Informationen mit «Geheimnischarakter».[1426] Die Ausweitung datenschutzrechtlicher Vorgaben auf «belanglose» Personendaten ist der Paradigmenwechsel, der mit dem Volkszählungsurteil vollzogen wird.[1427] Und genau dieser Aspekt, der in Deutschland als entscheidende Neuerung qualifiziert wird – von den besonders schützenswerten Daten zu sämtlichen Daten –, ist in BGE 113 I 1 *nicht* ausschlaggebend. Immerhin unterscheidet sich BGE 113 Ia 1 (aber auch BGE 113 Ia 257, der sich gleichermassen mit dem Einsichtsrecht in persönliche Akten bei der Kantonspolizei befasste) in einem wichtigen Punkt vom Mikrozensus-Urteil: Im Sachverhalt, der dem Schweizer Urteil zugrunde lag, waren die Personendaten bereits erhoben. Es ging *nicht um die Überprüfung der Zulässigkeit der Datenerhebung*. Vielmehr ging es darum, dass der Bürger *Einsicht in die ihn betreffenden Akten begehrte,* womit es um eine *retrospektive Perspektive* ging. Anders stand in den beiden Entscheiden des Bundesverfassungsgerichts die Erhebung von Angaben (personenbezogenen Daten) der Bürgerinnen und Bürger zur Überprüfung. Die datenschutzrechtlichen Vorgaben setzen mit anderen Worten früher an. Insofern wurde stets die hierfür geschaffene gesetzliche Grundlage in die grundrechtlichen Erwägungen integriert. Im Bundesgerichtsentscheid indessen verfolgten die Ausführungen rund um ein Recht auf *Akteneinsicht* die Notwendigkeit, wonach Bürger wissen sollen können, wer was wann und bei welcher Gelegenheit über einen weiss. In BGE 113 I 1 wurde ein Beleg für die (implizite) bundesgerichtliche Anerkennung eines Rechts auf informationelle Selbstbestimmung gesehen.[1428]

In den Anfängen ist damit ein enger Bezug zwischen dem Recht auf Akteneinsicht und dem Recht auf informationelle Selbstbestimmung auszumachen. Das 1078

1425 Vgl. BVerfGE 65, 1, 154 – Volkszählung, Urteil vom 15. Dezember 1983, E 158.
1426 Buchner, 42.
1427 BVerfGE 65, 1, 154 – Volkszählung, Urteil vom 15. Dezember 1983, E 158; Simitis, Nomos-Komm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 34.
1428 Breitenmoser/Schweizer, St-GallerKomm.-BV, Art. 13 N 64 und N 72.

Akteneinsichtsrecht ist in der Schweiz gut aufbereitet.[1429] Die Anerkennung eines Rechts auf Akteneinsicht kurz vor und um den Zeitpunkt des Inkrafttretens des DSG dient der Lehre als Begründungselement für die Gültigkeit eines Rechts auf informationelle Selbstbestimmung in der Schweiz. Hierzu Schweizer:

> «1994 erwähnte das Bundesgericht der Schweiz das Akteneinsichtsrecht als Teil des Rechts auf informationelle Selbstbestimmung. Die nachgeführte Bundesverfassung der Schweiz enthält mit Artikel 13 ein Grundrecht über den Datenschutz. Die Regelung orientiert sich jedoch stark an Artikel 8 EMRK und spricht von Privatsphäre. Nach dem blossen Wortlaut wäre damit ein Rückschritt gegenüber dem modernen Grundrechtsverständnis begründet, weil damit nur ein Abwehrrecht begründet ist. Das Bundesgericht legte die Regelung jedoch mit konkreter Bezugnahme auf das Recht auf informationelle Selbstbestimmung aus und erhob es somit ebenfalls zum Rechtsgut von Verfassungsrang.»[1430]

1079 Explizit wird das Recht auf informationelle Selbstbestimmung in *BGE 120 II 118, E 3.a.* anerkannt, wobei es als Teil des Akteneinsichtsrechts verortet wird. In diesem Zusammenhang ist auch auf *BGE 122 I 360* einzugehen: Mehrere Zürcher Lehrkräfte hatten Einsicht in die über sie erstellten Datenblätter verlangt, die ihre Beziehungen zum sog. Verein für psychologische Menschenkenntnisse (VPM) dokumentierten. Ebendiese «Fichen» wurden im Personaldossier ab-

1429 Abgestützt wurden Akteneinsichtsrechte vorab auf den grundrechtlichen Anspruch auf Achtung des rechtlichen Gehörs, aber auch die persönliche Freiheit. Bei der Anerkennung des Akteneinsichtsrechts indes geht es um ein «retrospektiv» einsetzendes Kontrollinstrument. Zwar kennt auch das Datenschutzrecht selbst Einsichtsrechte und – wie das Bundesgericht mit Blick auf das damals unlängst in Kraft getretene DSG hinweist – Korrekturrechte. Einsichts- und Korrekturrechte sind mithin früh als Mechanismen zur Umsetzung datenschutzrechtlicher Anliegen anerkannt. Das Datenschutzrecht geht indes deutlich darüber hinaus: Das DSG befasst sich auch mit der Frage der Zulässigkeit der Erhebung von Personendaten an sich und formuliert weitere Vorgaben, die eingehalten werden müssen, damit Datenverarbeitungen (beispielsweise die Speicherung, Weiterleitung, Zusammenfügung, Kategorisierung usf.) zulässig sind. Datenschutzrechtliche Bestimmungen setzen mithin früher an und regeln umfassender. Die Kontrolle durch ein Einsichtsrecht des Subjektes ist lediglich ein «nachgeschaltetes» prozedurales Instrument, das auch dem Datenschutz bekannt ist. Das Datensubjekt soll wissen können, welche Daten über es erhoben wurden und vorliegen; es soll überprüfen können, ob diese korrekt sind. Offensichtlich wird damit eine Facette, ein Element der Idee eines Rechts auf informationelle Selbstbestimmung wiedergegeben. Die Möglichkeit, Einsicht in staatliche Datenbestände, die sich auf die eigene Person beziehen, zu erlangen und diese zu kontrollieren, entschärft die Beunruhigung – zumindest im Ansatz –, die daraus resultiert, nicht wissen zu können, wo welche Behörde welche Angaben über die betroffene Person verarbeitet. Daraus (und aus BGE 133 I 1a 1) auf die Anerkennung eines Rechts auf informationelle Selbstbestimmung zu schlussfolgern, geht allerdings zu weit, wenn man sich den Inhalt dieses Rechts vor Augen führt, wie ihn das Bundesverfassungsgericht geprägt hat. Immerhin kann man im Akteneinsichtsrecht, das ursprünglich aus dem Anspruch auf rechtliches Gehör und der persönlichen Freiheit abgeleitet wurde, einen Ansatzpunkt sehen, um über die Zielrichtung eines Rechts auf informationelle Selbstbestimmung nachzudenken: Es geht um die Milderung der Verunsicherung und die daraus resultierende Beschneidung freien Handelns, wenn man nicht weiss, wer was woher über einen weiss. Ein Recht auf informationelle Selbstbestimmung, das an seinen Anfang ein grundsätzliches Datenverarbeitungsverbot stellt, unterscheidet sich indes grundlegend von einem Akteneinsichtsrecht, das sich auf bereits erhobene Datenbestände bezieht, wobei über die Erhebungsbedingungen nichts weiter gesagt wird; zum «droit d'accès» bereits Steinauer, in: Universités de Berne, Fribourg, Genève, Lausanne et Neuchâtel (Hrsg.), 79 ff.

1430 Vgl. Schweizer, 55 ff.

gelegt. Den Lehrerinnen und Lehrern wurde zwar Einsicht in besagte Dokumente gewährt. Allerdings waren Quellen und Korrespondenzen, die Informationen im Zusammenhang mit dem Verein betrafen, teilweise abgedeckt. Die Beschwerden richteten sich gegen die Ablage entsprechender Angaben und Korrespondenzen der jeweiligen Lehrpersonen mit Blick auf den genannten Verein. Die Lehrpersonen vertraten die Ansicht, dass das Sammeln, Aufbewahren und Bearbeiten von Informationen über ihre Zugehörigkeit zum VPM ihre persönliche Freiheit sowie den Anspruch auf Achtung des Privat- und Familienlebens nach Art. 8 EMRK, die Vereinsfreiheit sowie weitere verfassungsmässige Rechte verletze. Deshalb müssten diese Daten aus ihren Personalakten entfernt werden. Das Bundesgericht knüpfte seine Erwägungen an das ungeschriebene Grundrecht auf persönliche Freiheit an, welches ebenso den Anspruch auf Schutz der persönlichen Geheimsphäre beinhalte.[1431] Einschränkungen seien zulässig unter Einhaltung der allgemeinen Voraussetzungen für Grundrechtseinschränkungen (insb. einer gesetzlichen Grundlage). Hierbei verwies das Bundesgericht auf Art. 17 Abs. 1 DSG: Das Bundesgericht interpretierte in Einklang mit der Auffassung des Bundesrates gemäss Botschaft die Anforderungen an die gesetzliche Grundlage äusserst grosszügig: Gefordert wurde nicht eine rechtliche Spezialermächtigung, die sich spezifisch auf die Datenbearbeitung beziehen muss. Vielmehr solle die Bearbeitung von Daten zulässig sein, wenn sie für die Erfüllung einer gesetzlichen Aufgabe erforderlich sei.[1432] Eine solche Interpretation – für die bis heute eingetreten wird[1433] – führt zu einer *Absenkung* des Datenschutzniveaus im öffentlichen Bereich des Bundes. Sie verwässert die Vorgabe einer klaren, spezifischen gesetzlichen Vorgabe, wonach Personendatenverarbeitungen im öffentlichen Sektor einer spezifischen gesetzlichen Grundlage bedürfen. Eröffnet werden weite Interpretationsräume, womit nahezu jede Personendatenverarbeitung, wenn im Kontext mit der Erfüllung einer öffentlichen Aufgabe stehend, als zulässig begründbar wird. An die Stelle des Gesetzgebers, der die Zulässigkeit der Personendatenverarbeitung im Lichte der konkretisierten öffentlichen Aufgabe und mit Blick auf die hier mit einer öffentlichen Funktion betrauten Personen resp. Stellen definiert, tritt die Interpretation der rechtsanwendenden Behörden, basierend auf der von ihnen angenommenen Interessen an der Verarbeitung. In besagtem Entscheid kommt das Bundesgericht im Ergebnis immerhin zu dem Schluss, dass die Sammlung der Angaben zu Vereinszugehörigkeiten nicht von einer hinreichenden gesetzlichen Grundlage getragen würde.[1434]

1431 BGE 122 I 360, E 5.a.
1432 Vgl. auch BBl 1988 II 414 ff., 467; BGE 122 I 360, E 5.b.bb.
1433 Vgl. Ballenegger, BSK-DSG, Art. 17 N 18.
1434 BGE 122 I 360, E 5.

1080 Bezüglich der Auslotung des Schutzes eines privaten Lebensbereiches von Personen, die öffentliche Funktionen wahrnehmen, ist *BGE 124 I 85* bemerkenswert.[1435] Es ging um eine Regelung des Kantons Basel-Stadt, welche die Identifizierung der Polizeibeamten normierte. An erster Stelle wurde die Uniform als Identifikationsmittel genannt: Jeder, der uniformiert sei, habe grundsätzlich auch ein Namensschild (Nachnamen) zu tragen. Gegen die geplante kantonale Gesetzesbestimmung wurde staatsrechtliche Beschwerde vom Polizeibeamtenverband eingereicht. Beklagt wurde namentlich eine Verletzung von Art. 8 EMRK. Das Bundesgericht ging zudem auf das ungeschriebene Grundrecht der persönlichen Freiheit ein.[1436] Es bestätigte seine bisherige Rechtsprechung zum ungeschriebenen Grundrecht auf persönliche Freiheit, wonach nicht jeder beliebige Eingriff eine Berufung auf die persönliche Freiheit rechtfertige. Die persönliche Freiheit schütze nicht vor jeglichem physischen oder psychischen Unbehagen. Das Bundesgericht bestätigte, dass zur persönlichen Freiheit «ein Anspruch auf Geheim- und Intimsphäre» gehöre. Der Name sei Teil dieser Privatsphäre (!). Ob und unter welchen Umständen der Name einem Dritten preisgegeben werde, liege im Ermessen des Einzelnen. Eine staatliche Verpflichtung zur öffentlichen Bekanntgabe des Namens greife in den Schutzbereich der persönlichen Freiheit ein. Der Name wurde in diesem Entscheid (absurderweise) als Personenangabe qualifiziert, die der *Geheim- oder Privatsphäre* angehöre. Diese Qualifikation erstaunt, gilt doch der Name gemeinhin als belanglose Personenangabe. Um die bundesgerichtliche Qualifizierung nachvollziehen zu können, ist diese zu kontextualisieren. Auf der Seite der einzelnen Polizistin steht wohl die Angst, infolge der Kenntnisnahme des zivilen Namens durch eine Bürgerin, mit der man eine «Begegnung» hatte, identifiziert und später beispielsweise aufgesucht zu werden. Insofern geht es um den Schutz der Polizeibeamten vor allfälligen «Retorsionen» vonseiten der Bürgerinnen und Bürger. Allerdings erfüllt die Angabe des Namens auf der Uniform im Polizeikontext eine wichtige Aufgabe. Sie wird mit der Qualifizierung des Namens als «geheim» und mit einem Recht auf Selbstbestimmung übersehen. Das Namensschild ermöglicht den mit Beamten konfrontierten Bürgern deren Identifizierung, womit ein *Kontrollmechanismus* gegenüber dem agierenden Beamten, aber auch der Polizei als staatlicher Institution an sich eingeführt wird. Der Polizist, der durch ein Namensschild ausgewiesen wird, tritt den Bürgerinnen nicht als anonyme Person entgegen. Das anonyme Handeln ist angsteinflössend. Mit

1435 Mit Hinweis auf BGE 124 I 85 wird die Praxis des Tragens eines Namensschildes zwecks Deeskalation des angespannten Verhältnisses zwischen Privatpersonen und Personen, die im Einsatz für private Sicherheitsdienstleister stehen, vorgeschlagen von Schuppli, Sicherheit & Recht 2019, 49 ff., 61; kritisch zur Namensschildpflicht in Anbetracht der «zunehmenden Gewalt» gegen Polizistinnen und Polizisten Tiefenthal, in: Tiefenthal (Hrsg.), Art. 21 N 10; vgl. auch OGer ZH, Beschluss und Urteil vom 19. März 2015, LF140077, E 3.8.; zum Thema Datenschutz und Polizei Oberholzer, in: Brem/Druey/Kramer/Schwander (Hrsg.), 427 ff.

1436 BGE 124 I 85, E 2.a. und b.

dem Namensschild wird der eine öffentliche Funktion wahrnehmende Beamte identifizierbar. Gleichzeitig wird sein Handeln überprüfbar, was eine *Abkehr von der anonymen Polizeigewalt* darstellt. Verhält sich eine Polizistin nicht korrekt, kann die betroffene Bürgerin dies infolge Kenntnis des Namens melden. Im Ergebnis wird die Verantwortlichkeit des polizeilichen Handelns, aber auch das *Vertrauen in die Polizei als Institution* gewährleistet. Der Name an der Uniform trägt dazu bei, die *Integrität polizeilichen Handelns zu gewährleisten*. Die Identifizierungspraxis ist eine Massnahme, mit der das korrekte polizeiliche Verhalten abgesichert wird. Polizeiliche resp. staatliche Gewalt wird damit begrenzt.

Aus einer solchen funktionellen und kontextuellen Perspektive betrachtet muss 1081
der Entscheid, der den Namen abstrakt als «geheim» taxiert und den Willen des Beamten – seine Selbstbestimmung – in den Vordergrund rückt, als *Fehlentscheid* bezeichnet werden. Das Urteil ist ein guter Beleg dafür, dass die isolierte Fokussierung auf die Natur einer bestimmten Personenangabe oder auf ein subjektives Recht der Selbstbestimmung zur Bewältigung von Herausforderungen unter dem Titel des Datenschutzes zu kurz greift. So falsch es ist, den Namen per se als geheim zu qualifizieren, so falsch ist die heute vorherrschende umgekehrte Ansicht, wonach der Name als nicht schutzwürdig und entsprechend als allgemein sowie beliebig verarbeitbar beschrieben wird. Entscheidend ist stets der *Verarbeitungskontext*. Ebendies hat Simitis für den Namen wie folgt illustriert: Wenn es darum geht, dass der Name als Identifikator einer bestimmten Person an die Mafia gegeben wird, welche diese auf der Blacklist führt, handelt es sich um keine «harmlose, belanglose» Personenangabe. Wenn der Name dagegen dazu erfragt wird, um eine online bestellte Ware zuzustellen, kommt dem Namen eine gänzlich andere Bedeutung zu. Anders gewendet: Derselbe Name ist nicht derselbe Name. Er hat zwar die gleichen Lettern, aber keineswegs immer dieselbe Bedeutung aus datenschutzrechtlicher Perspektive.

Einmal mehr erhärtet sich die Relevanz des *Kontextes* für die Lösung daten- 1082
schutzrechtlicher Herausforderungen. Wie aber könnte der in diesem Sachverhalt beschriebene Konflikt aus der Perspektive des Datenschutzes angemessen adressiert werden? Ein Lösungsvorschlag, welcher den kontextuellen Herausforderungen Rechnung tragen könnte, wäre in der Pseudonymisierung zu sehen. Polizeibeamte würden nicht ihren «Zivilnamen» auf dem Namensschild tragen, stattdessen ein Pseudonym oder eine Nummer. Die konkrete Polizistin würde dann vom Bürger nicht mit Zivilnamen identifiziert werden. Sie hätten auch keine «Angriffe» in ihrem privaten Lebensbereich zu fürchten. Eine Identifizierung der Beamten durch die zuständigen Stellen wäre dennoch möglich. Eine solche Lösung überzeugt dennoch nicht: Zunächst würden die Polizistinnen und Polizisten für die Bürgerinnen und Bürger weiterhin anonym bleiben. Zudem haben die persönlichkeitsrechtlichen Schutzinteressen von Personen mit einer entsprechen-

den öffentlichen Funktion als geringer beurteilt zu werden. Es ist das öffentliche Amt, das einen Eingriff resp. eine Einschränkung der Privatheitsinteressen legitimiert. Lösungen, die ein «Vorentscheidungsrecht» im Sinne eines Rechts auf informationelle Selbstbestimmung etablieren, wie auch die Pseudonymisierungslösung dürften als Pervertierung des Datenschutzes gewertet werden.[1437]

1083 *BGE 128 II 259* befasst sich *spezifisch mit Art. 13 Abs. 2 BV*. Ein Beamter hatte im Rahmen einer Einvernahme einen Wangenabstrich abgenommen, und zwar auf Anordnung des zuständigen Oberkommissionärs hin. Eine Verfügung des Staatsanwaltes lag der Massnahme nicht zugrunde. Letzterer wies die vom Betroffenen beantragte Vernichtung des Wangenabstriches ab und ordnete die Erstellung eines DNA-Profils sowie den Abgleich mit dem DNA-Profil-Informationssystem an. Der Beschwerdeführer verlangte in der Folge mit staatsrechtlicher Beschwerde die Vernichtung und Entfernung von DNA-Angaben, wobei er eine Verletzung von Art. 10 Abs. 2 und Art. 13 Abs. 2 BV rügte. Das Bundesgericht hielt zu Art. 13 Abs. 2 BV fest:

> «Art. 13 Abs. 2 BV schützt den Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen (informationelle Selbstbestimmung).»[1438]

1084 Weil die Erstellung eines DNA-Profils eine nahezu hundertprozentige Sicherheit bei der Identifizierung einer Person liefere, sei das Recht auf informationelle Selbstbestimmung betroffen. Allerdings vermeidet es der Entscheid, eine konkretisierende Strukturierung eines Rechts auf informationelle Selbstbestimmung zu formulieren.

1085 Aufschlussreich mit Blick auf den Schutzzweck des Datenschutzrechts und die in dieser Untersuchung formulierte These der systemischen Relevanz ist *BGE 129 I 232* Im Entscheid aus dem Jahre 2003 ging es um die Erhebung von Daten im Rahmen des *Einbürgerungsverfahrens*. Die SVP Zürich hatte eine Volksinitiative mit dem Titel «Einbürgerungen vor das Volk» lanciert. Der Gemeinderat erklärte die Initiative für ungültig. Dem Bundesgericht wurde die Angelegenheit per Stimmrechtsbeschwerde, nachdem der kantonale Instanzenzug ausgeschöpft war, zur Entscheidung vorgelegt. Es hatte zu prüfen, ob die geplante Einführung eines Urnenentscheides über Einbürgerungsgesuche die Bundesverfassung verletze. Um diese Frage zu beurteilen, setzte sich das Bundesgericht vorab mit der Begründungspflicht entsprechender Entscheidungen unter dem grundrechtlich geschützten Anspruch auf rechtliches Gehör auseinander sowie mit dem Diskriminie-

1437 In unzähligen weiteren Konstellationen, auch im privaten Bereich, wird der Name zur Überprüfung des Verhaltens eingefordert, beispielsweise im Rahmen einer schlechten Beratung in einem Geschäft. Auch hier ist es gängig, diesen zu nennen. Das Argument der gefürchteten Retorsion und damit des Privatheitsschutzes würde auch hier kaum allgemein als überzeugend angesehen werden.

1438 BGE 128 II 259, E 3.2.

rungsverbot. Sodann kam es in seinen Erwägungen zum Erhebungsprozess von Personendaten über die Gesuchsteller, deren Eignung geprüft werden sollte.[1439] Hier verortete das Bundesgericht einen Konflikt mit dem verfassungsmässigen Recht der Bewerberinnen und Bewerber auf Schutz ihrer Privatsphäre und auf Geheimhaltung ihrer persönlichen Daten unter Zitierung der Worte von Schweizer, wonach die einzelne Person selbst bestimmen können solle, ob und zu welchem Zweck Informationen über sie bearbeitet werden. Das Bundesgericht stellte fest, dass im Einbürgerungsverfahren der zuständigen Behörde detaillierte Angaben über Herkunft, Einkommen, Vermögen, Ausbildung, Tätigkeit, Sprachkenntnisse, Familienverhältnisse, Freizeitgestaltung, Leumund usw. gegeben würden, wobei es teilweise um besonders schutzwürdige Daten ginge. In ihrer Gesamtheit würden sich die Daten zu einem Persönlichkeitsprofil zusammenfügen, womit die Bearbeitung der genannten Daten einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung darstellen würden. Die Vorgaben von Art. 36 BV haben insofern eingehalten zu werden. Der Bewerber, der ein Gesuch zur Einbürgerung stelle und die nötigen Auskünfte liefere, willige zugleich ein, dass seine Daten den Mitgliedern der zuständigen Behörde zugänglich gemacht würden. Würden dagegen, wie es das Initiativbegehren verlange, die in Zürich Stimmberechtigten an der Urne über das Einbürgerungsgesuch entscheiden, so müssten schützenswerte Daten der Bewerber zehntausendfach vervielfältigt und an alle stimmberechtigten Bürgerinnen und Bürger der Stadt verteilt werden. Dies wäre ein *unverhältnismässiger Eingriff in die Privat- und Geheimsphäre der einbürgerungswilligen Personen*. Entsprechend qualifizierte das Bundesgericht die detaillierten und umfassenden Datensammlungen und deren Weitergabe an die zur Beurteilung der Einbürgerung designierten Personen inklusive sensibler Angaben, mithin die Erhebung von Persönlichkeitsprofilen, als *schweren Eingriff in das Recht auf informationelle Selbstbestimmung*, um zugleich mit den folgenden Ausführungen Unklarheit zu schaffen:

> «Art. 13 BV gewährleistet das Recht auf eine Privat- und eine persönliche Geheimsphäre. Abs. 2 schützt den Einzelnen vor Beeinträchtigungen, die durch die staatliche Bearbeitung seiner persönlichen Daten entstehen […]. Die einzelne Person soll selbst bestimmen können, ob und zu welchem Zwecke Informationen über sie bearbeitet werden […].»[1440]

Das Bundesgericht effektuiert mit diesem Urteil das Datenschutzrecht weniger mit seiner verwirrlichen Referenz auf verschiedene Konzeptionen, was den Grundrechtsschutz anbelangt. Es tut dies vielmehr, indem es ein massenweiser Datenfluss umfassender persönlicher Angaben von einer Person zu den Bürgerinnen und Bürgern verbietet, die der das Einbürgerungsgesuch stellenden Person zugleich in weiteren Rollen begegnen. Das Urteil grenzt damit verschiedene ge- 1086

1439 BGE 129 I 232, E 4.2.2. und E 4.3.
1440 BGE 129 I 232, E 4.3.2.

sellschaftliche Bereiche voneinander ab und problematisiert dazwischen stattfindende Datenflüsse. Damit geht von diesem Entscheid ein Anstoss aus, für das Datenschutzrecht eine neue Sichtweise zu entwickeln, die über die subjektivrechtliche Fokussierung hinausgeht.

1087 Es folgen mehrere Entscheide, die sich detaillierter auf das Recht auf informationelle Selbstbestimmung beziehen. Bevor kursorisch auf diese einzugehen ist, ein interessantes Diktum der damals amtierenden Eidgenössischen Datenschutzkommission:

> «Dem Kerngehalt dieses Grundrechts nach muss die einzelne Person gegenüber fremden staatlichen oder privaten Bearbeitungen von sie betreffenden Informationen letztlich bestimmen können, ob und zu welchem Zweck diese Informationen über sie bearbeitet werden. Nur wenn der einzelnen Person das Recht auf Einwilligung oder Widerspruch gegenüber staatlichen Stellen und privaten Interessenten zuerkannt wird, kann sie sich gegen mittelbare oder unmittelbare Beeinträchtigungen durch Informationstätigkeiten wehren. Müsste sie hingegen das Erforschen von Konsumgewohnheiten, eine Kreditauskunft, eine geheime Sicherheitsprüfung als „Missbrauch von persönlichen Daten" nachweisen, könnte sie sich nur in Ausnahmefällen gegen staatliche und private Informationstätigkeiten wehren.»[1441]

1088 Schweizer/Rechsteiner weisen auf diese Erwägungen mit den knappen Worten hin: «Dem ist u. E. nichts zuzufügen».[1442] Anders BGE 133 I 77, wonach die Aufbewahrung von Videoüberwachungsaufnahmen von öffentlichen Plätzen während mehr als 100 Tagen einen schwerwiegenden Eingriff in das in Art. 13 Abs. 2 BV geschützte informationelle Selbstbestimmungsrecht darstelle, da es die Gefahr einer missbräuchlichen Verwendung der Videoaufzeichnungen erhöhe.[1443]

1089 In zweierlei Hinsicht aufschlussreich ist BGer 6B_4/2011 vom 28. November 2011. Zum einen, weil er Versäumnisse beim Namen nennt, was die Klärung des grundrechtlichen Schutzobjektes anbelangt, und zum anderen, weil es in dem betreffenden Sachverhalt offensichtlich um eine Kollision zwischen zwei verschiedenen Kontexten ging.[1444] Ein Mörder (X) unterzog sich aufgrund eines «Behandlungsvertrages» mit dem Psychiatrisch-Psychologischen Dienst (PPD) des Amts für Justizvollzug des Kantons Zürich einer Therapie. Ziel der Behandlung war die Minimierung resp. Eliminierung der Rückfallgefahr. Der «Vertrag» sah differenzierte Informations- und Auskunftsrechte gegenüber den Justizbehörden vor. So sollten die Therapeuten regelmässig oder auf Anfrage über die Behandlung

1441 VPB 69 (2005) Nr. 106, E 2.3.
1442 Schweizer/Rechsteiner, in: Passadelis/Rosenthal/Thür (Hrsg.), § 2 N 2.3.
1443 BGE 133 I 77, E 5.3.; zur präventiv-polizeilichen Videoüberwachung des öffentlichen Raums mit Blick auf die Funktionsweisen der Technologie, zu erfüllenden Zwecke sowie zu Vorgaben gemäss deutschem und US-amerikanischem Verfassungsrecht grundlegend Bartsch, 17 ff.; zur Videoüberwachung in öffentlichen Räumen auch Weydner-Volkmann/Feiten, digma 2019, 218 ff.; vgl. auch Rudin, digma 2007, 34 ff.
1444 Richtungsweisend für den kontextuellen Ansatz sind die Arbeiten von Nissenbaum; vertiefend hierzu auch dritter Teil, IX. Kapitel.

berichten, wobei der Täter Einsicht in die erstellten Berichte erhalten sollte. Die Justizbehörden wurden damit nicht nur über die Einhaltungen der Sitzungen informiert, sondern auch über sich abzeichnende Gefährdungssituationen. Zum Kernpunkt des Konfliktes wurde, dass der PPD einen ihm zugänglich gemachten Therapiebericht der Abteilung Straf- und Massnahmenvollzug des Kantons Bern vorlegte. X kündigte daraufhin den Behandlungsvertrag und machte geltend, dass die Weitergabe des Berichtes ohne seine Einwilligung unzulässig gewesen sei. X rügte, dass die Voraussetzungen für einen Eingriff in sein Grundrecht auf informationelle Selbstbestimmung im Sinne von Art. 13 Abs. 2 BV nicht erfüllt gewesen seien. Nach Ausschöpfung des kantonalen Instanzenzuges befasste sich das Bundesgericht mit der Angelegenheit. Es zitierte hierbei zunächst wörtlich einen Satz, wie ihn das Bundesverfassungsgericht im Rahmen seiner ausführlichen Erwägungen zu einem Recht auf informationelle Selbstbestimmung formuliert hatte, und äusserte sich zur Tragweite des Importes des Begriffes in die Schweiz. Hierzu lauten die rechtlichen Erwägungen des höchsten Schweizer Gerichts:

> «Das vom deutschen Bundesverfassungsgericht im Jahre 1983 in seinem „Volkszählungsurteil" begründete Grundrecht auf informationelle Selbstbestimmung „gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".»[1445]

Sogleich allerdings verweist es auf die im Volkszählungsurteil definierten Schran- 1090
ken des Rechts:

> «Jedoch besitzt der Einzelne nach diesem Entscheid nicht eine absolute Herrschaft über seine Daten, sondern muss Einschränkungen im überwiegenden Allgemeininteresse hinnehmen.»[1446]

In der Folge räumt das Bundesgericht erstmals unter Referenz auf den Beitrag 1091
von Belser die *unsachgemässe Verwendung* «des Rechts auf informationelle Selbstbestimmung» ein, indem es festhält:

> «Rechtsprechung (vgl. BGE 128 II 259 E. 3.2 S. 268; 129 I 232 E. 4.3.1 S. 245) und Lehre verwenden den Begriff der informationellen Selbstbestimmung im untechnischen, beschreibenden Sinne, interpretieren das Schweizerische Recht aber teilweise auch nach dieser Konzeption kritisch.»[1447]

Das Bundesgericht führte alsdann die grundrechtliche Diskussion für die Schweiz 1092
wieder auf ihre Grundlagen zurück. Unter Bezug auf Biaggini weist es folglich hin:

> «Gemäss Art. 13 Abs. 2 BV hat jede Person Anspruch auf Schutz vor Missbräuchen ihrer persönlichen Daten. Diese Verfassungsbestimmung begründet in erster Linie Abwehran-

1445 BGer 6B_4/2011 vom 28. November 2011, E 2.3.
1446 BGer 6B_4/2011 vom 28. November 2011, E 2.3.
1447 BGer 6B_4/2011 vom 28. November 2011, E 2.3.

sprüche, teils auch Ansprüche auf staatliches Tätigwerden und darüber hinaus Schutzpflichten, die in erster Linie den Gesetzgeber ansprechen.»[1448]

1093 Hat das Bundesgericht bis hierhin einen Beitrag zur Klärung der bislang diffusen Beschreibung auch der datenschutzrechtlichen Grundrechtssituation geleistet, präzisiert es die Rechtslage weiter mit dem Passus:

> «Entgegen dem zu eng geratenen Wortlaut (BIAGGINI, a. a. O., N 11) schützt Art. 13 Abs. 2 BV nicht nur vor dem Missbrauch persönlicher Daten, sondern erfasst grundsätzlich jede staatliche Bearbeitung solcher Daten. Ein Grundrechtseingriff unterliegt den Voraussetzungen von Art. 36 BV.»[1449]

1094 Der Entscheid liefert Klärung dergestalt, dass er die bisher ungenügende Konsolidierung des Grundrechts gemäss Art. 13 Abs. 2 BV problematisiert. Der Sachverhalt führt darüber hinaus die ganze Komplexität der Regulierung von Datenflüssen zwischen verschiedenen Kontexten vor Augen: Der Erfolg des Therapieverhältnisses hängt massgeblich davon ab, dass sich die in Therapie befindliche Person auf die Vertraulichkeit des in diesem Rahmen Geäusserten verlassen kann.[1450] Muss sie davon ausgehen, dass im Therapiekontext offenbarte Informationen weitergereicht werden, kann der Therapieerfolg torpediert werden. Die zu therapierende Person wird unter Kenntnis des Umstandes, dass Therapiegespräche den Behörden des Strafvollzuges eröffnet werden, allenfalls bewusst Informationen zurückbehalten, die für die korrekte Einschätzung der von der Person ausgehenden Gefahren sowie für die erfolgreiche Therapierung entscheidend wären. Ein Informationstransfer kann dann gleichzeitig Ziele des Therapiekontextes wie des Strafvollzuges untergraben. Umgekehrt besteht ein Informationsinteresse vonseiten der strafvollziehenden Behörden, wobei entsprechende Informationen zur Einschätzung der Rückfallgefahr resp. der Therapiefortschritte unverzichtbar sind, auch um die öffentliche Sicherheit zu gewährleisten. Dieses systemische Dilemma lässt sich allerdings nicht durch individualrechtliche Dispositionsbefugnisse lösen. Vielmehr bedarf es einer Analyse der Auswirkungen von verschiedenen Gestaltungsformen von Personendatenflüssen zwischen den beschriebenen Kontexten. Im Ergebnis sollte es der Gesetzgeber sein, der nach einer entsprechenden Analyse einen Prozess definiert, welcher die bestmögliche Lösung zur Wahrung der Ziele *beider Kontexte* zu gewährleisten vermag. Eine individualrechtliche Fokussierung auf ein – wie auch immer definiertes – Recht auf informationelle Selbstbestimmung vermag dieser (komplexen) Herausforderung nicht gerecht zu werden.

1448 BGer 6B_4/2011 vom 28. November 2011, E 2.4.; m. w. H. zur formulation maladroite Meyer, in: Kahil-Wolff/Sinomin (Hrsg.), 87 ff., 89.

1449 BGer 6B_4/2011 vom 28. November 2011, E 2.4.

1450 Vgl. zu diesem Kontext vertiefend Nissenbaum, 174 f.; zur Vertraulichkeit auch in diesem Kontext vgl. Harvey, U. Pa. L. Rev. 1992, 2385 ff.

Chronologisch betrachtet folgen mehrere Entscheide mit dem Konnex zwischen strafrechtlichen resp. administrativen Untersuchungen, auf deren Darstellung an dieser Stelle verzichtet wird.[1451] 1095

Zusammenfassend lässt sich festhalten, dass entgegen dem klaren Wortlaut von Art. 13 Abs. 2 BV die grundrechtliche Situation nicht geklärt ist. Die Rechtsfiguren «Privatsphärenschutz», «informationelle Selbstbestimmung», «Missbrauchsverhinderung im Rahmen der Datenverarbeitung» kommen nahezu beliebig zum Einsatz. Fest steht, dass sich der grundrechtliche Schutz im Kontext von Datenverarbeitungen – laut Rechtsprechung – nicht auf sog. «sensible Daten» beschränken kann. Es ist diese Ausweitung des Schutzes des Menschen vor Bearbeitungen von «gewöhnlichen Daten», die unter den Schutz der informationellen Selbstbestimmung gestellt wird. Die bundesverwaltungsgerichtliche sowie bundesgerichtliche Rechtsprechung schafft im Lichte des Verfassungstextes, des ausführenden Datenschutzgesetzes sowie der gesetzgeberischen Materialien keine 1096

1451 Vgl. insofern namentlich 138 I 256 – Ein zunächst Tatverdächtiger verlangte die Löschung der im Zusammenhang mit ihm und einem Delikt gesammelten Polizeiinformationen, nachdem die gegen ihn eingeleitete Strafuntersuchung rechtsgültig eingestellt worden war. E 5.5. lautet kurz und bündig: «Gestützt auf das informationelle Selbstbestimmungsrecht (Art. 13 Abs. 2 BV, Art. 8 Ziff. 1 EMRK) kann sich die betroffene Person zur Wehr setzen, dass ihre Personendaten ohne ersichtlichen Grund auf lange Zeit in einem öffentlichen Register gespeichert werden. Wann dies im Einzelnen zutrifft, hängt in Anbetracht der unbestimmt umschriebenen Grundlage im Wesentlichen von den konkreten Umständen und im Sinne einer umfassenden Interessenabwägung von der Schwere des Grundrechtseingriffs ab.» Das Bundesgericht beurteilte im vorliegenden Fall, da das Delikt noch nicht aufgeklärt war, das öffentliche Interesse an der Aufbewahrung der Angaben gegenüber dem privaten Löschungsinteresse als überwiegend; BVGer A-8073/2015 vom 13. Juli 2016 befasst sich mit der Zulässigkeit einer Publikation von Ergebnissen einer Administrativuntersuchung und entsprechend mit dem Öffentlichkeitsgesetz, das den Zugang zu amtlichen Dokumenten reguliert. Der EDÖB war in seiner Schlichtungsfunktion im Einsatz, wobei es neben der Publikation der Ergebnisse der Administrativuntersuchung namentlich auch um diejenige der Anonymisierung der «einschlägigen» Personen ging. In E 6.1.3. wendet sich das Bundesverwaltungsgericht der Interessenabwägung zu, indem es auf die Relevanz der gesamten Umstände des Einzelfalles hinweist, i. c. relevant war namentlich die Position der betreffenden Personen in der Verwaltung. Das Bundesverwaltungsgericht weist darauf hin, dass ein «Recht auf informationelle Selbstbestimmung» für (höhere) Angestellte der Bundesverwaltung eine andere Bedeutung habe als für Privatpersonen; BGE 143 IV 21 – ein Entscheid aus dem strafrechtlichen Kontext. Es ging um Editionspflichten gemäss Art. 265, 269 ff. StPO und, die Lücke betreffend, Anbietende von abgeleiteten Internetdiensten wie den sozialen Netzwerken und namentlich Facebook im damaligen eidgenössischen Fernmeldegesetz; BGer 1B_26/2016 – Urteil i. S. Ritzmann/Mörgeli. Das Bundesverwaltungsgericht bestätigt das Beweisverwertungsverbot im Verfahren gegen Prof. Ritzmann infolge einer Verletzung von StPO 196 f., weil die massenweise Erhebung von E-Mails und Telefonangaben aufgrund eines fehlenden hinreichenden Tatverdachtes nicht gegeben war. Die Erhebung wurde als unverhältnismässig beurteilt und entsprechend als Verletzung der Grundrechte der betroffenen Personen; BGE 140 I 2 – in Frage stand nochmals das interkantonale «Hooligan-Konkordat». Zur Erinnerung: Im Jahr 2007 schlossen die Kantone ein Konkordat über Massnahmen gegen Gewalt anlässlich von Sportveranstaltungen, welches später revidiert wurde. Gegen gewisse Änderungen des Konkordates ging Beschwerde beim Bundesgericht ein. Unter anderem befasste es sich hierbei mit einem Informationssystem mit dem sinnigen Titel HOOGAN; aufgrund des Konkordats sollte vor dem Zutritt in ein Stadium das Vorlegen eines Identitätsausweises verlangt werden und nach einer Abgleichung mit dem System ggf. der Zutritt verweigert werden können. Die Beschwerdeführer sahen darin, neben einer Verletzung der Bewegungsfreiheit, einen Verstoss gegen das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung (Art. 10 Abs. 2 i. V. m. Art. 13 Abs. 2 BV).

Klarheit, sondern vielmehr Orientierungslosigkeit. Zwar wird die Beachtung eines Rechts auf informationelle Selbstbestimmung behauptet. Allerdings werden weder Inhalt noch konkretisierende Vorgaben für dessen Verwirklichung in kongruenter Weise formuliert. Somit muss anhand dieses kursorischen Blickes auf die Rechtsprechung für den öffentlichen Bereich festgehalten werden, dass der Materie auch von der Rechtsprechung keine besondere Aufmerksamkeit und Sorgfalt zugemessen und entsprechend wenig strukturierende Wirkung durch die Rechtsprechung für das Datenschutzrecht generiert wird. Im Rahmen der Vorgaben für die zulässige Einschränkung der Grundrechte stellt – theoretisch – die Forderung einer hinreichenden gesetzlichen Grundlage zur Datenverarbeitung ein wirksames Instrument zur Gestaltung und Kontrolle von Personendatenverarbeitungsprozessen dar. Allerdings hat auch insofern die Rechtsprechung keinen Beitrag geleistet, der Notwendigkeit einer spezifischen gesetzlichen Grundlage für die Personendatenverarbeitung Nachdruck zu verleihen. Regelmässig münden sodann die Entscheidungen in eine Interessenabwägung für den konkreten Einzelfall.[1452]

1097 Die vom Gesetzgeber mit der offenen Gesetzgebung avisierte Konkretisierung auch durch die Gerichte fehlt über weite Strecken. Grundsätzliche oder gar richtungsweisende Vorgaben, die dem verfassungsrechtlichen Datenschutz (und den Fragen nach dessen Auswirkungen auf das Privatrecht) Griffigkeit und Gewicht verleihen würden, finden sich selten.

1098 Was immerhin mit diesem Schlaglicht auf den verfassungsrechtlichen Datenschutz sichtbar wurde, ist, dass dieser jeweils in spezifischen Kontexten besondere Bedeutung hat – im Strafverfolgungs- und Strafvollzugskontext, im Migrationskontext, aber auch im Steuerkontext sowie Sozialversicherungskontext. Hierbei zeigt sich, dass allem voran Flüsse von Personendaten zwischen verschiedenen Bereichen als eigentliche Kollisionen erscheinen und datenschutzrechtlich problematisiert und gerichtlich thematisiert werden.[1453] Herausforderungen, die – wie es an dieser Stelle scheint – durch den Gesetzgeber nach einer sorgfältigen Evaluation dessen, wie Datenflüsse die Kontexte, ihre Rationalitäten und Ziele bestmöglich gewährleisten resp. inwiefern sie diese torpedieren, zu adressieren sind. Die Rechtsprechung vermag diese Aufgabe nicht zu erfüllen.[1454]

1452 Kritisch zum Abwägungsparadigma in der Grundrechtsdogmatik Ladeur, Kritik, 12 ff.

1453 In den Anfängen wird die Thematik des rechtlichen Umgangs mit personenbezogenen Angaben sowohl in Rechtsprechung wie in der Lehre wohl im Recht auf Akteneinsicht diskutiert, wie es vorab aus dem Anspruch auf rechtliches Gehör abgeleitet wurde. Ein Recht auf informationelle Selbstbestimmung wird sodann zeitlich betrachtet im Dunstkreis der Folgejahre nach dem Volkszählungsurteil oft rezitiert. Allerdings bleibt dessen Inhalt konturlos. Insbesondere wird eine sich persistent haltende Bezugnahme auf ein Sphärendenken sichtbar, wonach Daten entsprechend als «besonders schützenswerte», «intime» Angaben ausgemacht werden.

1454 Vgl. bereits Bull, in: Hohmann (Hrsg.), 173 ff., 181, der konkrete gesetzliche Interessenabwägungen forderte, die ihrerseits kontextbezogen dargestellt werden.

Nach dieser *kursorischen Betrachtung der Rechtsprechung zum verfassungs- und öffentlich-rechtlichen Datenschutz* soll – erneut kursorisch – *die datenschutzrechtliche Judikatur* für den *privaten Bereich* umrissen werden. Sie lässt sich in zwei Blöcke einteilen. Die erste Gruppe von Entscheidungen konstituiert sich als Ergebnis individualrechtlicher Klagen wegen Persönlichkeitsverletzungen im Bereich des DSG durch betroffene Personen.[1455] Die zweite Gruppe umfasst Urteile, die auf einer Intervention des EDÖB nach Art. 29 Abs. 1 lit. a DSG basieren und die sog. «Systemfehler» adressieren.[1456] Auch im privatrechtlichen Bereich findet sich keine kohärente Umschreibung des Schutzobjekts sowie der Regelungsmechanik des Datenschutzrechts. 1099

2.2.2. Für den privaten Bereich

2.2.2.1. Fälle basierend auf individualrechtlichen Klagen

Kurz vor dem Inkrafttreten des DSG befasste sich *BGE 119 II 222* mit den Pflichten eines Praxisinhabers resp. dessen (potentiellen) Praxisnachfolgers hinsichtlich der Patientenakten und damit mit einer datenschutzrechtlichen Problematik. Zugleich standen der Wert der Patientenkarteien und die Angemessenheit des Kaufpreises zur Debatte. Der Wert und folglich der Kaufpreis wurden vom Praxisnachfolger als zu hoch reklamiert, weil die Akten weitgehend unleserlich und unverständlich seien. Damit einher ging die Frage nach den Pflichten mit Blick auf die Patientinnen und deren Krankengeschichten. Weil der ursprüngliche Praxisinhaber in der Zwischenzeit bei einem Autounfall ums Leben gekommen war, konnte dieser die Rechte der Patientinnen an ihren *sensiblen Daten* nicht mehr gewährleisten: Er wäre dazu verpflichtet gewesen, über die Praxisübernahme zu informieren und je nach Rückmeldung der jeweiligen Patientin deren Akte herauszugeben oder das Einverständnis zur Übergabe und Einsicht durch den Nachfolgearzt einzuholen.[1457] Weil das bernische kantonale Gesundheitsrecht eine Aufbewahrungspflicht vorsah, durften die Akten nicht vernichtet werden. Ein Recht auf Einsicht – über die Personalien hinaus – könne es allerdings erst nach einer Einwilligung der Patientinnen und Patienten geben. Diese müssten 1100

1455 Zur «Absicht des Gesetzgebers, die Verletzung der Persönlichkeitsrechte im Privatrechtsbereich im Einzelfall der individuellen Klage des Einzelnen zu überlassen und den Kläger nur in Fällen zu Kontrolltätigkeiten zu ermächtigen, in denen aufgrund der grossen Anzahl potenziell betroffener Personen ein öffentliches Interesse an dessen Tätigwerden besteht», vgl. BVGer A-3548/2018, Urteil vom 19. März 2019, E 1.6.3.

1456 Die jüngste Empfehlung, die vom Adressaten nicht befolgt wurde und bezüglich derer der EDÖB in der Folge den Weg ans Bundesverwaltungsgericht beschritt, ist BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2019.

1457 Vgl. aus jüngster Zeit die «Episode», geschildert im Blick: <https://www.blick.ch/news/schweiz/mittelland/totales-chaos-im-aerztehaus-bremgarten-ag-sensible-patientendaten-in-falschen-haenden-id7024092.html> (zuletzt besucht am 30. April 2021).

über den Wechsel informiert werden und in der Folge entscheiden, ob sie durch den Nachfolger behandelt werden wollen (was das Einsichtsrecht begründe) oder ob die Akten herauszugeben seien. Die Notwendigkeit eines Einverständnisses in die Einsichtnahme durch einen Dritten, den praxisübernehmenden Arzt, betrifft aber eben nur Daten aus dem Intimbereich, womit sich in diesem Urteil – wie im Mikrozensus-Urteil und in BGE 113 Ia 1 – die Selbstbestimmung bloss auf Angaben aus dem (potentiellen) Intimbereich erstreckt. Von einem Recht auf informationelle Selbstbestimmung wird in diesem Entscheid nicht gesprochen.

1101 Auf dieses Recht wird in *BGE 120 II 118* Bezug genommen. Wie im öffentlichen Bereich wird in der Schweiz mit diesem Entscheid die Selbstbestimmung an ein Akteneinsichtsrecht gekoppelt, diesmal in die Personalakte durch den Arbeitnehmer einer Bank. In E 3. führt das Bundesgericht aus, dass ein Einsichtsrecht als Teil des Rechts auf informationelle Selbstbestimmung zu verstehen sei. Zugleich hielt das Bundesgericht unter Verweis auf die Botschaft fest, dass der Datenschutzgesetzgebung des Bundes ein Recht auf informationelle Selbstbestimmung zugrunde liege. Ebendies wurde in der Folge im Schrifttum rezipiert und zitiert.[1458]

1102 Erneut auf das Recht auf informationelle Selbstbestimmung referiert *BGE 127 III 481*, ein Entscheid aus dem Medienkontext. Das Urteil erinnert an die Problematisierung durch Warren/Brandeis, denn es geht um eine Kompatibilisierung des Mediensektors mit dem öffentlichen Informationsinteresse und dem Schutz des Privatlebens. Eine Verlegerin kündigte gegenüber dem in der Schweiz gerichtsnotorisch bekannten Minelli an, dass sie ein Portrait über ihn publizieren wolle. Minelli verwehrte sich dagegen, allerdings ohne Erfolg. Minelli wurde in dem daraufhin erscheinenden Bericht als «Wilderer» bezeichnet, was er als Verletzung der Ehre beurteilte und gerichtlich geltend machte. Zudem sei die Publikation einer Fotografie widerrechtlich. Das Gericht verneinte das Vorliegen einer Ehrverletzung, um in der Folge zur Überprüfung zu kommen, ob das Portrait – in seinem Wortteil und in seinem Bildteil – einen *Eingriff in die Privatsphäre darstelle*. Weil Minelli als relative Person der Zeitgeschichte gelten, müsse er eine gelegentliche Wortberichterstattung über sich tolerieren – auch wider seinen Willen. Zur Beurteilung der Zulässigkeit einer Publikation des Abbildes stützte sich das Bundesgericht auch auf Art. 12 Abs. 2 lit. b DSG, wonach Daten einer Person gegen deren ausdrücklichen Willen lediglich bearbeitet werden dürfen, sofern ein Rechtfertigungsgrund vorliege. Das Bundesgericht hielt hierzu fest:

> «Die gegen seinen Willen veröffentlichte Fotografie stellt deshalb eine Verletzung seines im allgemeinen Persönlichkeitsrecht (Art. 28 Abs. 1 ZGB) gründenden Rechtes am eige-

1458 Baeriswil, SJZ 1995, 336 ff., 337.

nen Bild sowie seines privatrechtlichen, im DSG konkretisierten Rechts auf informationelle Selbstbestimmung dar […].»[1459]

Weil im vorliegenden Fall für die Publikation der Wortmeldung wie auch für diejenige des Abbildes ein überwiegendes öffentliches Informationsinteresse, Art. 13 Abs. 2 lit. d DSG, vorliege, seien die Veröffentlichungen nicht widerrechtlich erfolgt. Das Urteil befasst sich mit einem spezifischen Themenfeld. Dieses wird in den USA als entscheidend gesehen, auch für einen Entscheid, auf eine allgemeine Datenschutzgesetzgebung für den privaten Bereich zu verzichten. Gemeint ist die hohe Bedeutung, welche der Rede- und Pressefreiheit zugemessen wird und der gegenüber ein Recht auf informationelle Selbstbestimmung als Kontrapunkt gelesen wird.[1460] In Europa gelten spezifische datenschutzrechtliche Vorgaben für den Medienbereich. Für Deutschland ist anerkannt, dass sowohl die Pressefreiheit als auch die informationelle Selbstbestimmung die «Kommunikation in einer freiheitlichen Gesellschaft ermöglichen sollen».[1461] Beide, die Pressefreiheit resp. die Freiheit der Berichterstattung, gelten als unverzichtbare Grundrechte für demokratische Staatssysteme. Damit erfüllen sie nicht nur individualrechtliche Interessen, sondern institutionelle Interessen des Gemeinwohls.[1462] 1103

Die Kollision zwischen verschiedenen Kontexten wurde unter Inklusion des Medienkontextes anhand des Beitrages von Warren/Brandeis an früherer Stelle herausgearbeitet.[1463] *Pro memoria:* Die Autoren verwehrten sich gegen Publikationen von Berichten über die persönliche Lebensführung, das «Privatleben», in der Yellow Pres. Sie problematisierten die Medienberichterstattung über persönliche Lebensverhältnisse einzig und allein zur Befriedigung der allgemeinen Neugier und aus wirtschaftlichen Interessen. Damit werden unterschiedliche Zielrichtungen im Medienbereich sichtbar: neben dem Unterhaltungsinteresse das «sachlich motivierte Informationsinteresse» über Tatbestände, die im «Allgemeininteresse» liegen, zudem kommerzielle Interessen. Die Schweiz hat, wie der Entscheid Minelli zeigt, mit den Figuren der relativen und absoluten Person der Zeitgeschichte ein Instrumentarium entwickelt, welches die Berichterstattung über Personen mit spezifischen Rollen aufgrund eines überwiegenden Informationsinteresses überwiegen lässt. Müsste stets im Sinne einer informationellen Selbstbestimmung die Einwilligung eingeholt werden, wäre journalistisch bedeutsame Berichterstattung unmöglich.[1464] 1104

1459 BGE 127 III 481, E 3; zum Entscheid und den Figuren der absoluten und relativen Person der Zeitgeschichte auch Vogt/Wiget, in: Arter/Jörg (Hrsg.), 129 ff., 150 f.
1460 Vgl. Buchner, 20 ff.; Höning, 19 ff.; vertiefend Richards, Vand. L. Rev. 2010, 1295 ff., 1296 ff.
1461 Dix, NomosKomm-BDSG, § 41 N 1.
1462 Ders., a. a. O.
1463 Ders., a. a. O.
1464 Ders., a. a. O.

1105 Es folgen zwei Entscheidungen zum Recht am eigenen Bild, das bemerkenswerterweise ohne Bezug auf das DSG, stattdessen isoliert auf Art. 28 ff. ZGB geltend gemacht wurde. *BGE 136 III 401* lag folgender Sachverhalt zugrunde: X bot über eine Homepage einen Escort-Service sowie eine Bilder- und Filmgalerie mit «erotischen Fotos und Filmen» an. Er schloss im Oktober 2006 mit Y einen Vermittlungsvertrag für den Escort-Service. Zugleich schloss man einen Modelvertrag, mit welchem sich Y zur Erstellung von erotischen Filmen und Bildern bereit erklärte. Die Verträge berechtigten die Agentur zu einer uneingeschränkten, zeitlich und örtlich unbegrenzten Nutzung, Speicherung und Verwertung der Bilder. Bereits im Januar 2017 wurde der Rücktritt vom Escort-Vertrag vereinbart. Den Film wollte X dennoch auch in Zukunft verkaufen, allerdings ohne Erstattung einer Provision. Er «offerierte» einen Verkaufsstopp gegen eine Zahlung von CHF 4500.00. Y forderte in der Folge ein gerichtliches Verbot, ihre Fotos und Filme öffentlich zugänglich zu machen. Hierzu das Bundesgericht:

> «Das sogenannte ‚Recht am eigenen Bild' ist eine Unterart des allgemeinen Persönlichkeitsrechts von Art. 28 ZGB (statt vieler ANDREAS MEILI, in: Basler Kommentar, […], N 17 zu Art. 28 ZGB). Grundsätzlich darf niemand ohne seine (vorgängige oder nachträgliche) Zustimmung abgebildet werden, sei es durch Zeichnung, Gemälde, Fotografie, Film oder ähnliche Verfahren (BGE 127 III 481 E. 3 a/aa S. 492; MEILI, a. a. O., N 19 zu Art. 28 ZGB; MARC BÄCHLI, Das Recht am eigenen Bild, 2002, S. 89).»[1465]

1106 Zwar vertrete ein Teil der Lehre, dass die Einwilligung (ungeachtet der Frage, ob diese tatbestandsausschliessend oder rechtfertigend wirke) jederzeit widerruflich sei. Das Bundesgericht kommt in Anbetracht der Realität der «Kommerzialisierung des eigenen Bildes» zu dem Schluss, dass es grundsätzlich zulässig sei, vertragliche Verpflichtungen einzugehen, mit denen das Recht am eigenen Bild veräussert werde.[1466] Es weicht damit das «Dogma» der ideellen Natur des Persönlichkeitsschutzes auf und anerkennt unmissverständlich die Markt- und Vertragsfähigkeit eines Persönlichkeitsgutes, des eigenen Bildes, und damit einer personenbezogenen Angabe. Schranken der Einwilligung finden sich aufgrund von Art. 27 ZGB.[1467] Im Kernbereich der Persönlichkeit soll ein vertraglicher Bin-

1465 BGE 136 III 401, E 5.2.1.

1466 BGE 136 III 401, E 5.2.2.; vgl. für Deutschland insb. Götting, 12 ff., der die Entwicklung einer vermögensrechtlichen Seite des Persönlichkeitsrechts auch anhand des Rechts am eigenen Bild beschreibt.

1467 BGE 136 III 401, E 5.4.; vertiefend zur Kommerzialisierung der Persönlichkeit insb. Büchler, AcP 2006, 300 ff.; Dies., in: Honsell/Portmann/Zäch/Zobl (Hrsg.), 177 ff.; Bunneberg, *passim*; Gregoritza, *passim*; Klüber, *passim*; Beuter, *passim*; Meier, *passim*; Emmenegger, in: Gauch/Pichonnaz (Hrsg.), 209 ff.; zur Frage nach der Persönlichkeit als Immaterialgut, auch mit einem Blick auf das US-amerikanische Right of Publicity, Weber, in: Honsell/Zäch/Hasenböhler u. a., 411 ff.; das Right of Publicity ist das Recht jeder Person, prominent oder nicht, ihre Identität resp. Personendaten mit Blick auf den kommerziellen Gebrauch zu kontrollieren, womit es sich auf die commercial speech bezieht; vgl. McCarthy, Colum.-VLA J.L. & Arts 1995, 124 ff., 130 f.; Beuthien, in: Beuthien (Hrsg.), 9 ff.; Ders., NJW 2003, 1220 ff.; zu den Publicity Rights auch Bergmann, Loyola of Los Angeles ELR 1999, 479 ff.; zur Verwertung der Persönlichkeit in den Medien

dungsausschluss gelten.[1468] Ebendies nahm die Vorinstanz im vorliegenden Fall der strittigen erotischen Aufnahmen an. Das Bundesgericht allerdings vermochte der Auffassung, wonach ein bedingungsloser Rücktritt möglich sei, nicht zu folgen. Die Beschwerdegegnerin habe sich rechtsgültig und bindend verpflichtet und es seien – auch in Anbetracht der heute vorherrschenden moralischen Vorstellungen – keine Gründe ersichtlich, den Beschwerdeführer zu verpflichten, die Aufnahmen entschädigungslos zu entfernen.[1469]

Im Bundesverwaltungsurteil vom 10. April 2012 fragte sich für eine Zustellung 1107
der persönlichen Pensionskassenausweise in einem unverschlossenen Couvert an den Arbeitgeber zwecks Weiterleitung an die versicherte Person, ob der Arbeitgeber als Dritter zu qualifizieren sei und ob ein Eingriff in die informationelle Selbstbestimmung vorliege. Das Bundesverwaltungsgericht qualifizierte den *Arbeitgeber als Dritten*, da er die strittigen Angaben nicht zur Wahrnehmung seiner strategischen Aufgaben benötigen würde und daher auch keine Kenntnis davon erhalten sollte.[1470] Aufgrund der fehlenden gesetzlichen Grundlage oder einer Einwilligung durch den Arbeitnehmer hätte eine unverschlossene Weiterleitung an den Arbeitgeber nicht erfolgen dürfen.[1471] Die AXA müsse alle erforderlichen Massnahmen treffen, um bei der Zustellung der Vorsorgeausweise die Persönlichkeitsrechte der bei ihr versicherten Personen nicht zu verletzen.[1472] Der Entscheid thematisiert, obschon er die Frage nach einer Verletzung informationeller Selbstbestimmung und damit einen individualrechtlichen Konflikt adressiert, die Relevanz der informationellen Abschottung von Kontexten – des Sozialversicherungs- und Arbeitskontextes.[1473]

BGE 136 III 410 befasste sich mit einer Sachverhaltskonstellation, die im letzten 1108
Teil dieser Arbeit vertieft beurteilt wird. Sie gab in der Schweiz Anlass zu intensiven Debatten – die Observation im Versicherungskontext. Wie im vorangehenden Entscheid stützte das Bundesgericht seine Argumentation erneut ausschliess-

---

auch Bungart, *passim*; die rechtliche Bewältigung mit wirtschaftlichen Bestandteilen der Persönlichkeit resp. des Right of Publicity manifestiert sich ebenso in Konkurssituationen, vgl. insofern z. B. Campbell, 13 J. Intell. Prop. L. 2005, 179 ff.; s. auch Götting, 168 ff. und 191 ff. zum Right of Privacy sowie zum Right of Publicity gemäss US-amerikanischem Recht; als intellectual property wird das Right to Publicity qualifiziert von Gallagher, Santa Clara L. Rev. 2005, 581 ff., 581; dazu, dass das Right to Privacy ein Personal Right ist, das Right to Publicity dagegen ein Property Right Bergmann, Loyola of Los Angeles ELR 1999, 479 ff., 493; zum Right to Publicity als Recht, das den wirtschaftlichen Wert von Prominenz schützt, vgl. Franke, S. Cal. L. Rev. 2006, 958 ff.; zum Right to Publicity in den USA sodann Meyer Caroline B., 84 ff.; Seemann, 69 ff.

1468 Vgl. BGE 136 III 401, E 5.2.2. und E 5; m. w. H. Hotz, KuKo-ZGB, Art. 27 N 1 ff. und N 3 ff., insb. N 5 f.; zur Entwicklung des Right to Privacy durch Warren/Brandeis und der Weiterentwicklung zu einem Right to Publicity auch Moskalenko, IJC 2015, 113 ff., 114 ff.

1469 BGE 136 III 401, E 5.5. und E 5.6.

1470 BVGer A-4467/2011 vom 10. April 2012, E 6.3.2.

1471 BVGer A-4467/2011 vom 10. April 2012, E 8.3.2.3.

1472 BVGer A-4467/2011 vom 10. April 2012, E 10.4.

1473 Vertiefend, wenn auch nicht exakt zu dieser Konstellation und zu diesem Fall, doch aber zum Austausch von Gesundheitsdaten zwischen Arbeitgeber und Versicherung, Pärli, *passim*.

lich auf den zivilrechtlichen Persönlichkeitsschutz und Art. 28 ZGB – obschon die Zulässigkeit der «Verarbeitung personenbezogener Angaben» i. S. des DSG zur Debatte stand. Zugleich behandelte das Bundesgericht das Recht auf «Privatsphäre». Dem Urteil lag folgender Sachverhalt zugrunde: X erlitt einen Autounfall und machte einen Haushaltsschaden gegenüber den Unfallverursachenden und deren Haftpflichtversicherungen geltend. Die kantonalen Gerichte wie das Bundesgericht wiesen den Anspruch ab. Begründungsrelevant waren u. a. die Dokumentationen, welche die Haftpflichtversicherung zur Klärung des Haushaltsschadens mittels Observation durch eine Detektei vorgelegt hatte. Im Haftpflichtprozess wurde dann auch eine Persönlichkeitsverletzung infolge der Observationen ins Feld geführt. Verlangt wurde eine Feststellung der Persönlichkeitsverletzung durch die gemeinschaftlich organisierte Bespitzelung sowie Schadenersatz, die Unterlassung weiterer Observationen sowie die Herausgabe des vorhandenen «Beweismaterials». Das Bundesgericht deutete an, dass es sich weiterhin am *Konzept der Sphärentheorie* orientiere, indem es von einer Erhebung von Aktivitäten im öffentlichen Raum, die von jedermann wahrnehmbar seien, ausgehe.[1474] Zugleich verwies es auf eine in der Lehre zu verzeichnende Tendenz, wonach im Rahmen des Rechts am eigenen Bild die Einwilligung als tatbestandsausschliessend zu qualifizieren sei. Eine Persönlichkeitsverletzung sei rechtfertigbar durch überwiegende private oder öffentliche Interessen. *I. c.* ginge es um das Interesse, nicht zu Unrecht Versicherungsleistungen erbringen zu müssen. Notwendig sei eine Abwägung zwischen dem Integritätsschutz der observierten Person gegen das Interesse, einen Versicherungsbetrug auszuschliessen. Es handle sich um einen «Ermessensentscheid», wobei nicht nur die Tatsache, dass die Versicherungsleistungen beantragende Person zur Mitwirkung bei der Ermittlung der Beeinträchtigung verpflichtet sei, sondern auch die Häufigkeit, Tageszeit, Örtlichkeit, die eingesetzten Medien zur Observation usf. in die Erwägungen einzufliessen haben. Im vorliegenden Fall wurde anhand der Beobachtung von Alltagsverrichtungen wie Einkäufen nachgewiesen, dass keine Einschränkungen vorlägen. Entsprechend kam das Bundesgericht zum Schluss:

> «Insgesamt kann nicht beanstandet werden, dass das Obergericht von einem höherwertigen Interesse der Beschwerdegegner ausgegangen ist und die festgestellten Persönlichkeitsverletzungen als durch überwiegende Interessen gerechtfertigt betrachtet hat.»[1475]

1109 Kein anderes Ergebnis – so die Ansicht des Bundesgerichts – würde sich aus Erwägungen gestützt auf Art. 8 EMRK und der darauf basierenden Rechtsprechung ergeben.[1476]

1474 Vgl. BGE 136 III 410, E 5.2.
1475 BGE 136 III 410, E 4.4.
1476 Vgl. BGE 136 III 410, E 6.2.; beachte indes die Einschlägigkeit der Figur der *«reasonable expectations of privacy»* gemäss Art. 8 EMRK und vertiefend dritter Teil, IX. Kapitel mit einer Analyse eines Urteils des EGMR im Zusammenhang mit einer privatdetektivischen Observation im Bereich der

Einige Jahre später zeigte sich diese Einschätzung in Anbetracht des Entscheides des EGMR im Urteil 61838/10 vom 18. Oktober 2016 in einem anderen Licht.[1477] Das Urteil, sein Sachverhalt sowie die Argumentation wird im letzten Kapitel dieser Schrift analysiert. Hier genügt ein Hinweis: Die Auseinandersetzung mit der Entscheidung des EGMR basierend auf Art. 8 EMRK für Konstellationen der Observation im Bereich der Sozialversicherungen, durchgeführt durch einen Privatdetektiv, macht die Problematik einer Bearbeitungspraxis als *Kollision verschiedener Kontexte sichtbar*. Sie reicht weit über einen individual- und subjektivrechtlichen Konflikt hinaus.[1478] 1110

Vergleichbar der Befund für die Situation der Überwachung durch Arbeitgebende, der in Kürze i. S. eines Einschubs erwähnt sei unter Referenz auf eine weitere Entscheidung des EGMR unter Referenz auf Art. 8 EMRK, den Entscheid *Bârbulescu v. Romania*.[1479] Der EGMR befand über die Zulässigkeit einer Überwachung am Arbeitsplatz sowie die Verwertbarkeit der Resultate. Der Beschwerdeführer hatte den geschäftlichen Yahoo Messenger Account trotz des ausdrücklichen firmeninternen Verbotes zum Austausch über persönliche Angelegenheiten, wie seine Gesundheit und sein Sexualleben, privat genutzt. Der Arbeitgeber beendete daraufhin das Arbeitsverhältnis unter Einhaltung der gesetzlichen Kündigungsfrist. Der Arbeitnehmer focht die Kündigung an und rügte, dass die Überwachung seiner Kommunikation durch den Arbeitgeber einen Verstoss gegen sein Recht auf Achtung des Privat- und Familienlebens gem. Art. 8 EMRK darstellte. Der EMRK legte Grundsätze für die Überwachung der Kommunikation von Mitarbeitenden fest: Arbeitnehmer müssen um die grundsätzliche Möglichkeit einer Überwachung der Korrespondenz und anderer Kommunikation wissen. Weiter hat der Arbeitgeber einen wichtigen Grund für den Eingriff zu haben, d. h. einen konkreten Verdacht. Die Überwachung müsse im Umfang begrenzt und verhältnismässig sein (Interessenabwägung zwischen dem Recht des Arbeitnehmers auf 1111

Sozialversicherungen gegen die Schweiz EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016.

1477 Im Sinne eines Einschubes, weil öffentlich-rechtlicher Natur, sei hier auf BGer 8C_29/2009 verwiesen, der durch Beschwerde an den Europäischen Gerichtshof gezogen wurde. Man referierte hierbei auf das Leiturteil BGE 135 I 169, worin die sozialrechtliche Abteilung des Bundesgerichts bei der Beurteilung der Beschwerde in öffentlichen Angelegenheit festhielt, dass die Anordnung einer Überwachung Versicherter durch die Unfallversicherung in einem bestimmten Rahmen zulässig sei. Der EGMR hielt – anders als das Schweizer Bundesgericht – sowohl für den öffentlich- als auch für den privatrechtlichen Bereich fest, dass die Überwachung versicherter Personen und die Aufzeichnung von Videomaterial in den von Art. 8 EMRK geschützten Privat- und Familienbereich eingreife. Die gesetzliche Grundlage zur Rechtfertigung des Eingriffes, wie in Art. 8 Abs. 2 EMRK gefordert, sei indes ungenügend. Weder das ATSG noch das UVG böten hinreichend klare gesetzliche Grundlagen, um entsprechende Eingriffe qua Observation zu legitimieren.

1478 Vertiefend hierzu dritter Teil, IX. Kapitel.

1479 EGMR Nr. 61496/08 – Bârbulescu/Romania, Urteil vom 12. Januar 2016; zur Observation von Arbeitnehmenden und ihren Grenzen vgl. Pärli, HAVE 2018, 228 ff.; Götz Staehelin/Bertschi, RR-VR 2020, 5 ff.; jüngst zum Datenschutzrecht im privatrechtlichen Arbeitsverhältnis grundlegend Kasper, *passim*.

Achtung seines Privatlebens und den Interessen des Arbeitgebers an der Sicherstellung der Erfüllung der Arbeitspflicht). Eine Überwachung am Arbeitsplatz hält vor Art. 8 EMRK stand, sofern die vom EGMR definierten Mindestanforderungen der Transparenz, Sicherheit, Rechtfertigung und Verhältnismässigkeit eingehalten werden.

1112 Zur Frage der Rechtmässigkeit geheimer Observation im Versicherungskontext äussert sich *BGE 137 I 327*, ein Entscheid infolge einer Beschwerde in öffentlichrechtlichen Angelegenheiten. Dennoch wird das Urteil – wegen der Thematik als Einschub – an dieser Stelle erwähnt: Im Mai 2008 meldete sich eine Frau aufgrund langwieriger Rückenschmerzen und psychischer Beschwerden bei der Invalidenversicherung zum Rentenbezug an. Es folgten mehrere medizinische Abklärungen, nach denen die IV-Stelle die Zusprechung einer ganzen Invalidenrente bei einem Invaliditätsgrad von 70 Prozent in Aussicht stellte. Fraglich war, ob eine Überwachung durch einen Privatdetektiv rechtlich zulässig sei und ob die Observationsergebnisse als Beweismittel verwertet werden dürfen.[1480] Während das kantonale Gericht einen begründeten Anfangsverdacht für die Anordnung der Observation und damit ihre Erforderlichkeit ablehnte,[1481] sah das Bundesgericht die Observation wegen aufkommender Zweifel an den behaupteten Beeinträchtigungen als objektiv geboten an.[1482] Da die Observation zudem in einem verhältnismässig kurzen Zeitraum, nämlich während drei Tagen, stattfand und die Aufnahmen nur Verrichtungen des Alltags ohne engen Bezug zur Privatsphäre zeigten, wurde der Eingriff in die Persönlichkeitsrechte der Versicherten nicht als schwer qualifiziert.[1483] Die Observationsergebnisse durften als Beweismittel verwertet werden.[1484]

1113 Die Kontextrelevanz datenschutzrechtlicher Herausforderungen lässt sich sodann anhand von *BGE 138 III 425* nachzeichnen. In dem Entscheid ging es um die Durchsetzung des Auskunftsrechts gemäss Art. 8 DSG und die «Machenschaft», das datenschutzrechtliche Instrument zur Beweiserhebung und Prozessvorbereitung einzusetzen.[1485] Kritisch bezeichnet dies Rosenthal als «Schindluder» mit dem Auskunftsrecht, wobei die Gerichte ohne Not den Einsatz des Auskunftsrechts zu datenschutzfremden Zwecken geschützt haben, namentlich in dem hier interessierenden Entscheid.[1486] Das Bundesgericht hatte über die Pflicht einer Bank zur Erteilung einer Auskunft über bankinterne Angaben von Bankkunden

1480 Vgl. BGE 137 I 327, E 4.
1481 Vgl. BGE 137 I 327, E 4.2.
1482 Vgl. BGE 137 I 327, E 5.4.2.2.
1483 Vgl. BGE 137 I 327, E 5.6.
1484 Vgl. BGE 137 I 327, E 7.3.
1485 Hierzu Wiget/Schoch, AJP 2010, 999 ff.
1486 Vgl. Rosenthal, Jusletter vom 20. Februar 2017, N 5, wobei der Autor davon ausgeht, dass diesem Vorgang mit den Rechtsrevisionen Einhalt geboten wird.

zu befinden, was auch im Lichte von Art. 2 ZGB beurteilt wurde (und der Frage der zweckwidrigen Einsetzung des Auskunftsrechts, nämlich einer verpönten vorprozessualen Beweisausforschung). Das Bezirksgericht hatte das Begehren der Ehepartner AY und BY gegenüber der Bank auf Auskunft gemäss Art. 8 DSG betreffend die bankinternen Angaben zu ihrem Kundenprofil und Anlagezielen als zweckwidrig und entsprechend rechtsmissbräuchlich beurteilt. Das Auskunftsrecht diene der Verteidigung der Persönlichkeitsrechte und nicht der Vorbereitung eines Zivilprozesses. Das Obergericht folgte dieser Argumentation nicht und verpflichtete die Bank, die Auskunft zu erteilen. Das Auskunftsrecht gemäss Art. 8 DSG, so das Obergericht, sei ohne Interessennachweis vorgesehen und bedürfe entsprechend keiner Bindung an einen «datenschutzrechtlichen Zweck». Das Bundesgericht bestätigte sowohl die Anwendbarkeit des DSG (beachte insofern Art. 2 Abs. 2 lit. c DSG) wie auch die fehlende Bindung des Auskunftsrechts an einen Interessennachweis. Es präzisierte allerdings, dass ein Interessennachweis angezeigt sei, um die Frage eines rechtsmissbräuchlichen Einsatzes des datenschutzrechtlichen Auskunftsrechts zu überprüfen.[1487] Das Bundesgericht sah i. c. keine Zweckwidrigkeit im Auskunftsbegehren, da die Ehepartner die Auskünfte gerade zu dem Zweck, die dokumentierten Angaben auf ihre Richtigkeit hin zu überprüfen, benötigten. Entsprechend schützte es das Auskunftsbegehren.[1488]

Im Sinne eines *Zwischenfazits* lässt sich festhalten, dass es *kaum Gerichtsentscheide* infolge von *persönlichkeitsrechtlichen Klagen wegen Verletzungen des DSG* gibt. Der Weg über das Zivilgericht ist – in Anbetracht der «grenzenlosen Personendatenverarbeitung» – folglich als nur wenig effizientes Instrument zu bezeichnen, um der Einhaltung des Datenschutzrechts im privaten Bereich Nachachtung zu verschaffen. Die individualrechtliche Durchsetzung, die logische Folge der persönlichkeitsrechtlichen Anknüpfung und individualrechtlichen Fokussierung auf den Schutzbereich des DSG für den privaten Bereich, greift nur ganz selten – in Anbetracht der quantitativen Bedeutung von Personendatenverarbeitungen in einer «technologisch aufgerüsteten Informationsgesellschaft».[1489] 1114

Die wenigen Gerichtsentscheide referieren auf diverse Konzepte wie die Sphärentheorie, aber auch das Recht auf informationelle Selbstbestimmung. Damit generieren sie keine Konsolidierung mit Blick auf das datenschutzrechtliche Schutzobjekt und sind nur beschränkt tauglich, Leitplanken für ein wirksames und 1115

1487 BGE 138 III 425, E 4.3.

1488 Ein weiterer Entscheid zum Auskunftsrecht im Bankenbereich ist BGE 141 III 119. Dem Datenschutzrecht kommt im Bankensektor eine besondere Bedeutung zu, vgl. namentlich auch im Kontext des Steuerstreites mit den USA: BGE 139 II 404 und BGer 4A_524/2014 vom 10. Februar 2016.

1489 Vertiefend zur persönlichkeitsrechtlichen Basierung des DSG für den privaten Bereich zweiter Teil, VI. Kapitel.

griffiges Datenschutzrecht zu liefern. Weiter fokussiert die Rechtsprechung, die aus individualrechtlichen Klagen wegen Persönlichkeitsverletzungen basierend auf dem DSG resultiert, spezifische Rechte wie namentlich das Recht am eigenen Bild oder das Auskunftsrecht. Im Ergebnis laufen die gestützt auf persönlichkeitsrechtliche Klagen gefällten Entscheide auf eine Interessenabwägung im Einzelfall hinaus.[1490]

1116 Ergiebiger für die Effektuierung des Datenschutzgesetzes ist, wie sogleich zu zeigen ist, die Rechtsprechung, die im Anschluss an Empfehlungen durch den EDÖB bei sog. Systemfehlern, vgl. Art. 29 DSG, ergeht. Nach Art. 29 Abs. 1 lit. a DSG klärt der EDÖB von sich aus oder auf Meldung Dritter den Sachverhalt ab, wenn ein sog. *Systemfehler* vorliegt. Als Systemfehler gelten Bearbeitungsmethoden, welche die Persönlichkeit einer grösseren Anzahl von Personen verletzen. Wird einer vom EDÖB erlassenen Empfehlung nicht Folge geleistet, eröffnet sich der Weg zunächst an das Bundesverwaltungsgericht und in letzter Instanz an das Bundesgericht. Insofern sind jüngst mehrere namhafte Urteile ergangen, so das Logistep-Urteil[1491], Google Street-View-Urteil[1492], Money-House-Urteil[1493], Lucency-Urteil[1494] und jüngst der Entscheid i. S. Helsana Zusatzversicherungs-AG[1495]. Mit der Totalrevision werden Interventionen des EDÖB nicht mehr an die Kategorie des Systemfehlers angeknüpft, vgl. Art. 49 ff. nDSG. Eine vertiefte Auseinandersetzung mit den nach bisherigem Recht infolge von Systemfehlern ergangenen Entscheidungen ist dennoch aufschlussreich, namentlich für die Entwicklung eines datenschutzrechtlichen Rekonfigurationsvorschlags.

2.2.2.2. Fälle basierend auf Empfehlungen und Klagen des EDÖB

1117 Eine chronologische Präsentation der einschlägigen Entscheidungen würde an ihren Anfang das Logistep-Urteil stellen.[1496] Da dieses im Zuge dieser Schrift wegen seines Charakters als Leitentscheid wiederholt thematisiert wurde, soll an

1490 Eindrücklich im Zusammenhang mit der sog. gestörten Vertragsparität und dem privatrechtlichen Verhältnismässigkeitsgrundsatz die Worte von Derleder, in: Jestaedt/Lepsius (Hrsg.), 234 ff., 243: «Nur auf dieser Basis lässt sich eine grundrechtsorientierte Weiterentwicklung der Rechtsordnung realisieren, bei der die Angewiesenheitslagen im Besonderen zu beachten sind. Das schliesst es auch aus, die jeweils durch systematische Rechtsanwendung erzielten Ergebnisse mit der Sosse eines allgemeinen, nicht grundrechtsgebundenen zivilrechtlichen Verhältnismässigkeitsgrundsatzes zu überziehen, der jeden Konflikt zum Einzelfall macht».

1491 BGE 136 II 508.

1492 BGE 138 II 346; kritisch zum Vorgehen im Rahmen der Interessenabwägung mit analogem Einwand für das Logistep-Urteil Meier, medialex 2011, 69 f.

1493 BVGer A-4232/2015.

1494 BVGer A-5225/2015.

1495 Vgl. BVGer A-3548/2018 – der Entscheid ist hervorragend geeignet, um die Defizite einer Konzeption, welche den persönlichkeitsrechtlichen Ansatz in das Zentrum der Aufmerksamkeit rückt, nachzuzeichnen.

1496 BGE 136 II 508.

dieser Stelle der Hinweis auf eine vom Urteil angestossene Rechtsentwicklung genügen: Mit der Teilrevision des URG sollen Unsicherheiten, die hinsichtlich der Zulässigkeit von Personendatenverarbeitungen zwecks Aufdeckung von Urheberrechtsverletzungen im Zuge des Urteils entstanden seien, beseitigt werden.[1497]

Der Entscheid Google-Street-View, *BGE 138 II 346,* wird mit einigen Kernbefunden für die Effektuierung des Datenschutzrechts herausgegriffen. In dem Entscheid findet sich nicht nur eine Referenz auf ein «Recht auf informationelle Selbstbestimmung». Darüber hinaus beinhaltet das Urteil konkretisierende Ausführungen zum Inhalt der generalklauselartigen Bearbeitungsgrundsätze, der daraus resultierenden Anforderungen an die Verarbeitungsmethode sowie zur Bedeutung der Rechtfertigungsgründe. Weiter referiert das Bundesgericht auf die Sphärentheorie, die es in diesem Entscheid im Kontext moderner Datenverarbeitungstechnologien weder als obsolet noch als hinreichend starkes Bewältigungsinstrument taxiert.[1498] Das Bundesgericht stellt in diesem Entscheid alsdann eine «Variation» des «Grundrechts auf informationelle Selbstbestimmung» vor. Zugleich wirft es Fragen in Bezug auf die Auswirkungen auf das Privatrecht auf. Entsprechende «Kernaussagen» an dieser Stelle sind: 1118

> «Im Bereich des Datenschutzes garantiert das verfassungsmässig geschützte Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV und Art. 8 Ziff. 1 der Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten [EMRK; SR 0.101]), dass grundsätzlich ohne Rücksicht darauf, wie sensibel die fraglichen Informationen tatsächlich sind, dem Einzelnen die Herrschaft über seine personenbezogenen Daten zusteht […]. Nach Art. 35 Abs. 3 BV sorgen die Behörden dafür, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden. Der Verwirklichung dieses verfassungsrechtlichen Auftrags dient im vorliegenden Zusammenhang unter anderem das Tätigwerden des EDÖB gemäss Art. 29 DSG […].»[1499]

Auch in diesem Urteil fehlt eine Begründung für die «Uminterpretation» des Missbrauchsverbotes gemäss Art. 13 Abs. 2 BV in ein Selbstbestimmungsgrundrecht. Offensichtlich wird dem Recht auf informationelle Selbstbestimmung eine andere Bedeutung zugemessen, als es mit dem Volkszählungsurteil des Bundesverfassungsgerichts geschah. Aus Letzterem wurde wie gesagt die Verankerung eines prinzipiellen Verarbeitungsverbotes mit Erlaubnistatbestand gefolgert. Dieses Regime gilt gemäss DSGVO ebenso für den privaten Bereich.[1500] Die Schweiz allerdings sieht in ihrem DSG kein entsprechendes System vor, auch nicht nach 1119

1497 Vgl. Art. 66j E-URG vom 11. Dezember 2015, abrufbar unter: <https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2015/2015-12-11/vorentw-urg-d.pdf> (zuletzt besucht am 30. April 2021).

1498 BGE 138 II 346, E 8.2.; vgl. auch den Entscheid zu Google vom Bundesverwaltungsgericht, BVGer A-7040/2009 vom 30. März 2011, E 3.3.3., m. w. H.

1499 BGE 138 II 346, E 8.2.

1500 Vgl. Art. 6 DSGVO; die DSGVO kann aufgrund von Art. 3 DSGVO extraterritoriale Wirkung entfalten, weshalb namentlich auch Schweizer Unternehmen mit ihren Verarbeitungshandlungen bei Erfüllung der Tatbestandselemente in ihren Anwendungsbereich fallen können.

der Totalrevision. Zwar kann eine Widerspruchslösung durchaus als Instrument und Ausdruck einer Selbstbestimmung qualifiziert werden.[1501] Nichtsdestotrotz unterscheidet sich dies konzeptionell grundlegend vom System des Verarbeitungsverbots mit Erlaubnistatbeständen. Zudem stösst die Widerspruchslösung in der Realität auf Grenzen. Von einem Herrschaftsrecht des Einzelnen zu sprechen, vermag vor diesem Hintergrund nicht zu überzeugen. Wird in der Schweiz von einem Recht auf informationelle Selbstbestimmung gesprochen, ist damit in erster Linie wohl auch gemeint, dass sich der grundrechtliche Schutz des Menschen im Kontext von Datenverarbeitungen nicht auf «sensible Daten» beschränkt. Ebendies drückt auch das DSG aus. Mit einer entsprechenden «Ausweitung» des grundrechtlichen Schutzbereiches von «sensiblen Daten» auf Daten jeglicher «Art» wird der Schritt vollzogen, der für Deutschland als zwischen Mikrozensus-Urteil und dem Volkszählungsurteil liegend beschrieben wurde. Wenn allerdings die Ausweitung der Schutzwirkung von «sensiblen Daten» auf «gewöhnliche Daten» gleichgesetzt wird mit der Abkehr von einem Schutz vor missbräuchlicher Datenverarbeitung und der Hinwendung zu einem Schutzregime der informationellen Selbstbestimmung, werden zwei unterschiedliche Anknüpfungen vermengt. Die Behauptung, wonach ein «Herrschaftsrecht des Einzelnen an seinen personenbezogenen Daten» besteht, suggeriert einen Rechtsbestand, welcher in einer solchen Gestalt im schweizerischen Recht und namentlich im DSG für den privaten Bereich nicht verbürgt wird.

1120 Gleichwohl sind mehrere Aspekte des Entscheides erwähnenswert, mit denen das Bundesgericht für das Datenschutzrecht und dessen Wirksamkeit Impulse setzt: Erstens befasst es sich eingehend mit den Verarbeitungsgrundsätzen des DSG und verleiht ihnen Konturierung. Zweitens wiederholt es, was im Logistep-Urteil entschieden wurde, nämlich dass *Rechtfertigungsgründe im Rahmen von Art. 12 Abs. 2 lit. a DSG nur mit grosser Zurückhaltung angenommen werden dürfen*.[1502] Indem das Bundesgericht bestätigt, dass ein Verstoss gegen die allgemeinen Bearbeitungsgrundsätze nur restriktiv legitimiert werden dürfe, verleiht es dem mit den Verarbeitungsgrundsätzen etablierten «Minimalstandard» Beständigkeit. Die Rechtsprechung, wonach die Mindestanforderungen in Gestalt der allgemeinen Verarbeitungsgrundsätze nur ganz ausnahmsweise verhandelbar sind, vermittelt dem Datenschutz(gesetz) in der Schweiz Nachachtung. Der unbeschränkten und beliebigen Flucht in rechtfertigende überwiegende Interessen oder dem Weg über die rein formelle Einholung der Einwilligung wird damit ein Riegel vorgeschoben, was eine Stabilisierung der Mindestvorgaben in Bezug auf die Integrität der Datenverarbeitung etabliert. Diese nur beschränkt verhandelba-

1501 Hierzu vertiefend bereits zweiter Teil, IV. Kapitel.

1502 BGE 138 II 346, E 7.2.; BGE 136 II 50, E 6.3.1. mit Verweis auf E 5.2. ff.; meines Erachtens sollte diese Zurückhaltung auch nach Totalrevision des DSG und Art. 30 f. nDSG fortgelten.

re Einhaltung der allgemeinen Verarbeitungsgrundsätze ist – nochmals – für ein Regime, das in diesen die *primäre Schranke der prinzipiellen Verarbeitungsfreiheit* festsetzt, von zentraler Bedeutung. Anders figurieren die allgemeinen Verarbeitungsgrundsätze in den Systemen mit prinzipiellem Verarbeitungsverbot als zusätzliche, gewissermassen zweite Schranke der Personendatenverarbeitung, vgl. Art. 5 f. DSGVO.[1503] Darüber hinaus ist der Entscheid i. S. Google Street View insofern beachtlich, als er zumindest implizit an der so tief verwurzelten Konzeption von «öffentlich» und «privat» rührt, welche die Fortentwicklung auch des Datenschutzrechts blockiert.[1504]

Zwar verwirft das Bundesgericht die Sphärentheorie nicht und bezieht sich 1121
in wenig überzeugender Weise auf den Bestand eines Rechts auf informationelle Selbstbestimmung. Gleichwohl liegt seiner Entscheidung der Befund zugrunde, dass einzig und allein deshalb, weil ein Personendatum in der «Öffentlichkeit» erhoben wurde – es geht um die Fotografie von Personen im öffentlichen Raum – der datenschutzrechtliche Schutz *nicht als obsolet* gelten kann.[1505] Die Begründung knüpft das Bundesgericht zwar im Recht am eigenen Bild an. Allerdings zeigen die geforderten Anonymisierungen, dass vonseiten des Gerichts die Situation als gänzlich unterschiedlich beurteilt wird für den Fall, dass eine Person im öffentlichen Bereich quasi per Zufall durch andere Menschen gesehen wird, was auch wieder vergessen wird, oder, ob eine Person im öffentlichen Raum fotografiert wird und in der Folge deren Abbild zeitlich und persönlich unbeschränkt im Internet abgerufen werden kann.[1506] Die *Technologie verändert die Datenflüsse in markanter Weise*, was das Gericht denn auch aus datenschutzrechtlicher Perspektive adressiert. Indem das Bundesgericht verlangt, dass Personen – die zuvor im öffentlichen Raum fotografiert wurden – im Internet nicht mehr erkennbar sein dürfen, anerkennt es die Notwendigkeit eines Schutzes von Personenangaben, die nach traditioneller Auffassung «öffentlich» waren – im öffentlichen Raum aufgenommen wurden –, wenn diese im Internet publiziert werden. Das Bundesgericht verlässt damit eine räumlich verhaftete Perzeption. Zugleich bahnt es der Erkenntnis den Weg, dass Verarbeitungszusammenhänge anzuerkennen sind, wobei sich mit dem Transfer von Personenangaben in das

1503 Auf die Unterschiedlichkeit des Regimes mit Blick auf die DSGVO weist auch BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.3. hin, ohne allerdings eine systematische und harmonisierende Auslegung des Schweizer Rechts mit Blick auf das europäische Recht vorzunehmen.

1504 Vgl. dazu Nissenbaum, 158, 225, 232; zum Abbild dieser Dichotomie im dualistischen Regime des DSG, vgl. zweiter Teil, IV. Kapitel.

1505 Das Thema wird uns im Zuge der Entwicklung eines eigenen Lösungsansatzes anhand der im öffentlichen Raum vorgenommenen Versicherungsobservation vertiefend beschäftigen, vgl. dritter Teil, IX. Kapitel.

1506 Insofern auch Nissenbaum, 10, 51 f., 192 f., 219 ff.

Internet, wie es bei Google Street View geschieht, die *Topografie der Verarbeitungshandlungen massgeblich verändert*.[1507]

1122 Eine Aufweichung der Kategorisierung von Personendaten in öffentliche und private Angaben findet sich weiter in *BVGer A-4232/2015,* der sich ebenso mit Datenverarbeitungen im Internet beschäftigte. Wiederholt hatte sich das Bundesverwaltungsgericht mit der Auskunftei Moneyhouse zu befassen. Den vorläufigen Abschluss bildet das Urteil vom 18. April 2017. Der EDÖB hatte mehrere Empfehlungen zu den durch Moneyhouse im Internet angebotenen Dienstleistungen formuliert, denen die Moneyhouse AG allerdings nicht nachkam.[1508] Nachdem das Bundesverwaltungsgericht die Befugnis des EDÖB, i. c. Empfehlungen zu erlassen, bejaht hatte (Anwendbarkeit des DSG mit dessen privatrechtlichem Normenkomplex; E 4), überprüfte es die vom EDÖB beanstandeten Bearbeitungsprozesse von Moneyhouse im Lichte von Art. 12 f. i. V. m. Art. 4 ff. DSG. Es führte hierbei aus, es sei unbestritten, dass die Beklagte nicht besonders schutzwürdige Angaben bearbeite. Fraglich sei indes, ob die gesetzlich verstärkten Schutzmechanismen, wie sie für die Verarbeitung von Persönlichkeitsprofilen vorgesehen sind, greifen würden. In diesem Zusammenhang äusserte sich das Bundesverwaltungsgericht zu Inhalt und Problematik von Persönlichkeitsprofilen wie folgt:

> «Die miteinander verknüpften Personendaten erreichen relativ rasch eine Informationsdichte, die Verhaltensmuster und Persönlichkeitsprofile erkennen lassen (Probst, a. a. O., S. 30). Die Betroffenen haben oft keine Kenntnis vom Bestehen eines Profils und können so dessen Richtigkeit und Verwendung nicht kontrollieren. Einmal erstellt, können aber Persönlichkeitsprofile den Betroffenen der Freiheit berauben, sich so darzustellen, wie er will. Sie vermögen mithin die Entfaltung der Persönlichkeit wesentlich zu beeinträchtigen. Deshalb sollen sie, gleich wie besonders schützenswerte Daten, nur unter bestimmten Voraussetzungen erstellt und bearbeitet werden dürfen.»[1509]

1507 Vgl. zur Videoüberwachung des Aussen- wie Innenbereiches eines Mietshauses BGE 142 III 263, wo das Bundesgericht vorab auf den Unterschied zwischen Miet- und Arbeitsrecht verweist, wobei letzteres mit Art. 328b OR eine Spezialregelung findet. Eine solche Sondernorm fehle für die Datenbearbeitung im Kontext des Verhältnisses von Vermieter und Mieter; anwendbar ist das DSG und Art. 28 ZGB. In der Folge prüft das Bundesgericht die Zulässigkeit des installierten Videoüberwachungssystems im Lichte von Art. 12 f. i. V. m. Art. 4 DSG. Es hält fest, dass ein Interesse der Vermieter sowie der zustimmenden Mieterschaft an der Prävention und Aufklärung von Einbrüchen sowie Vandalismus nicht jegliche Überwachungsmassnahme legitimiere. Es habe eine Abwägung namentlich mit dem Interesse auf Schutz der Privatsphäre der nicht zustimmenden Partei stattzufinden. Hierbei seien sämtliche Umstände des Einzelfalles für die Beurteilung relevant, beispielsweise die Grösse der Liegenschaft. Das Bundesgericht stützt die Erwägung der Vorinstanz, wonach die 24-stündige und damit dauerhafte Überwachung im Eingangsbereich des Mehrfamilienhauses, die eine systematische Erhebung des Verhaltens des Beschwerdegegners ermöglicht, einen erheblichen Eingriff in die Privatsphäre darstelle (E 2.2.2.). Das Bundesgericht befand ebenso in Anbetracht der überschaubaren Verhältnisse, dem Fehlen einer konkreten «Bedrohungssituation» sowie der hinreichenden Absicherung anhand weniger Kameras darauf, dass bestimmte Kameras zu entfernen seien.

1508 EDÖB, Datenschutz, Empfehlungen, Bern 2021, <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April 2021).

1509 BVGer A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.2.1.

Das Bundesverwaltungsgericht evaluierte sodann die unterschiedlichen Dienste der Moneyhouse und betonte, dass für die Qualifikation einer Bearbeitung als «Bearbeitung eines Persönlichkeitsprofils» Inhalt und Menge von personenbezogenen Angaben entscheidend seien. Nicht massgeblich sei, ob entsprechende personenbezogene Angaben bereits öffentlich zugänglich seien oder nicht. Einschlägig sei einzig, ob die Verknüpfung von Daten Aufschluss über einen oder mehrere wesentliche Aspekte der Persönlichkeit eines Individuums gäbe.[1510] Namentlich der entgeltliche Dienst gegenüber registrierten Nutzern (Premium-Usern) ginge weit über eine reine Bonitätsauskunft hinaus (bei der einzig die Identität, Betreibungen usf. ausgewertet werden), indem er *umfassende Angaben* zu Name, Alter, Adresse, familiären Verhältnissen, Wohnsituation, Nachbarschaft, Beruf und früheren Berufen, Ausbildung usf. gibt, was vom Bundesverwaltungsgericht als Bearbeitung von Persönlichkeitsprofilen qualifiziert wurde.[1511] Weil es sich hierbei um eine gemäss DSG qualifizierte Datenverarbeitung handle, seien spezifische Schutzvorkehrungen zu beachten. Insbesondere bedarf die Weitergabe von Persönlichkeitsprofilen an Dritte eines Rechtfertigungsgrundes, Art. 13 DSG.[1512] Vorliegend kam eine Einwilligung der betroffenen Personen in Frage. Die Beklagte allerdings konnte nicht nachweisen, dass sie die explizite Einwilligung der betroffenen Personen nach rechtzeitiger Information, vgl. Art. 4 Abs. 5 DSG, eingeholt hatte.[1513] Entsprechend prüfte das Bundesverwaltungsgericht das Vorliegen eines überwiegenden Interesses der Datenbearbeiterin, wobei aufseiten der Datenbearbeitenden oft wirtschaftliche Interessen und das Streben nach Profit im Vordergrund stünden.[1514] Es bestätigte die Rechtsprechung, wonach Rechtfertigungsgründe bei Verstössen gegen die allgemeinen Bearbeitungsgrundsätze nur ganz ausnahmsweise angenommen werden dürften. Zu berücksichtigen seien indes nicht nur gewinnstrebende Interessen der Datenverarbeitenden, sondern auch Informationsinteressen Dritter. Allerdings ginge der Transfer von Angaben zu Lebens- und Wohnsituation über das hinaus, was zur Erfüllung eines legitimen Interesses an einer Bonitätsauskunft gehöre. Eine solche lasse sich bereits aufgrund von Betreibungsauszügen beschaffen; weitere Angaben seien insofern nicht von einem öffentlichen Interesse gedeckt, zumal diese nicht geeignet seien, mit hinreichender Sicherheit etwas über die Wirtschaftskraft einer Person auszusagen. Das Bundesverwaltungsgericht räumte Wirtschaftsinformationen auch mit Blick auf Angaben, wie sie dem Handelsregister zu entnehmen sind, hohe Relevanz zu. An Personen dagegen, die keine relativen oder absoluten Perso- 1123

1510 BVGer A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.2.4.
1511 BVGer A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.2.5.2.
1512 Die Konstruktion des Persönlichkeitsprofils wird mit dem totalrevidierten DSG nicht mehr verwendet; neu wird das sog. «Profiling» geregelt.
1513 BVGer A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.4.1.
1514 BVGer A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.4.2.

nen der Zeitgeschichte seien, bestünde kein allgemeines öffentliches Interesse, welches über den punktuellen Aspekt der wirtschaftlichen Persönlichkeit hinausginge. Entsprechend könne kein allgemeines öffentliches Informationsinteresse an Angaben über private Lebensverhältnisse wie Verwandtschaftsverhältnisse, Wohnsituation usf. angenommen werden. Dies gelte selbst dann, wenn sich solche Angaben beispielsweise aus einem Handelsregisterauszug erschliessen lassen.[1515] Über Angaben, die keine Bonitätsrelevanz haben, dürfe nicht ohne die Zustimmung der betroffenen Personen verfügt werden. Die Beklagte allerdings würde Persönlichkeitsprofile erstellen und weitergeben, wofür weder Einwilligung noch überwiegende Interessen oder von Dritten vorlägen. Unter Hinweis auf BGE 136 III 583, wonach überwiegende private und öffentliche Interessen bloss zurückhaltend angenommen werden dürfen, können die wirtschaftlichen Interessen der Beklagten die Interessen am Persönlichkeitsschutz der zahlreichen von den Datenbearbeitungen betroffenen Personen nichtübertrumpfen. Der Eingriff in die Persönlichkeitsrechte sei nicht gerechtfertigt. Folglich ordnete das Bundesverwaltungsgericht die Löschung der mit Persönlichkeitsprofilen verknüpften Angaben an, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit beinhalten, die über die Bonität hinausgehen. Mit dem Entscheid wird folglich ein *privater Lebensbereich* auch im Internet vor *informationellen Übergriffen aus wirtschaftlichen Interessen* heraus klar abgegrenzt.[1516]

1124 Es folgte der Entscheid Lucency, *BVGer A-5225/2015 vom 12. April 2017*. Er sei etwas kürzer umrissen, zumal ihm nicht der Charakter eines Leitentscheides für das Datenschutzrecht zukommt. Gleichwohl zeigt er die Bedeutung behördlicher Aktivitäten zwecks Effektuierung des Datenschutzgesetzes: Drei in Deutschland lebende Personen hatten sich an den EDÖB gewandt, weil sie unerwünscht Werbeschreiben für eine Bank erhalten hatten. Die fraglichen Adressangaben waren über die Lucency AG bezogen worden. Die Lucency AG hatte mehrere Auskunftsbegehren nicht erfüllt; ebenso wenig war sie der Registrierungspflicht nachgekommen. Das Bundesverwaltungsgericht verurteilte das Marketing-Unternehmen zur Erfüllung der besagten Pflichten. Der Adresshandel und die Geschäftsmodelle von Auskunfteien stellen sich im Lichte des Datenschutzrechts seit jeher als Herausforderung dar – dieser Teil wird sich im Rahmen der Auseinandersetzung mit den faktischen Herausforderungen etwas genauer damit befassen.[1517]

1515 BVGer A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017, E 5.4.2.2.; vgl. z. B. Weichert, wrp 1996, 522 ff., 522; Ders., DuD 2005, 582 ff.

1516 Zur kommerziellen Nutzung von Personendaten mittels Werbeaktionen weiter BVGer A-5225/2015 – Lucency, Urteil vom 12. April 2017.

1517 Vgl. nachfolgend dritter Teil, VII. Kapitel, B.

Mit dem Adresshandel hatte sich das Bundesgericht bereits früh zu befassen, *BGE 97 II 97*, der im Sinne eines Einschubes erwähnt wird: Der Betreiber M des Adressverlages bot verschiedene Adresslisten zum Kauf an. Bei einer der Listen handelte es sich um das Verzeichnis der Mitglieder des Vereins «Philanthropische Gesellschaft Union». Ebendieses bot er in seiner Gesamtheit mit rund 400 Adressen zu etwas über CHF 300.00 feil; ein Segment, beschränkt auf Adressen in Zürich, war bereits für rund CHF 15.00 zu haben. Auf Klage hin befand das Bundesgericht, dass der Verkauf der Liste mit Namen der Vereinsmitglieder ein Verstoss gegen den Schutz der Privatsphäre der Mitglieder und des Vereins selbst sei und urteilte auf Unterlassung des Adressverkaufs. Zur Begründung hiess es, dass die Mitgliedschaft in einem Verein eine unter dem Schutz von Art. 28 ZGB stehende persönliche Angelegenheit sei, deren Weitergabe und damit Veröffentlichung nicht zulässig sei. 1125

Betreffend *BVGer A-5225/2015 vom 12. April 2017* sollen drei Schlaglichter gesetzt werden. Erstens ging es in dem Entscheid um einen internationalen Sachverhalt, was aktuell eher die Regel als die Ausnahme ist. Der EDÖB wurde auf Ersuchen von drei in Deutschland lebenden Personen – Deutschland gilt als Vorreiter, was den Schutz datenschutzrechtlicher Anliegen anbelangt – gegenüber der in der Schweiz ansässigen Lucency AG tätig. Zweitens zeugte das Verhalten der Beklagten in Anbetracht der im Urteil dargelegten Vorgeschichte nicht von Bewusstsein gegenüber der Relevanz des Datenschutzrechts und seiner Einhaltung, ebenso wenig von Respekt gegenüber der Autorität des EDÖB. Indem der EDÖB seiner Empfehlung Nachdruck durch den Gang an das Bundesverwaltungsgericht verlieh und ebendieses der Gewährleistung des Auskunftsrechts sowie der Registrierungspflicht für Personendatensammlungen zum Durchbruch verhalf, ist der Lucency-Fall ein Zeugnis der behördlichen Effektuierung des Datenschutzgesetzes *de lege lata*.[1518] 1126

Einen vorläufigen Schlusspunkt bildet der *Entscheid des Bundesverwaltungsgerichts A-3548/2018 i. S. Helsana+ vom 19. März 2019*, der Mitte Mai 2019 rechtskräftig wurde. Das Urteil soll an dieser Stelle nicht erschöpfend in Bezug auf seine Erwägungen zu den datenschutzrechtlichen Vorgaben analysiert werden.[1519] Die Empfehlungen des EDÖB und sein erneut konsequenter Gang an das Bundesverwaltungsgericht bei ihrer Nichtbeachtung durch die Adressatin, namentlich aber auch die äusserst sorgfältige und ausführliche Entscheidfindung des Bundesverwaltungsgerichts dokumentieren, dass das Datenschutzrecht eben- 1127

1518 Hinzuweisen ist unter dem Thema des Adresshandels im Lichte des Datenschutzrechts auch auf die im Zusammenhang mit der Veröffentlichung von Adressdaten im Internet durch die Itonex AG erlassene Empfehlung des EDÖB vom 15. November 2011, vgl. <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April 2021).

1519 Vgl. insofern die Beiträge von Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; Vasella/Ziegler, digma 2019, 80 ff.; Pärli, SZS 2018, 107 ff.

so in der Schweiz einen Bedeutungswandel vollzieht. Zu beurteilen war das von der Zusatzversicherungs-AG betriebene, appbasierte Programm Helsana+.[1520] Am 26. April 2018 erliess der EDÖB eine Empfehlung gegenüber der Helsana Zusatzversicherungs-AG, deren Umsetzung am 22. Mai 2018 von Letzterer abgelehnt wurde. In der Folge reichte der EDÖB Klage gegen die Helsana Zusatzversicherungs-AG mit folgendem Rechtsbegehren ein: Die Entgegennahme und Weiterbearbeitung von Personendaten aus der Grundversicherung sowie das Einholen von Einwilligungserklärungen hierzu seien zu unterlassen. Ebenso Abstand zu nehmen sei von der Bearbeitung der Kassenzugehörigkeitsangaben und weiteren Personendaten aus der Grundversicherung. Sie erfolge zum Zweck, unrechtmässig geldwerte Rückerstattungen zu leisten. In diesem Zusammenhang gespeicherte Personendaten seien innert gerichtlich festgelegter Frist und unter Anweisung an Dritte zu löschen. Die Beklagte verlangte Abweisung der Klage. Es folgten Replik und Duplik, wobei sich alsdann das Bundesverwaltungsgericht mit mehreren *datenschutzrechtlichen Grundsatzfragen* zu befassen hatte: Beurteilt wurde die Frage, ob der Normenkorpus des DSG für Bundesbehörden auf als Bundesorgan handelnde Private oder derjenige für den privaten Bereich anwendbar sei. Es folgten Auslegungsfragen bezüglich die allgemeinen Verarbeitungsgrundsätze und spezifisch zum Rechtmässigkeitsprinzip. Zudem fand eine Auseinandersetzung mit den Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung statt, sodann mit dem verzahnten Regelungsregime des DSG mit Spezialgesetzgebungen (i. c. des Versicherungsbereichs). Das Urteil wurde an verschiedenen Stellen in Bezug auf seine verschiedenen Aspekte bereits dargestellt (so z. B. die Anwendbarkeit der privatrechtlichen Bestimmungen des DSG, aber auch die Verarbeitungsgrundsätze). An dieser Stelle sollen kursorisch und gerade nicht erschöpfend die wichtigsten Themen des Urteils umrissen werden. Der Fokus der Darstellung allerdings richtet sich darauf, das Urteil für den in dieser Schrift angeregten Paradigmenwechsel produktiv zu machen.[1521]

1128 Nachdem sich das Bundesverwaltungsgericht eingehend mit der Aktiv- und Passivlegitimation des Klägers sowie der Beklagten und hierbei mit Art. 2 sowie Art. 29 DSG sowie Art. 35 VGG befasst hatte, wies es vorab auf die Anwendbar-

1520 Nach diesem Programm sollten Nutzende über die App für bestimmte Aktivitäten, z. B. Sport, Pluspunkte sammeln können, wobei der Nachweis per Foto-Upload erfolgte. Später sollten die Pluspunkte in Barauszahlungen, Sachleistungen, Gutscheine von Partnerbetrieben umgewandelt werden können. Nutzungs- und bonusberechtigt sollten Versicherungsnehmer einer Versicherungsgesellschaft der Helsana AG sein. Um die Teilnahmeberechtigung (i. e. die Eigenschaft, Versicherungsnehmerin resp. Versicherungsnehmer bei einer Helsana-Gesellschaft zu sein) sowie die Berechnung der Boni zu klären, holte die Helsana Zusatzversicherungs-AG bei den Antragstellenden die Einwilligung zu Personendatenverarbeitungsprozessen ein, um «Daten von der obligatorischen Krankenversicherung der Helsana-Gruppe zur Zusatzversicherung zu übertragen».

1521 Vertiefend zum Urteil im Lichte des Datenschutzrechts *de lege lata* vgl. Bühlmann/Schüepp, Jusletter vom 15. März 2021; Blonski, digma 2019, 100 f.; auch *de lege ferenda* Vasella/Ziegler, digma 2019, 80 ff.

keit des Grundsatzes der Sachverhaltsabklärung von Amtes wegen hin, Art. 44 Abs. 2 VGG. Das Bundesverwaltungsgericht qualifizierte das Rechtsverhältnis zwischen den betroffenen Personen und der Beklagten als nicht öffentlicher Natur und erklärte Art. 12 ff. DSG als einschlägig.[1522] Mit Blick auf die Einhaltung der allgemeinen Verarbeitungsgrundsätze von Art. 4 DSG führte es Folgendes aus: Der Transfer von Personendaten, die durch und zwecks Grundversicherung erhoben worden waren, an die Zusatzversicherung zwecks Evaluation der Teilnahmeberechtigung am Helsana+-Programm, verletze das *Zweckbindungsgebot gemäss* Art. 4 Abs. 3 DSG. Zum Rechtmässigkeitsgebot hielt das Bundesverwaltungsgericht fest, dass eine Personendatenverarbeitung nur dann unrechtmässig i. S. v. Art. 4 Abs. 1 DSG sei, wenn gegen eine Norm verstossen werde, die zumindest auch, direkt oder indirekt, dem Schutz der Persönlichkeit diene.[1523] Zum Rechtmässigkeitsprinzip führte das Gericht aus, dass die Beschaffung von Personendaten durch die Beklagte bei den Grundversicherungsgesellschaften nur rechtmässig sei, wenn auch die Bekanntgabe der Personendaten rechtmässig sei. Entsprechend untersuchte das Bundesverwaltungsgericht, ob die im Bereich der obligatorischen Krankenversicherung agierenden Versicherungsgesellschaften der Helsana-Gruppe zur Herausgabe der Personendaten an die Beklagte berechtigt waren. Da diese unter Art. 3 lit. h DSG fiele, seien Art. 16 ff. DSG anwendbar. Folglich dürfen Personendaten nur basierend auf einer gesetzlichen Grundlage gemäss Art. 17 Abs. 1 DSG bearbeitet werden. Zu beachten sei weiter die Spezialgesetzgebung: Nach Art. 84 KVG dürfen Personendaten ver- oder bearbeitet werden, die notwendig sind, um die nach dem KVG übertragenen Aufgaben zu erfüllen. Art. 33 ATSG statuiert, dass Personen, die an der Durchführung, Kontrolle oder Beaufsichtigung der Durchführung der Sozialversicherungsgesetze beteiligt sind, gegenüber *Dritten* Verschwiegenheit zu bewahren haben. Und Art. 84a Abs. 5 lit. b KVG normiert, dass Organe, die mit der Durchführung des Krankenversicherungsgesetzes betraut seien, Personendaten in Abweichung von Art. 33 ATSG an Dritte bekannt geben dürfen, sofern die *betroffenen Personen im Einzelfall schriftlich eingewilligt* haben. Anders das Regime gemäss DSG, wonach gemäss Art. 19 Abs. 1 lit. b DSG Bundesorgane Personendaten nur bekannt geben dürfen, wenn hierfür eine Rechtsgrundlage besteht oder wenn die betroffene Person im Einzelfall eingewilligt hat.[1524] Das Bundesverwaltungsgericht hielt fest, dass die Helsana Versicherungs-AG, Progrès und Helsana Zusatzversicherungs-AG jeweils juristische Personen seien, weshalb es sich i. c. um eine Bekanntgabe an Drittpersonen handle.[1525] Mit anderen Worten wurde eine daten-

1522 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 4.5.5.
1523 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.4.
1524 Kritisch zum Paradigma der Eigenverantwortung und Selbstbestimmung in diesem Kontext Pärli, SZS 2018, 107 ff.
1525 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 4.8.2.

schutzrechtliche «Konzernprivilegierung» abgelehnt. Die Bekanntgabe der Personendaten aus der obligatorischen Krankenpflegeversicherung erfolge nicht in Ausübung einer durch das KVG übertragenen Aufgabe; eine Ausnahme von der sozialversicherungsrechtlichen Verschwiegenheitspflicht gemäss Art. 84a Abs. 1–4 KVG liege nicht vor. Folglich sei eine Datenbekanntgabe nur unter den *kumulativen Voraussetzungen von Art. 19 DSG und Art. 84a Abs. 5 lit. b KVG zulässig*. Die Nutzungs- und Datenschutzbestimmungen von Helsana+ beinhalten weder eine explizite Einwilligung in die Bekanntgabe von Personendaten aus der obligatorischen Krankenpflegeversicherung an die Beklagte, noch werde erwähnt, dass die Einwilligung auch für Bearbeitungen durch andere Personen als die Beklagte gelte – nämlich weitere Versicherungsgesellschaften. Demnach liege keine transparente Information i. S. v. Art. 4 Abs. 5 DSG vor. Zudem sei die Information betreffs Verarbeitungszweck unzureichend: Die Teilnehmerinnen und Teilnehmer könnten nur schwer erkennen, in welche Datenverarbeitung sie einwilligen. Somit läge keine angemessene Informiertheit als Voraussetzung der gültigen Einwilligung gemäss Art. 4 Abs. 5 DSG vor. Ebenso wenig erfolge die Einwilligung in die Datenbekanntgabe durch die obligatorische Krankenpflegeversicherung im Einzelfall, wie in Art. 19 Abs. 1 DSG und Art. 84a Abs. 5 lit. b KVG gefordert. Zudem werde die Formvorgabe der Schriftlichkeit gemäss Art. 84a Abs. 5 KVG nicht eingehalten.

1129 Im *Ergebnis* befand das Bundesverwaltungsgericht, dass eine gültige Einwilligung in die Bekanntgabe von Personendaten aus der obligatorischen Krankenversicherung an Dritte fehle und damit auch eine Verletzung des Rechtmässigkeitsgebotes i. S. v. Art. 4 Abs. 1 DSG sowie eine widerrechtliche Persönlichkeitsverletzung vorliege. Das erste Rechtsbegehren wurde insofern gutgeheissen, als die Beklagte im Rahmen des Programmes Helsana+ die Entgegennahme und Weitergabe von Personendaten der Helsana Grundversicherung zu unterlassen habe. Abgewiesen wurde das Rechtsbegehren, den Beklagten zu verbieten, Einwilligungen einzuholen.

1130 Der Entscheid verleiht dem Datenschutzrecht *de lege lata* unbestritten Nachdruck, wobei die Ausführungen zur Zweckbindung, Rechtmässigkeit sowie zu den Einwilligungsvorgaben richtungsweisend sind. Bemerkenswert sind namentlich auch die Argumentationsstränge des Bundesverwaltungsgerichts, mit denen die Vorgaben der Spezialgesetzgebung und damit die Vorgaben aus dem Kontext der obligatorischen Krankenversicherung, die in erster Linie für die Grundversicherung einschlägig sind, über das DSG auch für einen Zusatzversicherer relevant werden. Die Argumentation des Bundesverwaltungsgerichts führt zu einer Konstruktion, die sich als eine Art datenschutzrechtlicher Durchgriff beschreiben liesse. Die Einhaltung spezialgesetzlicher Datenschutzvorgaben wird nicht nur durch den direkten Adressaten – die Anbieter der obligatorischen Kranken- und

Grundversicherung – verlangt. Vielmehr ist sie auch durch die Zusatzversicherung beachtlich. Mit einer solchen weiten Auslegung der allgemeinen Verarbeitungsgrundsätze des DSG unter Inklusion der für den Kontext der obligatorischen Krankenversicherung geltenden datenschutzrechtlichen Spezialbestimmungen verleiht das Bundesverwaltungsgericht der systemischen Schutzdimension des Datenschutzrechts Nachachtung. Ein Rückzug auf die tradierte Anknüpfung im Subjekt- und Persönlichkeitsschutz bleibt gleichwohl präsent: Das Bundesverwaltungsgericht hält fest, dass ein Verstoss gegen das Rechtmässigkeitsprinzip gemäss DSG nur dann vorliege, wenn eine Norm ausserhalb des DSG verletzt werde, die direkt oder indirekt zumindest auch dem Schutz der Persönlichkeit diene.[1526]

2.2.2.3. Zusammenfassende Schlussfolgerungen

Die datenschutzrechtliche Judikatur inklusive ihrer Entwicklungen und der Beiträge, die sie für die Effektuierung des eidgenössischen Datenschutzgesetzes leistet, lässt sich nach dieser kursorischen Darstellung wie folgt *resümieren*: 1131

Erstens wird dem Datenschutzrecht und spezifisch dem Datenschutzgesetz für den öffentlichen Bereich bislang mehr Beachtung zugemessen als demjenigen für den privaten Bereich. 1132

Zweitens wird im privatrechtlichen Bereich die Durchsetzung des Datenschutzrechts von Gesetzes wegen *primär auf die Schultern der Individuen* gelegt. Allerdings sind persönlichkeits- und individualrechtliche Klagen sowie Urteile nach Verstössen gegen das Datenschutzgesetz Raritäten. Wenn indes die Durchsetzung der Rechtseinhaltung primär individualrechtlich konzipiert ist, diese jedoch kaum effektuiert wird, liegt darin ein Schwachpunkt der aktuellen Datenschutzgesetzgebung und des Durchsetzungsinstrumentariums. Das Vakuum wird weiter akzentuiert, wenn der EDÖB nur beschränkt kompensierend agieren kann, weil er limitierte Kompetenzen wie auch Ressourcen hat. Der Schwachpunkt wird immerhin mit der Totalrevision etwas beseitigt; zudem werden die durch die kantonalen Behörden verhängbaren Bussen markant verschärft. 1133

Einen Beitrag zur Effektuierung des Datenschutzrechts im privaten Bereich haben – *drittens* – die Empfehlungen des EDÖB wegen Systemfehlern mit allfällig folgenden Bundesverwaltungsgerichts- und Bundesgerichtsentscheiden geleistet. In der vergangenen Dezennie lässt sich insofern eine Intensivierung der Behördenaktivität verzeichnen. Der EDÖB intervenierte vermehrt mit Empfehlungen und setzte missachtete Empfehlungen konsequenter auf gerichtlichem Wege durch. Die Empfehlungen und Gerichtsentscheide dokumentieren eine zusehends ernst- 1134

1526 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018, E 5.4.2.

hafte Auseinandersetzung mit dem Datenschutzrecht und seiner Anwendbarkeit. Den Empfehlungsaktivitäten des EDÖB bei Systemfehlern und der gerichtlichen Durchsetzung kommt entsprechend *Signalwirkung* für die Bedeutung des Datenschutzrechts zu. In Anbetracht der Relevanz von Personendatenverarbeitungen müssen jedoch selbst diese datenschutzrechtlichen Durchsetzungsaktivitäten vonseiten der Schweizer Behörden als Einzelfälle bezeichnet werden.

1135 *Viertens:* Die bislang ergangenen behördlichen Empfehlungen und Entscheidungen des Bundesverwaltungsgerichts leisten zwar durchaus einen Beitrag zur Konsolidierung der datenschutzgesetzlichen Vorgaben sowie allfällig ebenso anwendbarer spezialgesetzlicher Bestimmungen. Aus einer materiellrechtlichen Perspektive lassen sich folglich gerade den Empfehlungen des EDÖB und den Entscheidungen des Bundesverwaltungsgerichts gewisse Leitlinien für die Auslegung der generalklauselartigen Datenverarbeitungsgrundsätze, die Hierarchisierung von Rechtfertigungsgründen, aber auch die Einwilligungsvorgaben entnehmen. Gleichwohl sind die bislang ergangenen Entscheidungen nicht in der Lage, Antworten auf die zahlreichen Auslegungsfragen zu geben, die sich im Zusammenhang mit einem generalklauselartigen Regime stellen.

1136 Ein datenschutzrechtliches Regime, in welchem die *Demarkationslinien der prinzipiellen Verarbeitungsfreiheit durch generalklauselartige Bearbeitungsgrundsätze gezogen* werden, ist jedoch, *fünftens*, unter dem Titel seiner Effektuierung problematisch.[1527] Im Ergebnis laufen die Entscheide zudem nicht selten auf eine *Interessenabwägung im konkreten Einzelfall* hinaus. Wenn das DSG für den privaten Bereich in erster Linie mittels Generalklauseln *die* entscheidenden Vorgaben zulässiger Datenverarbeitungen formuliert, diese indes durch die rechtsanwendenden Behörden nur punktuell konkretisiert werden, erstaunt es nicht, wenn die Adressaten dieser Generalklauseln des DSG sich auf eine gewisse Orientierungslosigkeit bei der Umsetzung des DSG berufen. Die datenschutzgesetzlichen Generalklauseln entbehren über weite Strecken der notwendigen konkretisierenden und strukturierenden Rechtsprechung (und Lehre). Dies ist der faktischen Einhaltung der datenschutzgesetzlichen Vorgaben in der Praxis abträglich.

1137 Die vonseiten der Behördenpraxis eher rudimentär generierte Strukturierungswirkung für das DSG im privaten Bereich darf und muss, *sechstens*, als Ausdruck dessen gelesen werden, dass der Datenschutz in der Schweiz lange nicht als prioritäres Anliegen interpretiert wurde.[1528] Mit den jüngsten datenschutzrechtlichen

1527 Bekanntermassen kommt im Rahmen der Auslegung gerade auch von Generalklauseln und unbestimmten Rechtsbegriffen der Rechtsprechung und Lehre eine entscheidende Rolle zu, vgl. auch Art. 1 ZGB.

1528 Deutlich wird dies wohl auch in den Versäumnissen vonseiten des Gesetzgebers mit Blick auf die Totalrevision des DSG; diese Position erstaunt im Lichte auch der Entwicklungen in der EU aufgrund der DSGVO, aber auch für eine Gesellschaft, die Daten als das neue Gold und sich selbst als Informationsgesellschaft bezeichnet.

Neuerungswellen ändert sich dies allerdings. Nach bisherigem Regime ist zudem in Erinnerung zu rufen, dass der EDÖB eher mit bescheidenen Ressourcen auszukommen hat. Weil unter dem aktuellen Regime das Risiko datenschutzrechtlicher Konsequenzen in der Schweiz *de lege lata gering ist,* resultiert hieraus kaum ein Anreiz, der Datenschutz-Compliance in der Unternehmenspraxis hohe Bedeutung zuzumessen. Inwiefern die Neuerungen qua Totalrevision mit der Neuordnung der Kompetenzen des EDÖB, aber auch dem verschärften strafrechtlichen Bussenkatalog hier eine Änderung bringen, wird sich weisen müssen.

Siebtens hat die Behördenpraxis nicht unwesentlich zu einer gewissen Verwirrung beigetragen, was Schutzobjekt und -gegenstand resp. Schutzkonzept des Datenschutzgesetzes der Schweiz anbelangt. Wird in der Judikatur von einem *Herrschaftsrecht* des Datensubjektes gesprochen, suggeriert dies einen Rechtsbestand, der in der Schweiz gesetzlich nach DSG nicht garantiert wird.[1529] Wenn in der Behördenpraxis die Idee eines Rechts auf informationelle Selbstbestimmung in Umlauf gebracht wird, mit welcher das Zustimmungsrecht des Einzelnen assoziiert wird, werden in der Gesellschaft falsche Erwartungen geweckt. Das DSG verbürgt für den privatrechtlichen Bereich gerade kein informationelles Selbstbestimmungsrecht. Geht man dennoch und dann fälschlicherweise von einem solchen Rechtsbestand aus, resultiert hieraus ein weiteres Risiko, welches auch die künftige Weiterentwicklung des Datenschutzrechts blockieren kann: Wird in einem Regime der Selbstbestimmung ein Wirkungsdefizit attestiert, liegt die Schlussfolgerung nahe, dass es das *«unbedachte» Datensubjekt* ist, dem die Verantwortung für die fehlende Wirksamkeit des Datenschutzrechts zugewiesen wird – ein Fehlschluss, wie in dieser Arbeit an verschiedenen Stellen sichtbar wurde und weiter sichtbar werden wird. 1138

Der kursorische Blick auf die Frage, ob und inwiefern das Datenschutzrecht in der Schweiz durch die Behördenpraxis effektuiert wird, zeigte – *achtens* – die *systemische Dimension datenschutzrechtlicher Herausforderungen*. Der EDÖB interveniert mit einer Empfehlung bei sog. Systemfehlern. Solche werden dann angenommen, wenn Personendatenverarbeitungen eine Vielzahl von Personen betreffen. Der Begriff des Systemfehlers wird in quantitativer Weise konkretisiert. Damit ist die Frage entscheidend, ob viele Personen von einer Bearbeitungsmethode betroffen sind. Gleichwohl lässt sich in dieser Konstruktion erneut die systemische Dimension feststellen, womit die insofern ergehenden behördlichen Entscheidungen in einer weiteren resp. ergänzenden Weise zu lesen sind: Es geht in der Regel um Kollisionen zwischen verschiedenen gesellschaftlichen Bereichen infolge bestimmter Personendatenflüsse. Gerade dieses prozedurale Instrumentarium der Empfehlungen des EDÖB infolge von Systemfehlern mit der Weiter- 1139

1529 Vertiefend hierzu zweiter Teil, VI. Kapitel, B.2., insb. 2.2.

zugsmöglichkeit an eine gerichtliche Instanz ermöglichte es, den fragmentierenden Blick auf das einzelne Subjekt und das Personendatum als Quasi-Objekt zu überwinden.

1140 Wenn nun der Effektuierung des Datenschutzgesetzes durch die schweizerische Behördenpraxis ein durchzogenes Attest ausgestellt wurde, welche Bedeutung wird dem Datenschutz in den Medien sowie in der politischen Debatte zugemessen?

3. Die Bedeutung der Medien für den Datenschutz

1141 Die Liaison zwischen den Medien und dem Datenschutz ist – erinnert man sich an den bereits diskutierten Beitrag von Warren/Brandeis[1530] – eine lange, komplexe und ambivalente Beziehung: Präsentierten sich dazumal die Medien als *Verletzer der Privatheit*, sind sie heute gleichzeitig *Garant sowie Gegenspieler* datenschutzrechtlicher Anliegen. In der aktuellen Medienberichterstattung nehmen Themen des Datenschutzes und der Digitalisierung einen *zentralen Platz* ein.[1531] Die mediale Landschaft hat sich im Zuge der datenschutzrechtlichen Neuerungswellen weiter verändert.

1142 Gerade auch das Inkrafttreten der DSGVO im Mai 2016 und der Ablauf der Umsetzungsfrist im Mai 2018 sowie die seither erlassenen behördlichen Massnahmen und Sanktionen führten zu einer Intensivierung der medialen Berichterstattung.[1532] In der Schweiz wird sodann die Totalrevision des DSG auch medial zur Kenntnis genommen, was zu einer Sensibilisierung der Allgemeinheit führt. In den Medien spiegelt sich, dass dem Datenschutzrecht und seiner Einhaltung heute eine neue Bedeutung zugemessen wird – es ist die Rede von einer Zeitenwende. Der kursorische Blick über die Medienberichterstattung zum Datenschutzrecht lässt mit Blick auf das Ziel, die Einhaltung des Datenschutzrechts zu effektuieren, bereits Erfolge erkennen.[1533]

1530 Vgl. Warren/Brandeis, Harv. L. Rev. 1890, 193 ff.

1531 Müller, NZZ vom 14. Juli 2017, EU-Datenschutzverordnung tangiert auch die Schweiz, <https://www.nzz.ch/wirtschaft/folgen-der-neuen-datenschutz-grundverordnung-eu-datenschutzverordnung-tangiert-auch-die-schweiz-ld.1306009> (zuletzt besucht am 30. April 2021); Städeli, NZZ am Sonntag vom 03. Februar 2018, Die EU schützt die Privatsphäre ihrer Bürger – davon profitieren auch Schweizer, <https://nzzas.nzz.ch/wirtschaft/eu-schuetzt-privatsphaere-buerger-davon-profitieren-schweizer-ld.1353937?reduced=true> (zuletzt besucht am 30. April 2021); Zeit online, DSGVO, Hamburg 2021, <https://www.zeit.de/thema/dsgvo> (zuletzt besucht am 30. April 2021).

1532 Gesprochen wird von einer «Zeitenwende», vgl. Nuspliger, NZZ vom 17. Mai 2018, <https://www.nzz.ch/international/eu-datenschutz-was-sie-ueber-die-zeitenwende-wissen-muessen-ld.1384889> (zuletzt besucht am 30. Mai 2021).

1533 Vgl. zur Busse der CNIL gegenüber Google: FAZ vom 21. Januar 2019, DSGVO-Busse für Google in Frankreich, <https://www.faz.net/aktuell/wirtschaft/diginomics/google-muss-dsgvo-busse-in-millionenhoehe-zahlen-16000661.html> (zuletzt besucht am 30. April 2021); zur Busse gegenüber Knuddels: Budras/Jansen, FAZ vom 22. November 2018, Datenschützer bestrafen massenhaften Datenklau, <https://www.faz.net/aktuell/wirtschaft/diginomics/dsgvo-datenschuetzer-bestrafen-mass

Bis zu diesem von der DSGVO angestossenen Paradigmenwechsel im Datenschutzrecht nahmen die Medien eine andere, eine kompensierende Rolle wahr. Pointiert artikulierte es im Jahr 2003 Vesting. Der Medienrechtswissenschaftler bezeichnete «das mediale Rauschen» als die *Hauptwirkung des Datenschutzes*.[1534] Mit der DSGVO und der Totalrevision des DSG, der Einhaltung des Datenschutzrechts durch die Einführung von Umsetzungsinstrumenten, dem Ausbau prozeduraler und organisatorischer Massnahmen sowie der Verschärfung und der Erweiterung möglicher behördlicher Massnahmen dürfte sich die Lage entsprechend ändern. 1143

In den Jahren vor der jüngsten Datenschutzrechtsrevisionswelle, in denen das Vollzugs- und Einhaltungsdefizit des Datenschutzrechts zusehends medial problematisiert wurde, hatten die *Medien auch eine Auffang- oder Kompensationsrolle:* Das *Reputationsrisiko* infolge einer «negativen Presse» wurde und wird (noch) vonseiten der personendatenverarbeitenden Unternehmen in der Schweiz als deutlich höheres Risiko eingeschätzt als die Konfrontation mit einer persönlichkeitsrechtlichen Klage oder einer Empfehlung vonseiten des EDÖB.[1535] 1144

Weil Datenschutz aufs Engste mit *Vertrauen* korreliert und die individualrechtlichen Instrumente nur rudimentär greifen, ist der Schritt an die *Medien* effizient, um namentlich Privatunternehmen in die Verantwortung zu nehmen. Die Medienberichterstattung über digitale Kanäle vermag zugleich einen äusserst breiten Adressatenkreis zu erreichen. Wegen Datenschutzverletzungen medial angeprangert zu werden, zeitigt in aller Regel auch wirtschaftliche Konsequenzen. Denn Menschen ist der Datenschutz wichtig, womit Entscheidungen, beim wem sie welche Produkte oder Dienstleistungen beziehen, ebenso von dem durch den Anbieter gewährleisteten Datenschutz mit abhängen dürfte. 1145

Wenn sich auch die kompensatorische Rolle der Medien in Anbetracht des (künftigen) wirksameren Rechts, wie es die DSGVO resp. nDSG bringt, abschwächen dürfte, bleibt sie gleichwohl bis heute erhalten – noch heute ist aus den unzähligen Medienberichten zu Datenschutz- und Datensicherheitsverstössen zu schliessen, dass das Datenschutzrecht unter einem Einhaltungs- und Durchsetzungsdefizit litt und weiterhin leidet. 1146

Mit der intensiven medialen Thematisierung des Datenschutzes wird seine *hohe Bedeutung in der und für die Gesellschaft* dokumentiert. Wenn auch manchmal polemisch, so illustrieren die mittlerweile beinahe täglich erscheinenden Berichte 1147

---

enhaften-datenklau-15903347.html> (zuletzt besucht am 30. April 2021); zu den zahlreichen Meldungen von Datenschutzverstössen, aber nur wenigen Bussen Jochum, Inside-It vom 7. Februar 2019, DSGVO: Viele Meldungen, wenig Bussen, <https://www.inside-it.ch/articles/53585> (zuletzt besucht am 30. April 2021).

1534 Vesting, in Ladeur (Hrsg.), 155 ff., 182.

1535 Zu den Änderungen qua Totalrevision DSG resp. DSGVO vertiefend dritter Teil, VIII. Kapitel, A.

über immer weiter greifende Datenerhebungen und -bearbeitungen, Datenschutzpannen, über Datendiebstahl und -handel, über Manipulationen sowie Überwachungsskandale die Aktualität sowie Dringlichkeit der Herausforderungen.[1536]

1148 Das Thema bewegt und beschäftigt die Menschen und die Allgemeinheit tiefgreifend. Die mediale Berichterstattung widerlegt die Meinung, wonach Datenschutz für die heutige Gesellschaft und die Menschen des 21. Jahrhunderts irrelevant geworden ist. Vielmehr zeigt sich mit ihr, dass Datenschutz ein *gesellschaftlich eminent wichtiges Thema* ist. Ebendies reflektiert eine Gesellschaft, die als Informationsgesellschaft resp. digitale Gesellschaft beschrieben wird.[1537] Zudem zeigt die Berichterstattung die facettenreichen Aspekte der Relevanz und Einschlägigkeit des Datenschutzes.[1538]

1149 Der Datenschutz zeigt sich in der Medienberichterstattung als eines der Sorgenkinder der digitalisierten Gesellschaften des 21. Jahrhunderts: Die Grossmehrheit der Berichterstattungen ist hinterfragend, beunruhigend und beunruhigt, entrüstet in Anbetracht der Nichteinhaltung datenschutzrechtlicher Vorgaben, zu lascher Gesetzgebungen und ungenügender Sanktionierungen. Einen prominenten Platz nehmen veritable Datenskandale sowie kriminelle Machenschaften ein. Dies sei anhand einiger ausgewählter Beispiele illustriert:

1150 Intensiv thematisiert wurden mutmassliche *Manipulationen im US-amerikanischen Präsidentenwahlkampf*. Berichtet wurde, dass über Facebook generierte Personenangaben an Cambridge Analytica gelangten, dort ausgewertet wurden, um alsdann gezielt auf den US-amerikanischen Wahlkampf einzuwirken.[1539] Cambridge Analytica habe mittels Algorithmen Personen ermittelt, die in ihrer Position potentiell schwankend gewesen seien und die für eine Wahl von Trump hätten gewonnen werden können. In der Folge wurden den betroffenen Personen passgenaue Nachrichten zugespielt, die namentlich auch die Gegenkandidatin resp. deren Programm herabsetzten. Entsprechende Nachrichten erfolgten gänz-

1536 Vgl. statt vieler Noser, NZZ vom 3. Februar 2016, 12; zur «datensammelnden Krake» privater Unternehmen Die Zeit vom 11. November 2010, 45 f.; zum «Sack voller Wanzen» in Gestalt der Mobiltelefone NZZ vom 28. April 2011, 57; sodann Der Spiegel vom 11. Januar 2010; zur Kritik an exzessiver Datensammlung beim Staatsschutz in der Schweiz NZZ vom 23. Oktober 2010, 13; zu Reputation und Privatsphäre im Internet NZZ am Sonntag vom 16. September 2012, 38; zum Diebstahl geheimer Daten NZZ vom 27. September 2012, 9 sowie NZZ vom 28. September 2012, 1; Handelszeitung vom 20. November 2015; für eine Zusammenstellung medialer Berichterstattung vgl. Pressespiegel des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten.

1537 Zum Informationsrecht der Informationsgesellschaft zu Beginn dieses Jahrtausends aufschlussreich bereits Dreier, in: Bizer/Lutterbeck/Riess (Hrsg.), 65 ff., dessen Beitrag bereits unter dem Titel der Governance steht.

1538 Vgl. auch Rosenthal, in: Passadelis/Rosenthal/Thür (Hrsg.), § 7 N 7.77 ff.

1539 Vgl. Spiegel, Cambridge-Analytica-Skandal, Zahl der Geschädigten deutlich höher als bekannt, Hamburg 2018, <http://www.spiegel.de/netzwelt/web/facebook-skandal-daten-von-87-millionen-nutzern-betroffen-a-1201288.html> (zuletzt besucht am 30. April 2021); vgl. auch den Beitrag «Fake America great again», abrufbar unter: <https://vimeo.com/471514311> (zuletzt besucht am 20. September 2021); vgl. Egli/Rechsteiner, AJP 2017, 249 ff.

lich im «Dunkeln» und auf intransparente Weise. Die Strategie von Cambridge Analytica, sich auf Schlüsselstaaten und ebenda auf Unentschlossene zu konzentrieren und auf diese gemäss ihres digitalen Fussabdruckes einzuwirken, wurde als erfolgreich beurteilt: Eine Dokumentarsendung – ausgestrahlt auf Arte – problematisierte, wie Facebook mit den sich hinter dem sozialen Netzwerk abspielenden Praktiken die *Demokratie gefährden würde*. In besagtem Bericht führte die Journalistin Cadwalladar aus, dass Informationstechnologien nicht nur disruptive Wirkungen auf die Zeitungen und den Journalismus gezeitigt hätten. Nunmehr würden sie darüber hinausgehend auch die Politik und damit die Demokratie zerstören. Ein ähnlicher Prozess wurde sodann im Zusammenhang mit dem Brexit problematisiert, wobei wiederum Beeinflussungen und Interventionen durch und über Cambridge Analytica medial thematisiert wurden.[1540] Seither wurde wiederholt vor der Einwirkung auf Wahlen und Abstimmungen sowie politische Prozesse über soziale Netzwerkegewarnt.

Weiter wurde in den letzten Jahren über mutmassliche Hackerangriffe auf das Handy der deutschen Bundeskanzlerin und Trojaner, die selbst ihren Computer infiziert hätten, berichtet.[1541] 1151

Prominent tauchten in den Medien sodann die NSA und Edward Snowden auf, der als vormaliger CIA-Mitarbeiter und Whistleblower über das Ausmass geheimer Überwachungsmassnahmen durch die Geheimdienste in den USA sowie Grossbritannien berichtete.[1542] 1152

In der Schweiz sorgte der Fichenskandal von 1989 für einen öffentlichen Aufschrei. 2010 führte erneut das Vorgehen des Staatsschutzes für etwas Aufruhr, wobei die Benennung (mit Fragezeichen) als «Skandal» auftauchte.[1543] 2017 zog sodann ein angeblich von der Schweiz nach Deutschland entsandter «Maulwurf» die öffentliche Aufmerksamkeit auf sich – er kam ans Licht und wurde bei seiner Mission, Steuerdaten zu erheben, wegen Spionageverdachts gefasst.[1544] Die datenschutzrechtlich relevanten Datenbeschaffungen und -manipulationen sind im *Bereich der «staatsgefährdenden» Aktivitäten und im (staats-)politischen* 1153

1540 Doward/Gibbs, The Guardian vom 4. März 2017, Did Cambridge Analytica influence the Brexit vote and the US election?, <https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump> (zuletzt besucht am 30. April 2021); aus entsprechenden Schilderungen ist gerade auch zu schlussfolgern, dass der Datenschutz weit über den Schutz des einzelnen Menschen hinausgeht, wie er sich in einer individualrechtlichen Konzeptionierung indes niederschlägt. In der dargelegten Situation sind keineswegs bloss die einzelnen Datensubjekte betroffen – darüber hinausgehend wird das demokratische und rechtsstaatliche System aufs Spiel gesetzt.

1541 Vgl. den Beitrag «Fake America great again», abrufbar unter: <https://vimeo.com/471514311> (zuletzt besucht am 20. September 2021).

1542 Vgl. z. B. die zahlreichen Artikel erschienen in der NZZ; lesenswert alsdann Snowden, Permanent Record, Fischer Verlag, 2019.

1543 Dazu Gugerli, Die Zeit vom 15. Juli 2010, Man merkt, wo die Post abgeht, <https://www.zeit.de/2010/29/CH-Fichenskandal> (zuletzt besucht am 30. April 2021).

1544 Vgl. NZZ vom 4. Mai 2017, 15; Die Zeit vom 4. Mai 2017.

Kontext angesiedelt. Sie werden traditionell mit dem öffentlichen Bereich assoziiert, wobei im Facebook-Skandal auch ein privater Akteur mitmischte. In der Presse spielen sie aktuell eine prominente Rolle.

1154 Auch aufseiten privatwirtschaftlicher Unternehmen wurden in den vergangenen Jahren mehrere Datenschutzvorfälle, Praktiken und Skandale von der Presse aufgegriffen. Im Jahr 2021 zum Beispiel das Leck bei Facebook.[1545] Die Deutsche Telekom GmbH war nicht nur «Opfer» eines Datendiebstahles im grossen Stil, bei dem rund 17 Millionen Daten entwendet wurden.[1546] Kurz darauf wurden auf dem Schwarzmarkt rund 4000 Festnetznummern mit passenden Kontonummern und Geburtsdaten der Inhaber feilgeboten. Weiter geriet die Deutsche Telekom in einer als Spitzelaffäre titulierten Angelegenheit in den Verdacht, Verbindungsdaten von Aufsichtsräten, Gewerkschaftsfunktionären sowie Journalistinnen gespeichert und ausgewertet zu haben.[1547] Der Discounter Lidl fand unter dem Titel des Datenschutzes Eingang in die Presse, wobei berichtet wurde, dass intime (gesundheitliche) Details über Mitarbeitende, wie etwa Schwangerschaftswünsche, systematisch dokumentiert wurden und Mitarbeitende am Arbeitsplatz mit Kameras illegal observiert wurden.[1548] So werden selbst und gerade in Deutschland, das als Datenschutzgewissen Europas gilt, problematische Datenverarbeitungspraktiken medial prominent thematisiert. Und auch für die Schweiz zeigt bereits der Blick auf die Seite des EDÖB und dessen Pressespiegel, der rund alle zwei Monate erscheint und für die Wochen 9–15 des Jahres 2017 über 40 Seiten umfasst, welch zentraler Stellenwert dem Datenschutz in den Medien zukommt.[1549]

1155 Die Publikumsmedien reflektieren zudem den *Facettenreichtum* sowie die *Komplexität* des Themas Datenschutz. Beide Aspekte geraten bei einer Fokussierung auf das DSG leicht aus dem Blickfeld. Zudem zeigt sich eine hohe Diversität an Fachrichtungen, aus denen sich Autorinnen und Autoren zum Thema äussern. Sie zeugen von den mannigfaltigen Aspekten, über die berichtet wird. Damit wird auch sichtbar, wie grundlegend und breit das Thema die Gesellschaft be-

1545 Vgl. EDÖB, Pressespiegel 2017, <http://www.kdsb.ch/documents/Pressespiegel09_15_17.pdf> (zuletzt besucht am 30. April 2021); Burghardt/Böhm/Buchmann et al., 3 ff.

1546 Vgl. <https://www.tagesschau.de/wirtschaft/unternehmen/facebook-nutzerdaten-101> (zuletzt besucht am 18. Juni 2021).

1547 M. w. H. Schiedermeier, 45 ff.

1548 Mit humoristischem Titel «Versteckte Kameras bei Lidl» berichtete darüber die NZZ am 11. September 2008, sodann <https://www.sueddeutsche.de/wirtschaft/lidl-muss-zahlen-millionen-strafe-fuer-die-schnueffler-1.709085> (zuletzt besucht am 30. April 2021); zu den datenschutzrechtlichen Grenzen von Mitarbeitendenüberwachungen, auch mit Hinweis auf die in den Schweizer Medien hohe Wellen schlagenden Observation eines Bankmanagers, Götz Staehelin/Bertschi, RR-VR 2020, 5 ff.; beachte zur Überwachung im Arbeitskontext EGMR Nr. 61496/08 – Bârbulescu/Romania, Urteil vom 12. Januar 2016.

1549 Vgl. EDÖB, Pressespiegel 2017, <http://www.kdsb.ch/documents/Pressespiegel09_15_17.pdf> (zuletzt besucht am 30. April 2021); Burghardt/Böhm/Buchmann et al., 3 ff.

schäftigt und wie umfassend sowie tiefgreifend Datenverarbeitungen und die Frage nach dem Schutz des Menschen – aber auch von Gesellschaftsbereichen – verhandelt werden. Informiert wird über die unzähligen Anwendungen neuer Informationstechnologien mit ihren Chancen, Risiken und Herausforderungen in den verschiedensten Feldern – vom Staatsschutz über das (elektronische) Patientendossier zur AHV-Nummer als einheitlichem Personen-Identifikator, von der Videoüberwachung im Nachbarschaftsverhältnis über den Einsatz von Drohnen zu Whistleblowing-Zwecken und Hackerangriffe, von der Identifizierung von Urheberrechtsverletzungen zu Google Street View, vom Minderjährigen-Datenschutz im Internet über die polizeilichen Überwachungs- und Analyseverfahren zur Ermittlung und Aufklärung von Straftaten oder dem Monitoring terroristischer Gefährdungen.[1550]

Damit fällt die *Breite* auf, in der das Thema aufgegriffen wird, sowohl bezüglich 1156
der Gefässe – von Computer- über Unterhaltungsmagazine und Tagespresse bis zu Filmen – als auch bezüglich der Autorenschaft. Vom Pfarrer bis zur Parlamentarierin, von Journalisten über Rechtsexperten zu Computerspezialistinnen – um nur einige zu nennen –, Personen verschiedenster Professionen nehmen sich des Themas an. Man mag dies zuweilen als Überschreitung von Kompetenzen abtun. Aufschlussreich hier die Charakterisierung von Drechsler, wonach – was den Datenschutz anbelangt – ausserordentlich viele «Fake News» kursieren.[1551] Sie können – ähnlich, wie es die Analyse der Behördenpraxis sichtbar machte – die Konsolidierung und Entwicklung des Datenschutzes und seines Rechts blockieren. Illustrativ hierfür ein Beitrag aus der NZZ, der mit beachtlicher Leichtigkeit strukturell verschiedene Datenschutzkonzepte in einem Dreizeiler vermengt:

> «Grundrecht auf informationelle Selbstbestimmung. Symbolische Datenschutzpolitik. Datenschützerische Anliegen erleben derzeit ein Hoch. Doch ob diese in der Praxis zu einem verbesserten Schutz der Privatsphäre beitragen, ist oftmals fraglich.»[1552]

Von welchem rechtlich verbürgten Schutzbereich soll nun die Leserschaft und 1157
Allgemeinheit nach der Lektüre einer solchen Passage ausgehen? Versteht man nicht bereits intuitiv und im nicht-juristischen Fachjargon Grundverschiedenes mit den Wendungen «Recht auf informationelle Selbstbestimmung» resp. «Garantie eines Privatsphärenschutzes»? Auch die Medienberichterstattung in der Schweiz zum Datenschutz vermittelt (ähnlich wie es für die Rechtsprechung attestiert wurde) kein kohärentes Bild der vom Datenschutz garantierten Rechtspositionen. Auch hier werden für die Schweiz in problematischer Weise falsche Vorstellungen sowie Erwartungen in Bezug auf datenschutzrechtliche Garantien

1550 Zur Videoüberwachung öffentlicher Bereiche Ruegg/Flückiger/November/Klauser, 3 ff.; zum elektronischen Patientendossier das einschlägige Spezialgesetz do Canto, sic! 2020, 177 ff., 181 ff.
1551 Drechsler, Workshop, 24. Mai 2018.
1552 Hofmann, NZZ vom 11. September 2014.

geweckt, was auch die Fortentwicklung des Datenschutzrechts *de lege ferenda* erschwert.

1158 Gleichwohl ist – im Sinne eines Einschubes – festzuhalten, dass die Bewältigung datenschutzrechtlicher Anforderungen nur durch das Zusammenwirken von Vertreterinnen und Vertretern verschiedenster Fachdisziplinen erfolgen wird. Das gilt *a fortiori* für den in dieser Arbeit entwickelten Ansatz eines Rechts auf informationellen Systemschutz. Die Verwirklichung des Datenschutzes benötigt nicht nur juristische sowie technologische Expertise, sondern auch ausgeprägtes organisatorisches sowie prozedurales Denken. Zudem ist das Verständnis für gesellschaftliche Fragen und die Gesellschaftsbereiche, inklusive ihrer rechtlichen Rahmenbedingungen relevant.

1159 Zurück zur medialen Berichterstattung und zum Datenschutzrecht. Zahlreiche Datenschutz(rechts)experten und -expertinnen melden sich medial zu Wort.[1553] Namentlich bei den nicht nur in Fachzeitschriften publizierenden Juristinnen und Juristen weist die grosse Zahl der auf das Datenschutzrecht spezialisierten Personen eine *feste Basis in der Praxis* und hierbei in der wirtschaftsrechtlich ausgerichteten Advokatur auf. Die datenschutzrechtliche Debatte wurde lange nicht unwesentlich in den Publikumsmedien geführt. Akademisch zog das Thema lange wenig Aufmerksamkeit auf sich. Immerhin haben die jüngsten Revisionsbewegungen in der EU, aber auch die Totalrevision des DSG in der Schweiz hier eine Intensivierung des wissenschaftlichen Interesses am Thema ausgelöst.

1160 In den Publikumsmedien sind und bleiben die Einschätzungen vonseiten der Expertinnen und Experten zugleich *kritisch* wie *kontrovers*. Ein Gastbeitrag in der NZZ vom 3. Mai 2017 von Rosenthal steht zwar unter dem Titel «Revision des Datenschutzgesetzes. Eine Mogelpackung». Der Autor kritisiert die geplanten Instrumente als «aufgeblasen», da diese bloss eine (formelle) Erhöhung des Schutzes suggerieren würden.[1554] In der Realität indes werde dieser Schutz nicht zu bewerkstelligen sein. Rosenthal legt damit auch im Rahmen einer Stellungnahme zu den Revisionsvorhaben seinen Finger in die Wunde des Datenschutzes: dessen faktische Umsetzung. Seine kritische Haltung zur faktischen Verwirklichung formalrechtlich verbürgter Garantien fasst er in wenigen Worten wie folgt zusammen:

> «Das häufige Argument, dass wir nachziehen müssen, damit uns die EU weiterhin als Land mit angemessenem Datenschutz anerkennt, halte ich für Angstmacherei. Die Schweiz hat ein sehr gutes Datenschutzniveau und ein Gesetz, um das wir im Ausland

1553 Geiser/Uttinger, NZZ vom 8. März 2017; Passadelis, NZZ vom 17. Mai 2017 und NZZ vom 7. November 2019; Thouvenin, Blick vom 12. September 2018.

1554 In dieser Arbeit allerdings wird vertreten, dass mehrere dieser Instrumente gerade auch darauf abzielen, den Datenschutz in der Realität griffiger zu machen, so beispielsweise das Verarbeitungsverzeichnis, aber auch die Dokumentations- und Rechenschaftspflichten.

> wegen seiner Vernunft beneidet werden. Der Vorentwurf ist ebenfalls erfreulich schlank. In dem Bereich, in welchem das DSG heute tatsächlich missbraucht wird, dem Auskunftsrecht, wurde aber nichts getan. Es wird heute primär dazu genutzt, vor einem Prozess die Gegenseite ohne Kostenrisiko auszuforschen. So profitiert meine Berufsgattung auch da weiterhin».[1555]

Das Schweizer Datenschutzrecht und namentlich das DSG werden in den Publi- 1161
kumsmedien oft mit den beiden Kategorien «zu viel» und «zu wenig» beschrieben. Damit erscheint die Rechtsmaterie erneut als eine, die zwischen zwei Polen aufgespannt wird und bipolar gedacht wird im Sinne von öffentlich (contra Datenschutz) und privat (pro Datenschutz). Allerdings ist das Rechtsgebiet eines, das *differenzierter* zu debattieren ist. In das Zentrum der Aufmerksamkeit haben die Fragen zu rücken, welche Schutzzwecke das Datenschutzrecht zu erfüllen hat und welche Instrumente geeignet sind, identifizierte Schutzzwecke effektiv zu erreichen.

Indikativ dafür, dass die datenschutzrechtlichen Herausforderungen facettenrei- 1162
cher sind und nicht pauschal mit der Frage nach zu viel oder zu wenig beantwortet werden können, sind die *diversifizierten Hintergründe der Autorinnen und Autoren*. Das Datenschutzrecht als Querschnittsmaterie ist keine isolierte Materie. Das ist auch gemeint, wenn das Datenschutzrecht als *Querschnittsmaterie* bezeichnet wird. Vielmehr ist es eine Normierung, die sich über zahlreiche Kontexte, Institutionen und Bereiche erstreckt. Teilweise wird sie übersteuert über Sonderregeln und Spezialerlasse. Damit zeigt sich in der Breite des Personenkreises, der sich zum Datenschutzrecht äussert, dass dieser für ganz *unterschiedliche Kontexte mit ihren Vertreterinnen und Vertretern relevant* ist.[1556] So hat sich beispielsweise die Institution der Kirche seit jeher um die Personendatenerfassung und auch den Schutz von Informationsflüssen mit dem Beichtgeheimnis gekümmert, wie der historische Teil zeigte. Die informationellen Praktiken dienten der Konsolidierung des Systems, einer Institution sowie der Abgrenzung von anderen Systemen, namentlich dem säkularen, sprich staatlichen Bereich.[1557] Noch heute äussern sich auch Pfarrer medial zum Datenschutz.

Im Zusammenhang mit der Einschlägigkeit diverser Kontexte und ihrer Abgren- 1163
zung nimmt ebenso in den Medien die Thematisierung der expansiven Kraft *wirtschaftlicher Begehrlichkeiten im Umgang mit Personendaten* viel Platz ein. Hierzu nur einige Titel: «Swisscom sait tout de vous et revend vos données à

1555 Rosenthal, NZZ vom 3. Mai 2017.

1556 Richtungsweisend zur Einschlägigkeit des Kontextes für den Datenschutz Nissenbaum, 1 ff. Das Kriterium wurde im Laufe dieser Schrift bereits an verschiedenen Stellen beleuchtet und wird insb. in diesem dritten Teil im IX. Kapitel als neues Leitkriterium resp. Paradigma für die Weiterentwicklung des Datenschutzrechts elaboriert werden.

1557 Kuse, SRF online, Wort zum Sonntag, Der gläserne Bürger – von Daten und Macht, Zürich 2015, <https://www.srf.ch/play/tv/wort-zum-sonntag/video/der-glaeserne-buerger---von-daten-und macht?urn=urn:srf:video:6c903f8c-bd28–43d0–913f-dbae701e3f2a> (zuletzt besucht am 30. April 2021).

des fins commerciales»[1558], «Swisscom-Raubzug auf persönliche Daten».[1559] Cineastisch wurde die Übergriffigkeit des Marktes eindrücklich im Kurzfilm «Das innere Auge» von Achim Wendel dargestellt. Es handelt sich um die Geschichte eines Mannes, der sich entscheidet, an einem Marketingexperiment teilzunehmen: Ein Chip wird in sein Gehirn eingesetzt. Damit können Informationen zu Strömungen, Befindlichkeiten und Begehrlichkeiten direkt an ein Marketingunternehmen übermittelt werden. Heute wird längst nicht mehr nur vom gläsernen Bürger gesprochen, vielmehr gibt es auch den gläsernen Konsumenten, die gläserne Sportlerin, die gläserne Versicherungsnehmerin und – in der Schweiz – jüngst den gläsernen Bauern.[1560]

1164 Der Topos der «gläsernen Person» verleitet dazu, den Fokus wiederum auf das einzelne Subjekt zu richten und dahinterstehende Kollisionen von Bereichen und namentlich der expansiven Tendenz ökonomischer Begehrlichkeiten zu übersehen. Es lohnt sich, nochmals an Warren/Brandeis zu erinnern. Die Autoren haben eindringlich den Schutz der heiligen Bezirke eines persönlichen Lebensbereiches gegenüber dem puren Profitstreben seitens der Presse zur Befriedigung primitiver Neugierde der Allgemeinheit gefordert. Mit einer solchen, über das einzelne Subjekt hinausgehenden Dimension datenschützerischer Herausforderungen sowie den tiefgreifenden Auswirkungen von Personendatenverarbeitungsprozessen auf etablierte gesellschaftliche Strukturen und Institutionen lässt sich unter Umständen der *markante Duktus* in der Medienberichterstattung zum Datenschutz erklären.[1561]

1165 Allgemein fällt für die Thematisierungen rund um das Private und den Datenschutz die *bildstarke und emotionale Rhetorik auf*. Zu dieser De Maizière im

1558 Le Matin Dimanche vom 2. April 2017.

1559 Saldo vom 15. März 2017.

1560 NZZ vom 7. Juni 2019, 13; http://www.haufe.de/recht/deutsches-anwalt-office-premium/zfs-08200 8-der-glaeserne-kraftfahrer-4-private-datenmacht_idesk_PI17574_HI2764028.html (zuletzt besucht am 30. April 2021); auch wissenschaftlich werden die Figuren thematisiert, z. B. der gläserne Sportler, durch Buchner, DuD 2009, 475 ff.; zum gläsernen Konsumenten Weichert, DuD 2003, 161 ff.; zum gläsernen Kunden Eckhardt/Fattebert/Keel/Meyer, 52 ff.; weiter zum gläsernen Patienten Schaar, 72 ff.

1561 Der Helsana+-Entscheid des Bundesverwaltungsgerichts aus dem Jahr 2018 ist ein Lehrstück für die entsprechenden Ausführungen. Die Anmerkung von Vasella zur Rezeption des Entscheides auf LinkedIn, wonach man nun meinen könnte, die Helsana sei eine kriminelle Organisation, ist bemerkenswert. Vielleicht kommt in der Rezeption eben gerade zum Ausdruck, dass das Programm, das gerichtlich datenschutzrechtlich beurteilt wurde, entgegen dem Urteil eben doch grundlegende Schutzgedanken des Sozialversicherungsrechts erodiert und es eben doch nicht nur um ein isoliert datenschutzrechtliches Problem geht, sondern stattdessen elementare Werte eines sozialen Kontexts aufgrund einer bestimmten Verarbeitungspraxis auf dem Spiel stehen; unlängst BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018.

Deutschen Bundestag im Rahmen der Diskussionen um das IT-Sicherheitsgesetz am 12. Juni 2015:

> «An markigen Schlagwörtern wie Cyberwar oder Identitätsklau fehlt es nicht.»[1562]

Berichtet wird von Sammelwut und Datenflut, vom Untergang des Privaten, vom Sack voller Wanzen und der Datenkrake, vom Gold und Öl des 21. Jahrhunderts.[1563] Eine Auseinandersetzung mit der Rolle des Datenschutzes in den Medien lässt das Echo des Luther*schen* Abgesangs auf die Menschheit wieder erklingen. 1166

Die Emotionalität, mit der das Thema des Datenschutzes in den Medien behandelt wird, kann abgetan werden als Relikt eines Menschen und einer Gesellschaft, die sich noch nicht an die Möglichkeiten der Digitalisierung usf. anpassen konnte und es bloss als eine Frage der Zeit sieht, bis Bedürfnisse nach Datenschutz untergegangen sind. In Anbetracht des jüngsten Facebook-Skandals scheint es indes zu kurz zu greifen, die teilweise empörte und empörende Medienberichterstattung einzig als Angstmacherei zu deklassieren. Vielmehr kann die emotional aufgeladene und intensive Debatte zum Datenschutz in den zeitgenössischen Medien als Indikator verstanden und für die Reflexion sowie Gestaltung des Datenschutzrechts selbst fruchtbar gemacht werden.[1564] Sie ist dann als Ausdruck und Abbild tiefer Irritationen anzuerkennen, die durch kaum mehr durchschaubare Technologien ausgelöst werden und, so scheint es, dazu geeignet sind, die Robustheit bedeutsamer Institutionen zu erodieren. Die medial artikulierte Beunruhigung soll damit als *Plädoyer* dafür verstanden werden, dass «Privatheit» auch heute noch – vielleicht mehr als jemals zuvor – gesellschaftlich als (rechtlich schutzwürdiger) Zweck und Wert verstanden wird (freilich ohne dass über die Ingredienzen vollständige Klarheit bestünde). Zu einer solchen Interpretation, welche datenschutzrechtlichen Anliegen und Zielen hohe Relevanz beimisst und die eine ungenügende Effektivitätswirkung vorhandener Instrumentarien kritisch reflektiert, veranlasst nach dem medialen Blick ebenso derjenige auf den politischen Diskurs wie – resultierend – die jüngsten rechtlichen Neuerungen. 1167

1562 De Maizière, Deutscher Bundestag, Bundestag beschliesst das IT-Sicherheitsgesetz, Berlin 2015, <https://www.bundestag.de/dokumente/textarchiv/2015/kw24_de_it_sicherheit-377026> (zuletzt besucht am 30. April 2021).

1563 Betschon, NZZ vom 28. April 1998, 58, in dem es um die Sammlung geografischer Daten durch Apple geht; Nuspliger, NZZ vom 23. Oktober 2010, 13, in dem es um die Datensammlung für den Staatsschutz geht; zum Ende des Privaten vgl. Whitaker, *passim*.

1564 Gesellschaftlicher Widerstand (der auch medial zum Ausdruck gebracht wird) wird als Detektionsmittel für ihren Ansatz beschrieben, vgl. Nissenbaum, 3, 6.

4. Die Bedeutung des Datenschutzes in der politischen Debatte

1168 Die politische Debatte der vergangenen Jahre zeigt, dass mehrere namhafte Politikerinnen und Politiker den Datenschutz zu einem wichtigen Anliegen ihres Engagements gemacht haben. Sowohl Bestrebungen, den Datenschutz zu stärken, als auch Bestrebungen, diesen in Schranken zu weisen, lassen sich mit Leitideen verschiedener parteipolitischer Kataloge vereinbaren. An dieser Stelle lohnt es sich in Erinnerung zu rufen, dass der Informations- sowie Datenzugriff resp. der Schutz des Menschen vor Informationserhebungen und -auswertungen – wie im ersten, historischen Teil dieser Studie gezeigt wurde – schon früh staatspolitisch und -philosophisch eine tragende Rolle spielte.[1565] Die Staatenbildung und die Ausbildung zu absolutistischen Staatssystemen waren darauf angewiesen, die «Bürgerschaft» mittels durchgreifender Verwaltungsapparate ebenso informationell erfassen zu können. Als eine Reaktion auf folgende Zugriffe wird die Verbürgung von Freiheitsrechten beschrieben. In deren Geiste soll den Menschen ein geschützter – privater – Bereich zukommen, aus dem sich der Staat grundsätzlich herauszuhalten habe. Freiheitsrechte sind in ihrer klassischen Ausprägung als Abwehrrechte gegenüber dem Staat ein Drahtzieher für das Schutzobjekt des Privaten als gewährleistungswürdige Facette menschlichen Lebens.[1566]

1169 Für einen starken Datenschutz wird derzeit politisch mit dem Argument eingetreten, wonach dieser ein unverzichtbares Element darstelle, um die Rechtsstaatlichkeit sowie Demokratie zu gewährleisten.[1567] Gleichzeitig nimmt der moderne Leistungs- und Sozialstaat für sich in Anspruch, zwecks effizienter Erfüllung seiner Aufgaben und zur Steuerung seines Handelns seine Bevölkerung informationell zu erfassen und die gesammelten Personendaten auswerten zu können.[1568]

1170 In der politischen Debatte zum Datenschutz der Schweiz von besonderer Bedeutung sind Effizienzerwägungen, die vonseiten der Privatwirtschaft proklamiert werden. So wie bereits dem DSG bei seiner erstmaligen Verabschiedung wurde ebenso der Totalrevision des DSG mit wirtschaftlichen Argumenten Widerstand entgegengebracht: Der Datenschutz und die neu vorgeschlagenen Instrumente,

1565 Grundlegend zum Konnex von Liberalismus und Privatheit Rössler, 27 ff.
1566 Dies., 28.
1567 Illustrativ für diesen Bedeutungszusammenhang ist der jüngste Facebook-Skandal; hierzu insb. Söbbing, InTeR 2018, 182 ff.; vgl. Spiecker genannt Döhmann, in: Epiney/Sangsue (Hrsg.), 1 ff., 3 ff.; zu diesen Zusammenhängen auch Hotter, 59 ff.
1568 Vgl. BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 115; vgl. zum Leistungsstaat mit seinen Verarbeitungsaktivitäten auch Simitis, in: Schlemmer (Hrsg.), 67 ff., 73; dazu, dass Datenverarbeitungen ebenso der Verwirklichung von Grundrechten dienen, Giesen, JZ 2007, 918 ff., 922.

wie z. B. das Inventar, hätten einen unangemessenen Aufwand für die Unternehmen zur Folge.[1569]

Ein letzter Aspekt soll an dieser Stelle nicht unerwähnt bleiben: Gezeigt wurde in dieser Schrift, wie sich im Anschluss an die Abgrenzung eines privaten Bereiches gegenüber einem öffentlichen i. S. des staatlichen Bereiches der private Bereich mit der Etablierung der bürgerlichen Gesellschaft weiter ausdifferenzierte. Wegbereitend für die sich hier ausbildende Kategorie des Privaten im Privaten waren Warren/Brandeis. Dieses Private im Privaten war, ist und bleibt bis heute ebenso in der politischen Debatte stark mit dem *familiär-häuslichen Bereich* assoziiert. Und dieses Verhältnis zwischen der «privaten» im Sinne der familiär-häuslichen Sphäre (die traditionsgemäss als Domäne der Frau und Mutter gilt) und der «öffentlichen» Sphäre (die traditionell als Domäne des Mannes gilt) wird noch heute in der Schweiz grundlegend verhandelt. Das Thema des Datenschutzes ist entsprechend in der politischen Debatte an die grossen gesellschaftlichen Kernkategorien angeknüpft. Gleichzeitig wird in der politischen Debatte ein Bild der Erosion entsprechender Kategorien durch die technologischen Entwicklungen beschrieben, was wiederum die emotionale Besetzung des Themas ermöglicht. Die Gefühle von Angst, Verunsicherung usf. lassen sich auch im politischen Diskurs abholen. 1171

In den letzten Jahren hat sich der Datenschutz und das Anliegen, diesen wirksam(er) auszugestalten, parallel allerdings die Chancen der digitalen Verarbeitungstechnologien zu nutzen, *weit oben auf der politischen Agenda etabliert*. Auch in der Schweiz lässt sich insofern eine eigentliche Zeitenwende nachzeichnen: Bis ca. 2014 zogen datenschutzrechtliche Anliegen in der Schweiz weder im politischen noch im wissenschaftlichen Kontext und ebenso wenig in der Praxis sonderlich viel Aufmerksamkeit auf sich. Vielmehr begann sich der Datenschutz in der Schweiz erst in dem Moment von seinem Randdasein zu emanzipieren, als das strenge und elaborierte Regime der DSGVO am Horizont erschien. Dieses lieferte den wohl entscheidenden Anstoss, das schweizerische DSG einer Totalrevision zu unterwerfen. Sie war auf der politischen Agenda der wichtigste Punkt im Bereich Datenschutzrecht.[1570] 1172

Die bis dahin anhängig gemachten politischen Vorstösse können als Indikatoren interpretiert werden, wonach man sich bereits früh der ungenügenden Wirksamkeit des aktuellen Datenschutzgesetzes bewusst war. Ein Blick auf die politischen 1173

1569 Aufschlussreich gesamthaft die ambivalenten Stellungnahmen im Rahmen des Vernehmlassungsverfahrens zum Vorentwurf vgl. auch die Zusammenfassung der Ergebnisse abrufbar unter: <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> (zuletzt besucht am 20. September 2021).

1570 BJ, Stärkung des Datenschutzes, Bern 2020, <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> (zuletzt besucht am 30. April 2020).

Vorstösse in den vergangenen zehn bis fünfzehn Jahren zeigt namentlich zweierlei:

1174 *Erstens* wurden datenschutzrechtliche Belange politisch für *diverse Bereiche* angebracht, womit erneut die kontextuelle Relevanz des Themas sichtbar wird – ein Aspekt, der übersehen wird, wenn das DSG als Querschnittsgesetz als das «eigentliche Datenschutzrecht» gelesen wird. Illustrativ die Vorstösse in den Bereichen des Jugendmediendatenschutzes, der Humanforschung[1571], der Cybersecurity[1572], der digitalen Identität[1573] oder im Urheberrecht[1574].

1175 *Zweitens* lässt sich ebenso für den politischen Diskurs die Bemühung nachzeichnen, den Schutzbereich, das Schutzobjekt resp. den Schutzzweck des Datenschutzrechts, insb. des Datenschutzgesetzes, akkurat abzubilden. Mit der Hoffnung auf eine «eindeutige» Definierung geht auch diejenige einher, die «Rezeptur» für ein wirksames Datenschutzrecht zu finden.

1176 Vor diesem Hintergrund erstaunt nicht, dass die Aufmerksamkeit in den politischen Debatten nicht unwesentlich auf die *akkurate Definierung der Rechtsposition des Individuums* abzielt. Auch hier kommt das gesamte Cluster an denkbaren und diversen Konzepten zum Einsatz. Ihre schlagwortartige Beschreibung erfolgt oft in untechnischer resp. nicht-juristischer Weise («Vulgarisierung»): Verhandelt wird das Missbrauchskonzept, der Schutz der Privatsphäre, das Recht auf informationelle Selbstbestimmung sowie ein Eigentum an Personendaten.

1177 Insofern seien nur einige wenige Vorstösse erwähnt, beginnend mit der parlamentarischen Initiative Vischer (14.413) – Grundrecht auf informationelle Selbstbestimmung. Der Urheber der Initiative hielt fest, dass Art. 13 Abs. 2 BV jede Person ausschliesslich vor dem «Missbrauch ihrer persönlichen Daten» schütze. Hiermit würde die Beweislast für den Missbrauch nicht dem Staat oder Internetbetreiber auferlegt, sondern den Bürgerinnen und Bürgern. Die Initiative forderte, den Wortlaut von Artikel 13 Abs. 2 BV dergestalt zu ändern, dass die Garantie nicht nur einen Anspruch auf Schutz vor Missbrauch gewährt, sondern ein Grundrecht auf informationelle Selbstbestimmung:

> «Nicht nur durch den NSA-Skandal hat der Datenschutz auch in der Schweiz eine neue Bedeutung und Beachtung erhalten. Generell gefährden die Risiken, die von den sich in horrendem Tempo perfektionierenden technologischen Möglichkeiten der modernen Datenverarbeitung ausgehen, die freie Entfaltung der Persönlichkeit. Denn wer nicht weiss oder beeinflussen kann, welche Informationen bezüglich seines Verhaltens gespei-

1571 Anfrage Eymann (19.1012): Zeitpunkt der Verfügbarkeit von Patientendaten zur Förderung der Humanforschung durch Schweizer Firmen und Hochschulen.

1572 Interpellation Bregy (19.3288): Cyberkriminalität – Wie sieht es insb. mit der Ausbildung der Strafverfolgungsbehörden aus?

1573 Interpellation Fiala (18.4169): Die Ausgabe von digitalen Identitäten ist eine Staatsaufgabe.

1574 Vgl. Art. 66j E-URG vom 11. Dezember 2015, abrufbar unter: <https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2015/2015-12-11/vorentw-urg-d.pdf> (zuletzt besucht am 30. April 2021).

> chert und vorrätig gehalten werden, ist in seinem Verhalten eingeschränkt. Beeinträchtigt ist dabei nicht nur die individuelle Handlungsfreiheit, sondern auch das Gemeinwohl, denn ein freiheitliches und demokratisches Gemeinwesen ist auf die selbstbestimmte Mitwirkung seiner Bürgerinnen und Bürger angewiesen. Der in der Bundesverfassung garantierte Datenschutz gemäss Artikel 13 Absatz 2 der Bundesverfassung schützt die einzelne Person lediglich vor dem Missbrauch. Das führt namentlich dazu, dass im Ergebnis die Beweislast der Grundrechtseinschränkung zulasten der Bürgerinnen und Bürger und nicht des Staates oder der Internetbetreiber verteilt ist. Mit der Ausweitung der Verfassungsbestimmung im beantragten Sinne wird eine neue verfassungsmässige Grundlage geschaffen, um dies zu ändern. Bisher scheiterten ähnliche Vorhaben. Die Erfahrungen der letzten Monate evozieren freilich dringenden Handlungsbedarf.»[1575]

Bereits vor diesem wichtigen Vorstoss zur Bereinigung der aktuellen Verfassungsbestimmung gab es Bemühungen, den «missratenen» *Verfassungstext zu korrigieren,* so die parlamentarische Initiative Schelbert (06.460) – Datenschutz. Vom Schutz vor Missbrauch zum Recht auf Selbstbestimmung. Sie wurde am 11. Dezember 2008 erledigt, will heissen, es wurde ihr nicht Folge gegeben. Mit der parlamentarischen Initiative Derder (14.434) – Schutz der digitalen Identität von Bürgerinnen und Bürgern – wurde zudem die Forderung, ein «Eigentum an Daten» anzuerkennen, in die politische Debatte eingeführt. Auch diese Initiative verlangte eine Änderung von Art. 13 BV, und zwar wie folgt: «Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung, ihres Brief-, Post- und Fernmeldeverkehrs sowie all ihrer eigenen Daten» (Abs. 1) und «Die Daten sind Eigentum der betreffenden Person; diese ist davor zu schützen, dass die Daten missbräuchlich verwendet werden» (Abs. 2). Die staatspolitische Kommission des Nationalrates nahm die Initiative am 16. Januar 2015 an, diejenige des Ständerates folgte diesem Entscheid am 20. August 2015. Zwei etwas ältere Vorstösse zeitigten Einfluss auf den Schweizer Gesetzgeber: das Postulat Hodgers vom 8. Juni 2012 (10.3383) – «Anpassung des Datenschutzgesetzes an die neuen Technologien» sowie das Postulat Graber vom 14. September 2010 (10.3651) – «Angriff auf die Privatsphäre und indirekte Bedrohungen der persönlichen Freiheiten». Damit richteten sich bereits in den Jahren vor der Totalrevision mehrere politische Vorstösse auf Ausbau, Fortentwicklung oder Klärungen im Datenschutzrecht.[1576] 1178

1575 Das Schweizer Parlament, Grundrecht auf informationelle Selbstbestimmung, Bern 2017, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20140413> (zuletzt besucht am 30. April 2021).

1576 Illustrativ nur der Hinweis auf die folgenden Vorstösse: Interpellation Feri (17.3531) – Digitalisierung im Gesundheitswesen; Postulat Munz (16.4054) – Schutz der Wahlen und Abstimmungen vor Big-Data-Missbrauch (erledigt); Interpellation Amherd (16.4051) – E-Vignette. Wann kommt sie? (erledigt); Postulat ShwaAB (16.4007) – Algorithmen, die im Einklang mit den Grundrechten stehen (erledigt); Motion Hubmann (07.3468) – Datenschutz im Gesundheitswesen (abgeschrieben); Interpellation Beglé (16.3963) – Die Schweiz, der digitale Tresor. Den Schutz der Unternehmen im Datenschutzgesetz beibehalten (erledigt); Interpellation Tornare (16.3837) – Zivile Drohnen. Kritische Infrastrukturen besser schützen (erledigt); Postulat Alleman (16.3789) – Digitalisierung im öffentlichen Verkehr. Herausforderungen im Bereich Datenschutz (erledigt); Postulat Feri (15.340) – Schutz

1179 Auf den Anstieg politischer Vorstösse im Bereich Datenschutz weist namentlich der erläuternde Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, datiert auf den 21. Dezember 2016, hin.[1577] Dass das DSG *de lege lata* den zeitgenössischen Herausforderungen und Entwicklungen nicht (mehr) zu genügen vermag, wird spätestens im Zuge der Totalrevision zum DSG offen anerkannt.[1578] Im politischen Kontext rückte damit die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz in das Zentrum. Zur Totalrevision sah man sich aufgrund der europäischen Entwicklungen und namentlich der DSGVO, aber auch des technischen Fortschritts sowie der ungenügenden Wirksamkeit des DSG veranlasst.[1579]

1180 Die Verabschiedung zog sich in die Länge: Am 12. Juni 2018 wurde beschlossen, die Beratungen aufzuspalten, wobei vorab die für den Schengen-Besitzstand relevanten Normen verabschiedet wurden. Die Beratungen zur Revision des DSG wurden im November 2018 von der staatspolitischen Kommission des Nationalrates verschoben. Die parlamentarischen Beratungen erfolgten später in der Herbstsession 2019, wobei der Nationalrat als Erstrat die Kommissionvorlage am 23./24. September beriet.[1580] Nach der Detailberatung im Nationalrat wurde der staatspolitischen Kommission des Ständerates eine Version zur Verhandlung gestellt, für welche bereits die Befürchtung geäussert worden war, dass sie den Anforderungen vonseiten der EU für den Angemessenheitsbeschluss nicht erfülle. Die staatspolitische Kommission des Ständerates schloss die Vorberatungen im November 2019 ab. Hier wurden mehrere Verschärfungen vorgeschlagen. In der Folge wurde der Entwurf in der Wintersession 2019 im Ständerat verhandelt.[1581] Verabschiedet wurde die Totalrevision am 25. September 2020. Sie tritt 2023 in Kraft, nachdem auch die Ausführungsbestimmungen zum DSG, die

der Persönlichkeitsrechte (noch nicht behandelt); Interpellation Schwaab (15.3045) – Zwingt uns das Tisa-Abkommen einen zweitklassigen Schutz der Privatsphäre auf? (noch nicht behandelt). Hierzu <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista> (zuletzt besucht am 30. April 2021); weiter geben eine Übersicht Vasella/Sieber auf <www.datenrecht.ch> (zuletzt besucht am 30. April 2021).

1577 Bundesamt für Justiz, Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Bern 2016, <https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/vn-ber-d.pdf> (zuletzt besucht am 30. April 2021).

1578 Bundesamt für Justiz, Stärkung des Datenschutzes, Bern 2020, <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> (zuletzt besucht am 30. April 2021); dritter Teil, VII. Kapitel, B.

1579 Botschaft DSG 2017–1084, 17.059, 6941 ff., 6943 ff.

1580 Vgl. zu den Wortprotokollen: <https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=47356> (zuletzt besucht am 30. April 2021).

1581 Daten:recht, Revision des DSG: SPK-SR will deutliche Verschärfungen; in der Wintersession im Ständerat, November 2019, <https://datenrecht.ch/revision-des-dsg-spk-sr-will-deutliche-verschaerfungen-in-der-wintersession-im-staenderat/> (zuletzt besucht am 30. April 2021).

VDSG sowie die Verordnung über die Datenschutzzertifizierung revidiert wurden.

Die wichtigsten Entwicklungstrends und zentralen Anpassungen der Totalrevision werden – in Anlehnung an den zweiten Teil dieser Arbeit in Gestalt von Strukturmerkmalen – im VIII. Kapitel dieses dritten Teils präsentiert.[1582] Dass die mit der Revision des DSG vorgesehenen Neuerungen erst ebenda zur Sprache kommen, ist dem Umstand geschuldet, dass die Verabschiedung der Totalrevision, ähnlich wie diejenige des ersten DSG, ebenso eine «élaboration pénible» war.[1583] Die Schweiz gewährleistet mit der Totalrevision des DSG eine Anhebung des Datenschutzniveaus, u. a. mittels Einführung neuer Regelungsinstrumente. Gleichwohl wird das Schutzniveau hinter demjenigen der DSGVO zurückbleiben. Die zeitlichen Entwicklungen dokumentieren erneut, dass der Datenschutz in der Schweiz einen schweren Stand hat. Ursächlich hierfür waren an erster Stelle – wie bereits im Zuge der Verabschiedung des DSG in den 1990er Jahren – Widerstände aus Wirtschaftskreisen. 1181

Das Bild zur Bedeutung datenschutzrechtlicher Anliegen in der Politiklandschaft der Schweiz soll durch Erwähnung einiger weiterer Projekte und Initiativen abgerundet werden: So ist beispielsweise auf das zum Zeitpunkt der Niederschrift dieser Studie noch in den parlamentarischen Beratungen befindliche Informationssicherheitsgesetz des Bundes hinzuweisen.[1584] Es wird als Instrument zur Gewährleistung der Cybersicherheit beschrieben.[1585] Mehrere Angriffe auf die Informationsinfrastruktur des Bundes haben Lücken in Bezug auf die Informationssicherheit offenbart sowie Defizite der einschlägigen zersplitterten Rechtsgrundlagen gezeigt. Mit dem Gesetz sollen Mindestanforderungen und -massnahmen, die Bundesbehörden zum Schutz ihrer Informationen und deren Systeme wie Netzwerke umzusetzen haben, definiert werden. Zudem soll es eine Standardisierung des Sicherheitskatalogs zwecks Vereinheitlichung und effizienter Implementierung der Sicherheitsmassnahmen beim Bund mit sich bringen, wobei es den internationalen Standards im Bereich der Informationssicherheit entspricht. Als bedeutsamste Massnahmen sind Risikomanagement, Klassifizierung von Informationen, Informatiksicherheit, Personensicherheitsprüfungen, Sicherheit bei sensitiven Beschaffungen sowie Unterstützung der Betreiber von kritischen Infrastrukturen im Bereich der Informationssicherheit durch den Bund zu nennen. Das Gesetz will auf eine Detailregelung der Massnahmen, die im Lichte des schnellen technischen Fortschrittes allzu bald Makulatur würden, verzichten. Vielmehr soll 1182

1582 Vgl. zu datenschutzrechtlichen Reformschritten teilweise auch kritisch Bull, Vision, 112 ff.
1583 Zu dieser im Rahmen der Verabschiedung des ersten DSG zweiter Teil, B.2.
1584 Botschaft Informationssicherheitsgesetz, BBl 17.028, 2959.
1585 Vgl. Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport, Informationssicherheitsgesetz, Bern 2020, <http://www.vbs.admin.ch/de/themen/informationssicherheit/informationssicherheitsgesetz.html (zuletzt besucht am 30. April 2021).

ein Gesetz im formellen Sinne geschaffen werden, auf dessen Basis Konkretisierungen durch Verordnungen und Weisungen erfolgen. Die sicherheitspolitische Kommission des Nationalrates ist zwar am 9. Oktober 2018 auf die Vorlage eingetreten, sistierte indes die Beratungen und beauftragte das VBS, bis Juni 2019 einen Verbesserungsvorschlag zu präsentieren.[1586]

1183 Sodann sind einige vom Bundesrat im Zusammenhang mit dem digitalen Wandel lancierte Projekte (z. B. E-Government, E-Justice, E-Health, elektronische Geschäftsverwaltung usw.) zu nennen. Nach der E-Government-Strategie aus dem Jahr 2007 und der Verabschiedung einer weiterentwickelten Version Ende 2015 folgte die Strategie des Bundesrates für eine digitale Schweiz vom 20. April 2016, die von derjenigen vom 5. September 2018 abgelöst wurde.[1587] Definiert werden Grundsätze, Kernziele, Aktionsfelder und Umsetzungsmassnahmen, damit die Chancen der Digitalisierung konsequent genutzt werden und sich die Schweiz als attraktiver Lebensraum, produktiver Wirtschafts- und innovativer Forschungsstandort durchsetzen kann. Dem Schutz der Person, deren Personendaten verarbeitet werden, sowie dem umsichtigen Umgang mit neuen Technologien wird ein besonderer Stellenwert zugemessen.

1184 Informations- und datenschutzrechtliche Anliegen resp. solche der Daten- und Informationssicherheit stehen heute weit oben auf der politischen Agenda. Damit wird anerkannt, dass die geltenden Regeln und Konzepte den aktuellen Herausforderungen nicht mehr angemessen Rechnung tragen können. Ein wirksames Regelungsregime, das seinen Aufgaben und Herausforderungen hinreichend gerecht wird – wozu namentlich auch die Wirksamkeit in der Realität gehört – kann allerdings nur entwickelt werden, wenn *Schwachstellen* der aktuellen Regelung identifiziert sowie die faktischen Herausforderungen hinreichend präzis erfasst sind. Entsprechend findet nachfolgend zunächst eine Auseinandersetzung mit den Erklärungsmustern statt, die für das attestierte Vollzugsdefizit des geltenden Datenschutzrechts angeführt werden. Chiffrierungen wie der «rasante technische Fortschritt», das «Gold der Personendaten» oder das «achtlose Datensubjekt» greifen zu kurz. Mit ihnen lassen sich Schwächen des geltenden Rechts nicht hinreichend exakt erfassen. Auf eine präzise «Problemanalyse» ist allerdings die Entwicklung von Ansätzen für ein wirkungsstarkes Datenschutzrecht angewiesen. Die anschliessenden Ausführungen befassen sich vorab mit der «Ursachenforschung» für das datenschutzrechtliche Vollzugsdefizit. Darauf-

1586 Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport, Informationssicherheitsgesetz, Bern 2020, <http://www.vbs.admin.ch/de/themen/informationssicherheit/informationssicherheitsgesetz.html (zuletzt besucht am 30. April 2021).

1587 Vgl. zu letzterer <https://strategy.digitaldialog.swiss/de/> (zuletzt besucht am 30. April 2021).

hin findet eine vertiefte Beschäftigung mit den faktischen Herausforderungen des Datenschutzrechts statt.[1588]

5. Erklärungsmuster für das Vollzugsdefizit

Die vorangehenden Ausführungen zu empirischen Erkenntnissen betreffend die Wirksamkeit des Datenschutzrechts sowie zur Bedeutung des Datenschutzes in Rechtspraxis und Lehre, in den Medien sowie im politischen Diskurs haben sichtbar gemacht, dass insb. für das DSG *de lege lata* von einem eigentlichen Vollzugsdefizit ausgegangen werden muss.[1589] Mit anderen Worten: Das Gesetz ist weitgehend toter Buchstabe geblieben – im privaten Sektor werden nicht nur die allgemeinen Verarbeitungsvorgaben ungenügend beachtet, auch die Betroffenenrechte haben keine grosse Bedeutung erlangt. Missachtungen der datenschutzgesetzlichen Vorgaben ziehen nur ganz ausnahmsweise rechtliche Konsequenzen nach sich, Bussen und Klagen wegen Persönlichkeitsverletzungen, Empfehlungen vom EDÖB und ein daran anschliessendes Gerichtsverfahren sind in Anbetracht der Bedeutung von Personendatenverarbeitungen selten. Das generalklauselartige Regime und die insofern einschlägige Behördenpraxis und Lehre vermochte nur ansatzweise strukturierende Vorgaben für personendatenverarbeitende Stellen und Unternehmen zu formulieren. Die geringfügigen und kaum je zu erwartenden Sanktionen wirken nicht abschreckend, womit vom aktuellen Datenschutzrechtsregime nur eine beschränkte faktische Regulierungs-, Präventiv- und Abschreckungsfunktion ausgeht.[1590] Abhilfe bringen sollen die jüngsten datenschutzrechtlichen Revisionen, deren Ziel insb. darin verortet werden kann, dem formellen Recht auch faktisch und in der Realität Griffigkeit und Wirksamkeit zu verleihen.[1591] 1185

Wie aber wurde der ernüchternde Befund, wonach das DSG *de lege lata* primär auf dem Papier Wirksamkeit entfaltet, in der Praxis indes über weite Strecken unbeachtet bleibt, bislang erklärt? Eine *Ursachenforschung* ist weiterhin aufschlussreich, zumal hieraus selbst über die Zeit nach der Totalrevision des 1186

1588 Aussagestark in diesem Zusammenhang Simitis, in: Schlemmer (Hrsg.), 67 ff., 68, wonach oft darauf geschlossen werde, dass es darum ginge, technische Entwicklungen zu kontrollieren. Damit würde eine Antithese konstruierbar, wonach die Privatsphäre zum Symbol für eine Gesellschaft werde, die sich weigere, sich den Zwängen des technischen Fortschrittes zu unterwerfen.

1589 Eine Diskrepanz zwischen *Deklarationen* hinsichtlich der Bedeutung des Datenschutzes und seiner faktischen Verwirklichung in Schweizer Unternehmen beschrieben unlängst Ebert/Widmer, 3 ff. Namentlich die KMUs stellen oft kein Budget für Datenschutzanliegen bereit, führen folglich kaum Schulungen durch, sind unsicher mit Blick auf die Anwendbarkeit der DSGVO und führen in der Regel auch keine Verarbeitungsverzeichnisse; mit Blick auf Deutschland grundlegend, allerdings vor der Anwendbarkeit der DSGVO, Buchner, 1.

1590 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 345; für weitere Hinweise die vorangehenden Ausführungen.

1591 Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.

DSG Hinweise auf fortbestehende konzeptionelle Schwachpunkte und allfällige Lösungsansätze generiert werden können.[1592] Damit lassen sich aus der Beschäftigung mit den präsentierten Erklärungsmustern für die nur ungenügende Wirksamkeit des bisherigen Datenschutzrechts Evaluationskriterien gewinnen, ob und inwiefern die aktuellen rechtlichen Neuerungen an den richtigen Stellen ansetzen.

1187 Eine Begründung für die bloss ungenügende Wirksamkeit des geltenden Datenschutzrechts wird im *Verhalten der Datensubjekte* selbst verortet: Nachlässigkeit, Überforderung oder fehlendes Bewusstsein für die Möglichkeiten der Personendatenverarbeitungen, aber auch die Verführbarkeit des Datensubjektes gelten als «Hauptrisiken» für den Datenschutz.[1593] In einer die Totalrevision des DSG vorbereitenden Evaluation wurde die Kenntnis in der Schweizer Bevölkerung über Bestand, Inhalt und Möglichkeiten des DSG als gering eingestuft:[1594] Von den zwei Dritteln der Befragten, die vom DSG überhaupt schon einmal gehört hatten, erklärte bloss ein Viertel, von der Möglichkeit der (gerichtlichen) Durchsetzungsinstrumente Kenntnis zu haben.

1188 Greift das Datenschutzrecht in der Praxis ungenügend, dann scheint es – obschon die verarbeitenden Stellen an erster Stelle die Adressaten der Datenschutzpflichten sind und gewissermassen als «Verantwortliche» oder «Verursacher» zu sehen sind – fast zwingend, das Datensubjekt insofern für eine defizitäre Wirkung des Datenschutzrechts verantwortlich zu machen. Illustrativ insofern selbst der EDÖB:

> «Der digitale Lebensstil ist von einer Sorglosigkeit im Umgang mit IKT geprägt, die abrupt in öffentliche Entrüstung umzuschlagen pflegt, sobald Medien oder Konsumentenschutzorganisationen eine Massenapplikation wegen angeblich unerlaubter Eingriffe in die Privatsphäre kritisieren. Die Öffentlichkeit erwartet, dass der EDÖB zumindest bezüglich der aktuell gängigsten Applikationen, die oft gratis im Netz verfügbar sind, proaktiv über Risiken informiert. Gleichzeitig soll er Möglichkeiten zur Wahrung der Privatsphäre aufzeigen und im Rahmen von aufsichtsrechtlichen Verfahren die Datenschutzkonformität solcher Massenapplikationen durchsetzen.»[1595]

1189 Exemplarisch zur Verantwortlichkeit der Datensubjekte in Bezug auf die (mangelhafte) Gewährleistung des Datenschutzes ebenso die Worte des Bundesrates:

> «Weiter kann aufgrund der vorliegenden empirischen Evidenz bilanziert werden, dass die betroffenen Personen die Persönlichkeit zwar schützen möchten, teilweise jedoch achtlos und überfordert sind. Laut der Bevölkerungsumfrage will die grosse Mehrheit der Bevölkerung an den neuen Möglichkeiten des Informationsaustauschs teilhaben. Gleichzeitig empfindet sie den Schutz ihrer persönlichen Daten als wichtig, auch im Bereich der neuen unübersichtlichen Konstellationen im Internet. Dennoch schützen sich die Betroffenen

1592 Unlängst die Analyse zu Schwachpunkten des DSG Thouvenin, digma 2019, 206 ff.
1593 Vgl. Bolliger/Féraud/Epiney/Hänni, II; BR, Schlussbericht Evaluation 2011–1952, 335 ff., 348; Grassegger, 9, spricht in seinem Essay von der «selbst verschuldeten digitalen Unmündigkeit».
1594 Bolliger/Féraud/Epiney/Hänni, 77 f.
1595 EDÖB, 24. Tätigkeitsbericht 2016/2017, 7.

> selbst nicht immer konsequent, fühlen sich bisweilen überfordert oder unterschätzen die bestehenden Möglichkeiten der Datenbearbeitung und deren Risiken. Die bisweilen grosszügige Preisgabe persönlicher Daten dürfte auch damit zusammenhängen, dass das Risiko eines Datenmissbrauchs und seiner Folgen als diffus und unwahrscheinlich wahrgenommen wird, zumindest im Vergleich zum unmittelbaren Nutzen des jeweiligen Angebots.»[1596]

Dass das Datensubjekt betreffend den Schutz von personenbezogenen Daten indifferent oder unsorgfältig sei, mag man weiter durch Umfrageergebnisse dokumentiert sehen, wonach lediglich rund 20 Prozent der befragten Personen die privacy policy meistens lesen würden.[1597] 1190

Als Beweis dafür, dass Privatheit und Datenschutz für die Menschen des 21. Jahrhunderts nur noch beschränkten Wert haben, wird zudem ein Phänomen ins Feld geführt, welches unter dem Begriff des Medien-Exhibitionismus eingefangen werden kann.[1598] Das Verhalten junger Menschen in sozialen Netzwerken wird insofern als indikativ dafür angeführt, dass sich diese nicht mehr um «privacy» kümmern.[1599] Darüber hinaus wird die (nicht wahrgenommene) Verantwortlichkeit des Individuums für die schwache Wirksamkeit des Datenschutzes mit der Bereitschaft der Menschen – der Konsumentinnen und Konsumenten –, für die Preisgabe von Personendaten Bonuspunkte, Rabatte usf. zu erhalten, erhärtet.[1600] 1191

Solche Argumente greifen allerdings zu kurz, um der Komplexität der Thematik und der dilemmatischen Situation gerecht zu werden, die auch, aber nicht nur im Datensubjekt kulminiert.[1601] Wenn dem Datensubjekt die Verantwortlichkeit dafür zugewiesen wird, dass das Datenschutzrecht nicht hinreichend wirksam wird, drängt sich das Hinterfragen eines Regelungsregimes auf, das den Datenschutz individualrechtlich anknüpft. 1192

Insofern ist zunächst beachtlich, dass Umfrageergebnisse unmissverständlich belegen, wonach selbst in der heutigen «digitalen Gesellschaft» dem ganz überwiegenden Teil der Menschen der Datenschutz wichtig ist.[1602] Auch für die Schwei- 1193

1596 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 342 f.
1597 M. w. H. Nissenbaum, 104 f.
1598 Dies., 106.
1599 Dies., 60 und 221, die ebendies sogleich als «kolossale Fehlannahme» bewertet – wobei vielleicht präziser von einer schlauen Fehlbehauptung insb. zu wirtschaftlichen Zwecken gesprochen werden könnte.
1600 Jüngst selbst im Kontext der Sozialversicherung vgl. Fall BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018; vgl. zu den verschiedenen Positionen der Individuen Bibas, Harv. J.L. & Pub. Pol'y 1994, 591 ff., 593; kritisch zur Eigenverantwortung im Zusammenhang zwischen Sozialversicherung und Personendatenverarbeitung auch in Bezug auf das Helsana+-Urteil Pärli, SZS 2018, 107 ff., 117 f.
1601 Dass es sich nicht isoliert um ein individuelles Dilemma handelt, sondern eine kollektive Dimension dahintersteht, wird im dritten Teil, IX. Kapitel vertieft.
1602 Vgl. <http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf> (zuletzt besucht am 30. April 2021); sodann die Evaluation von Burghardt/Böhm/Buchmann et al.; Bol-

zer Bevölkerung ergab eine erste repräsentative Datenschutz-Umfrage, dass es drei Vierteln der Bevölkerung wichtig bis sehr wichtig ist, wie mit ihren persönlichen Daten umgegangen wird. Geäussert werden allem voran Sorgen, was Personendatenverarbeitungen im Internet anbelangt.[1603] Neun von zehn Personen artikulierten das Bedürfnis, wonach Unternehmen und Staat ihre Daten schützen sollen. Die Datensubjekte resp. Betroffenen sind folglich keineswegs sorglos und indifferent gegenüber dem, was mit «ihren» personenbezogenen Daten geschieht. Empirisch wurde erhoben, dass Datenschutz auch heute – jeglichen gegenteiligen Behauptungen zum Trotz – einem Bedürfnis und Interesse der Datensubjekte, der Individuen entspricht.[1604] *Prima vista* scheint man insofern mit einem Widerspruch konfrontiert: Egal, welche Relevanz die Datensubjekte dem Datenschutz erklärtermassen (theoretisch?) zumessen, sie handeln nicht selten in einer Art und Weise, die einen zu der Annahme verführen mag, wonach für sie Datenschutz nicht relevant sei oder nur sekundäre Bedeutung habe.[1605] Der Befund ist erklärungsbedürftig, was denn auch im Zuge der nachfolgenden Ausführungen geschehen soll. Die Erklärung findet sich, so die hier – basierend auf jenem empirischen Befund – formulierte *These*, nicht nur in der «Achtlosigkeit des Datensubjektes».

1194 Es gibt mehrere Gründe, weshalb es zu kurz greift, Last und Verantwortung für den Datenschutz sowie die Wirkungsschwächen des DSG *in erster Linie dem Individuum* aufzubürden.[1606] Insofern sind einige der im Zuge dieser Schrift generierten Erkenntnisse zu rekapitulieren.

1195 Zunächst wurde das Regime des DSG für den privaten Bereich als eine Missbrauchsgesetzgebung qualifiziert.[1607] Personendatenverarbeitende Privatpersonen und Unternehmen dürfen Personendaten innerhalb der durch die generalklauselartigen Grundsätze gesetzten Schranken *prinzipiell frei* verarbeiten. Damit liegt die Verantwortung an erster Stelle und per se in den Händen der Verarbeitenden. Es obliegt den Verarbeitenden, die Einhaltung des Datenschutzes zu gewährleisten.

---

liger/Féraud/Epiney/Hänni, II; vgl. auch Nissenbaum, 186 ff.; BR, Schlussbericht Evaluation 2011–1952, 335 ff., 342; hierzu ebenso bereits Bäumler, digma 2003, 30 ff., 30, wobei sich der Autor mit der steigenden Bedeutung von Datenschutz-Audits und Gütesiegeln sowie der Relevanz von Privacy Enhancing Technologies befasst.

1603 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 342; zur Evaluation des Internetdatenschutzes in Deutschland Burghardt/Böhm/Buchmann, 3 ff.; zur Herausforderung der Regulierung des Datenschutzes im Internet nicht aus materiellrechtlicher, sondern aus zuständigkeitsrechtlicher Perspektive Balthasar, Jusletter IT vom 20. Februar 2014.

1604 Bolliger/Féraud/Epiney/Hänni, 45.

1605 Dies., 106.

1606 Vielmehr lässt sich dahinter oft eine dilemmatische Ausgangssituation und die Kollision zwischen verschiedenen Zielen und Interessen nachweisen, womit auch die im ersten Teil dieser Arbeit bereits angesprochene Akzessorietät des Datenschutzrechts zu dahinterliegenden Kontexten angesprochen ist.

1607 Vgl. zweiter Teil, VI. Kapitel, B.

Umgekehrt kommt den Datensubjekten in diesem Regime bereits von Gesetzes wegen keine Rechtsposition zu, die ihnen eine «Hauptrolle» im Verarbeitungsprozess resp. eine effiziente Kontrolle hinsichtlich des Umgangs mit ihren Personendaten einräumen würde: Die Transparenzvorgaben im DSG *de lege lata* sind wenig stark ausgebaut. Die Einwilligung des Datensubjektes ist keine prinzipielle Verarbeitungsvoraussetzung für Personendatenverarbeitungen des DSG im privaten Bereich. Und das Widerspruchsrecht, aber auch das Auskunftsrecht sowie die Klagebehelfe wegen Persönlichkeitsverletzungen, welche dem Datensubjekt auferlegen, unrechtmässige Datenverarbeitungen der Verarbeitenden durchzufechten und zu belegen, sind nicht geeignet, der Einhaltung des Datenschutzrechts Nachachtung zu verschaffen. 1196

Gleichwohl darf nicht voreilig die Schlussfolgerung gezogen werden, dass die «Aufwertung» der individualrechtlichen Position durch Einführung eines Rechts auf informationelle Selbstbestimmung (das diese Bezeichnung verdient) das Rezept zur Lösung der datenschutzrechtlichen Herausforderungen liefert. Denn selbst Datenschutzkonzepte, welche dem Individuum eine stärkere Position zuweisen, namentlich durch ein Verarbeitungsverbot mit Erlaubnistatbestand sowie Einwilligungskonstruktionen, sehen sich in Anbetracht der datenschutzrechtlichen Realitäten mit erheblichen Problemen konfrontiert.[1608] 1197

Bemerkenswert ist, wie zurückhaltend gerade in den Evaluationen die Rolle und Verantwortung der *Verarbeitenden* bei der Umsetzung und Einhaltung der datenschutzgesetzlichen Vorgaben thematisiert werden. Doch genau darin liegt ein eigentliches Defizit des aktuellen Regimes, zumal es die verarbeitenden Stellen sind, welche die Personendatenverarbeitungen durchführen, welche «Handelnde» und «Herrinnen» der Verarbeitungsprozesse und -praktiken sind. Sie haben Design, Durchführung und Umsetzung der Personendatenverarbeitungsprozesse in der Hand. Aufseiten der Verarbeitenden allerdings wird der «pragmatische Umgang mit dem Datenschutzgesetz» mit den Chancen und Herausforderungen der neuen Technologien, eigenen Interessen an einer weitgehend unbeschränkten Personendatenverarbeitung, den ungenügenden Risiken von Konsequenzen bei Nichteinhaltung des DSG sowie den ungenauen gesetzlichen Anleitungen usf. zu erklären versucht. Dass die Sicherstellung der Einhaltung von datenschutzrechtlichen Vorgaben *primär eine Verantwortung der Verarbeitenden* ist, scheint zumindest unter dem noch geltenden schweizerischen Recht nur ungenügend in deren Bewusstsein vorgedrungen zu sein. Eine am deliktsrechtlich und abwehrrechtlich strukturierten Persönlichkeitsschutz vorgenommene Anknüpfung des Datenschutzrechts, in welcher die Verletzung kaum je Folgen hat, verleitet dazu, 1198

1608 M. w. H. dritter Teil, VIII. Kapitel, B.

die *primäre und antizipierende Eigenverantwortung* für die Data Governance durch die personendatenverarbeitenden Stellen aus den Augen zu verlieren.

1199 Erst die *jüngsten Rechtsänderungen* werden insofern einen *Perspektivenwechsel* einleiten, als sie namentlich die sog. «Verantwortlichen» in eine proaktive Pflicht nehmen. Diese Terminologie ist in den neuen Erlassen nicht nur für datenschutzrechtliche Fragen der Rollen von Verantwortlichem und Auftragsverarbeiter wichtig, sondern gerade auch für den hier diskutierten Punkt aussagekräftig. Die datenschutzrechtlichen Neuerungswellen setzen keineswegs bloss und erst an der «starken» Hand der Behörden bei der Durchsetzung des Datenschutzes resp. seiner Verletzung an, womit man bisherigen Defiziten behördlicher Durchsetzungsinstrumente entgegentreten will. Vielmehr avancieren der Datenschutz und die Einhaltung der datenschutzrechtlichen Vorgaben zu einer Compliance- und Governance-Aufgabe der verarbeitenden Stellen und Unternehmen. Sie haben die erforderlichen Strukturen, Prozesse und Organisationszuständigkeiten zu etablieren und damit den Datenschutz operationalisierbar zu machen. In diesem Punkt ist von einem Paradigmenwechsel zu sprechen, den die DSGVO und die Totalrevision des DSG liefern.[1609]

1200 Ein weiteres Erklärungsmuster für die ungenügende Wirkungskraft des DSG *de lege lata* ist der «rasante technologische Fortschritt». Er stelle das geltende Recht auf den Prüfstand.[1610] Die Ausführungen zu den technischen Potenzen allerdings bleiben schematisch und grob: Vage wird attestiert, dass Personendatenverarbeitungen hohe Relevanz haben. Die Technologie entwickelt sich rasend schnell fort und die Vernetzungsmöglichkeiten im Internet haben das Sammeln, Verknüpfen und Auswerten von Personendaten stark vereinfacht. Technisch gäbe es kaum mehr Restriktionen, Informationen umfassend zu erheben, zu speichern, zu kopieren und während längerer Zeit aufzubewahren (Stichwort «Big Data»).[1611] Die Auswertungsmethoden hätten erhebliche Verbesserungen erfahren (Stichwort «Data Mining»).[1612] Immer mehr Lebensbereiche würden von der Digitalisierung erfasst, was zu einer «allgegenwärtigen Datenbearbeitung» führe (Beispiele sind Videoüberwachung, Biometrie-Systeme, GPS- oder mobilfunkgestützte Systeme zur Lokalisierung).[1613] Sodann machen Datenverarbeitungen keinen Halt an den Landesgrenzen.[1614] Vor diesem Hintergrund wird die Einhaltung

1609 Vgl. Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 f.; Dies., Schweizer Bank 21 vom 21. Mai 2018, 20 f.; Dies., NZZ vom 30. Oktober 2018, 10.
1610 Exemplarisch hierzu Botschaft DSG 2017–1084, 17.059, 6941 ff., 6969; BR, Schlussbericht Evaluation 2011–1952, 336 ff., 336 ff.
1611 Exemplarisch Bolliger/Féraud/Epiney/Hänni, I ff., 225 f.; EJPD, Bericht Begleitgruppe, 7; Brunner, Jusletter vom 4. April 2011, N 16 ff.
1612 Zu Methoden, Herausforderungen und Chancen von Data Mining im Milieu von Big Data vgl. die Beiträge in Chu (ed.); Eckhardt/Fattebert/Keel/Meyer, 46 ff.
1613 Vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 7076.
1614 Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.1.

der Verarbeitungsgrundsätze, sondern auch der Betroffenenrechte skeptisch beurteilt.[1615]

Bereits in den 1980er Jahren waren es die Herausforderungen des rasanten technologischen Wandels sowie die Unmöglichkeit, die Technik zu durchschauen, welche den Gesetzgeber zur Regelung mittels Generalklauseln veranlasste; der Gesetzgebungstechnik wurde das Attribut der «Technikneutralität» verliehen.[1616] Allerdings musste genau diese «Flucht in die Generalklauseln» als ein (ggf. vorläufiger) Schwachpunkt des Datenschutzrechts identifiziert werden. 1201

In der Konkretisierung der generalklauselartigen Verarbeitungsgrundsätze, aber auch in der Bereitstellung von Umsetzungsinstrumenten werden heute Ansätze verortet, ein bisheriges Defizit der Datenschutzgesetzgebung zu überwinden. Zudem lässt sich für das Datenschutzrecht ein Regelungsinstrument beschreiben, das ebenso ausgebaut wird und mit dem für die Homöopathie bekannten Rezept, «Gleiches mit Gleichem» zu behandeln, umschrieben werden kann. Das Datenschutzrecht sieht seit jeher den Einsatz von Technologien zu seiner Gewährleistung vor, so durch Instrumente wie Anonymisierung resp. Pseudonymisierung, Verschlüsselung sowie *datenschutzfreundliche Voreinstellungen*.[1617] Sie gelten als vielversprechendes Instrumentarium zur Umsetzung datenschutzrechtlicher Anliegen. Gleichwohl ist das Recht mit den technologischen Implementierungsmöglichkeiten nicht von der Aufgabe befreit, strukturierende Vorgaben für Personendatenflüsse zu definieren. Die Technologien können in der Folge einen Beitrag leisten, die rechtlichen Vorgaben umzusetzen.[1618] 1202

1615 Vgl. BR, Schlussbericht Evaluation 2011–1952, 335 ff., 343, 347, 349; als vollkommen genügend beurteilt Rosenthal das aktuelle Regime des DSG und äussert sich entsprechend kritisch zur Totalrevision, Jusletter vom 20. Februar 2017, N 1 ff.; schon früh forderte den verbesserten Datenschutz qua Technologien Rudin, digma 2001, 126 ff., 128.

1616 Vgl. Belser, in: Datenschutz-Forum Schweiz, 1 ff.; EJPD, Bericht Begleitgruppe, 1 ff., 10; Morscher, ZBJV 2011, 177 ff., 178, wobei der Autor vertritt, dass die Schweiz ein hohes Datenschutzniveau verbürge, 180; die Technikneutralität werde auch im Zuge der Totalrevision beibehalten, vgl. Benhamou/Tran, sic! 2016, 571 ff., 572.

1617 Zur Stärkung der technischen Datenschutzlösungen qua DSGVO Schweighofer, Jusletter IT vom 9. Februar 2016, N 7; in Bezug auf das Urheberrecht und die hohe Bedeutung technischer Schutzmassnahmen vgl. Bechtold, 3 ff.; zu den sog. PETs, den Privacy Enhancing Technologies, und der Frage nach ihren wirtschaftlichen Vorteilen vgl. London Economics (Hrsg.), *passim*; zum Datenschutz durch Technik auch Schaar, 220 ff.; zum Datenschutz durch Technik gemäss DSGVO Jandt, DuD 2017, 562 ff.; vgl. dazu, dass für eine bessere privacy im Internet die Gesetzgebungen, aber auch die Suchmaschinenbetreiber selbst mittels Neuerungen der Policies nur wenig erreichen, allerdings technische Mechanismen bedeutsam sind, Howe/Nissenbaum, in: Kerr/Steeves/Lucock (Hrsg.), 417 ff., 419 ff.

1618 Namentlich im Zuge der jüngsten rechtlichen Neuerungswelle erlangen technologische Instrumente zur Implementierung des Datenschutzrechts neue Bedeutung. Zu nennen sind insofern neben «privacy by design» und «privacy by default» die Anonymisierung, aber auch die Datenschutz-Folgenabschätzung; zur Gewährleistung des Rechts auf Löschung qua Technologien Hunziker, 118 ff.; vgl. im Zusammenhang mit dem Webtracking Howe/Nissenbaum, in: Kerr/Steeves/Lucock (Hrsg.), 417 ff., 421 ff., auch mit Hinweis auf die wissenschaftliche Diskussion zur Politik qua Technologie, 430 f.

1203 Für die Gestaltung eines Datenschutzrechts, das wirksam seine Ziele zu erreichen vermag, ist ein vertieftes Verständnis der *faktischen Herausforderungen des zeitgenössischen Datenschutzrechts* unabdingbar. An dieser Stelle ist anzufügen, dass es durchaus seit Längerem kritische Stimmen zum Konzept des DSG gibt. Die Totalrevision wird indes an den das geltende schweizerische DSG prägenden, im zweiten Teil dieser Arbeit herausgearbeiteten Strukturelementen festhalten, gleichwohl markante Kontrapunkte setzen. Bevor auf diese Neuerungen einzugehen ist, findet nachfolgend eine Auseinandersetzung mit den *faktischen Herausforderungen* des zeitgenössischen Datenschutzrechts statt. Zunächst wird ein genaueres Verständnis der *neuen Datenverarbeitungstechnologien* generiert. Alsdann kommt es zu einer Analyse des *Trends der Kommerzialisierung* von Personendaten. Mit diesen Ausführungen wird der Boden bereitet, um im VIII. Kapitel dieses dritten Teils die jüngsten Gesetzesneuerungen sowie die wissenschaftlich präsentierten Lösungsansätze zur Neugestaltung des Datenschutzrechts zu reflektieren. Hieraus wird alsdann die Ableitung eines neuen datenschutzrechtlichen Paradigmas möglich.

B. Faktische Herausforderungen – Vertiefung

> «Bei der Bearbeitung von Technik im Recht sind den Juristen Grenzen gesetzt. Sie müssen sich auf das Wissen der Ingenieure und Techniker stützen. So hält Meili in seiner Abhandlung über Stark- und Schwachstromanlagen fest: „Auf das Detail der technischen Vorschriften einzugehen, fehlt mir natürlich jede Kompetenz".»[1619]

1204 *An erster Stelle der faktischen Herausforderungen*, denen das Datenschutzrecht (und seine Wirksamkeit) unserer Tage begegnet, stehen *die technischen Entwicklungen*. Nachfolgend geht es darum, die informationstechnologischen Prozesse in einer auch für Rechts-, Geistes- und Sozialwissenschaftlerinnen nachvollziehbaren Weise zu beschreiben. Dabei soll das positive wie auch das negative Potential neuer Informationsverarbeitungstechnologien freigelegt werden.[1620] Zu den ausserrechtlichen Herausforderungen gehört *an zweiter Stelle die Transformation von (Personen-)Daten in Güter*, was vom Internet vorangetrieben wird und das geltende Datenschutzrecht auf eine harte Probe stellt.[1621]

1205 Beide Elemente – neue technologische Potenzen und Kommerzialisierungstendenzen – veranlassten bereits Warren/Brandeis dazu, den Schutz des Privaten auch im Privaten zu proklamieren. Eindrücklich haben sie nicht nur die disruptive

1619 Vgl. unter Zitierung von Meili Dommann, SZG 2005, 17 ff., 22.
1620 Hierzu namentlich Nissenbaum, 19 ff.
1621 Dazu insb. Vesting, in: Ladeur (Hrsg.), 155 ff., 168 ff.

Kraft neuer Technologien beschrieben.[1622] Sie haben ebenso den erodierenden Einfluss wirtschaftlicher Begehrlichkeiten auf den privaten Lebensbereich thematisiert: Die Presse nutze die (verwerfliche) «Neugier des einfachen Volkes» aus, um erkleckliche Gewinne aus der Publikation und Verbreitung privater Bilder und Geschichten aus dem persönlichen und familiären Lebensbereich zu generieren. Warren/Brandeis war diese Verbreitung und Ökonomisierung «privater Informationen» durch die Boulevardpresse ein Dorn im Auge, die ihrerseits erst durch den Zeitungsdruck und die Fotografie möglich geworden war.[1623]

Heute sind es längst nicht mehr nur die Eliten oder Prominente, die damit be- 1206
schäftigt sind, ihr Bildnis, ihre Stimme, ihren Schriftzug, ihre Lebens- und Familiengeschichte – allesamt personenbezogene Daten – zu schützen und die sog. Fremd- oder Zwangskommerzialisierung zu verhindern resp. die entsprechenden Personendaten zu kommerzialisieren (Eigenkommerzialisierung).[1624] Längst gibt «Otto Normalverbraucher» seine personenbezogenen Angaben preis, um im Gegenzug in den Genuss von Rabatten, Gutscheinen oder Diensten zu kommen.[1625] Doch bevor auf die Kommerzialisierung personenbezogener Angaben als hoch relevante Herausforderung des aktuellen Datenschutzrechts eingegangen wird, sollen vorab die aktuellen *Datenverarbeitungstechnologien* anhand ihrer *charakteristischen Möglichkeiten* beschrieben werden. Denn:

> «Die Befunde der Evaluation deuten […] darauf hin, dass sich die Bedrohungen für den Datenschutz aufgrund der fortschreitenden technologischen und gesellschaftlichen Entwicklungen seit einigen Jahren akzentuieren. Die technologischen Entwicklungen fordern das Datenschutzgesetz heraus, weil sie zu einer Zunahme von Datenbearbeitungen und zu intransparenten sowie verstärkt zu grenzüberschreitenden Datenbearbeitungen geführt haben. Ausserdem wird es immer schwieriger, die Kontrolle über einmal bekannt gegebene Daten zu behalten.»[1626]

1. Potenzen der neuen Technologien

Im Schlussbericht zur Evaluation des eidgenössischen Datenschutzgesetzes wer- 1207
den die neuen Technologien anhand von *vier Aspekten* charakterisiert.[1627]

1622 Hierzu auch Nissenbaum, 21; vertiefend Warren/Brandeis, Harv. L. Rev. IV./5/193, 193 ff., 195 ff.
1623 Interessant zur Fotografie, Tonaufnahmen sowie Filmen sowie zu Malerei und Schrift als externes Gedächtnis, auch mit historischen Bezügen, Mayer-Schönberger, Delete, 40 ff., insb. 59 ff.
1624 Eine gute Übersicht zur Kommerzialisierung des Persönlichkeitsrechts mit den rechtlichen Standpunkten findet sich z. B. bei Büchler, AcP 2006, 300 ff.; Dies., in Honsell/Portmann/Zäch/Zobl (Hrsg.), 177 ff.; Emmenegger, in: Gauch/Pichonnaz (Hrsg.), 209 ff.; Glaus, 5 f. und 99 beschreibt das Recht am eigenen Wort als Teil des informationellen Selbstbestimmungsrechts; zur unlauteren Werbung mittels Bildnissen Prominenter Beuthien/Hieke, AfP 2001, 353 ff.; grundlegend zu einem Persönlichkeitsschutz mittels Persönlichkeitsgütern Beuthien/Schmölz, *passim*.
1625 Hierzu auch Buchner, 148 ff.
1626 BR, Schlussbericht Evaluation 2011–1952, 335 ff., 336.
1627 Bolliger/Féraud/Epiney/Hänni, 23 ff.

Erstens wird die *zunehmende Leistungsfähigkeit* und Speicherkapazität von Computern sowie die steigende Übertragungseffizienz in Netzwerken genannt: Datenverarbeitungen – Erhebungen, Verknüpfungen sowie Übermittlungen – sind technisch betrachtet kaum mehr Restriktionen unterworfen. *Zweitens* wird *die gesteigerte Miniaturisierung und Digitalisierung* genannt, wobei mittlerweile in unzähligen Alltagsgeräten Datenverarbeitungstechnologien integriert sind («ubiquitous computing») – von der Kaffeemaschine und dem Staubsauger über das Handy, das als kleiner Computer längst mehr als ein mobiles Telefon ist und in sich unzählige Funktionen wie Kamera, Kommunikationsmedium, Taschenrechner usf. vereint, bis hin zum Auto, in dessen Lenkrad eine Kamera integriert sein kann, welche die Pupillenaktivität der fahrenden Person registriert und Meldungen an die Polizei oder Versicherung erstatten könnte, um nur einige Applikationen zu nennen.[1628] Folglich zeigt sich das Bild heute ganz anders als dasjenige in den Anfängen von Personendatenverarbeitungsanlagen, die wie Fabrikgebäude auf eigenen Arealen isoliert waren und in aller Regel vom Staat betrieben wurden.[1629] Längst trägt der einzelne Mensch in Gestalt von Uhren, Brillen oder Natels winzige, aber hoch effiziente Datenverarbeitungszentralen auf sich, die in stetem Austausch mit anderen Geräten und Netzen stehen. *Drittens* gilt die damit zusammenhängende *massenhafte Datenverarbeitung* als charakteristisch. Sie resultiert daraus, dass immer mehr Personen immer mehr Alltagsgeräte nutzen, die ebenso als Datenverarbeitungszentralen fungieren. Die so generierten Personendaten werden digital erfasst und – unterstützt von zusehends verknüpften Speichermedien – vernetzt. Und *viertens* sind die *Auswertungsmöglichkeiten* präziser und umfassender geworden.[1630]

1208 Mit dieser Beschreibung der Technologien anhand von vier Charakteristika teilweise vergleichbar ist die Nomenklatur, wie sie Nissenbaum in ihrem richtungsweisenden Werk «Privacy in Context» vorschlägt.[1631] Sie beschreibt die neuen Informationsverarbeitungstechnologien mittels *dreier Kernkapazitäten*. Die *erste* steht unter dem Titel des «*Tracking and Monitoring*» – also das Nachverfolgen und Beobachten, beispielsweise mittels Kundenkarten für «frequent shoppers», Telefon-Apps, die dazu dienen, Kinder zu überwachen, Videoüberwachungen im öffentlichen Raum[1632], E-Mail-Überwachungen am Arbeitsplatz u. a. m. *Die zweite Kernkapazität* stellt sie unter die Stichworte von «*Aggregation and*

1628 Vgl. zu weiteren Beispielen vgl. Mattern, in: Mattern (Hrsg.), 11 ff., insb. 13.
1629 Vesting, in Ladeur (Hrsg.), 155 ff., 165 ff.; Nissenbaum, 1; vgl. zur Informatisierung des Alltags die verschiedenen Beiträge in Friedemann (Hrsg.), *passim*.
1630 Bolliger/Féraud/Epiney/Hänni, 23 ff.
1631 Vgl. Nissenbaum, 21 ff.; wenn auch auf das Subjekt ausgerichtet findet sich ein Plädoyer für die Anerkennung ausdifferenzierter Privatheitsinteressen auch bei Samuelson, Stan. L. Rev. 2000, 1125 ff., 1171 f.
1632 Zur Videoüberwachung insb. im Lichte der verfassungsrechtlichen Vorgaben Flückiger/Auer, AJP 2006, 924 ff.

Analysis»: Erfolgte die massenweise Erhebung, Aggregierung und Auswertung von Personendaten in den Anfängen der Informationsverarbeitungstechnologien durch den Staat, ist sie heute ein zentrales Element auch zur Wirtschaftlichkeitssteigerung von privaten Unternehmen geworden. Die *dritte Kernkapazität* beschreibt Nissenbaum unter der Wendung «*Dissemination and Publication*»: Gerade durch das Internet ist die Verteilung sowie der «Access» zu Informationen weder zeitlichen noch mengenmässigen Schranken unterworfen. Diesen drei Kernkapazitäten widmen sich die folgenden Seiten, nicht ohne zweierlei vorauszuschicken:

Zum einen werden aktuelle Informationsverarbeitungstechnologien in ihren drei Kernkapazitäten in der Regel *nicht isoliert genutzt*. Vielmehr werden sie oft miteinander *kombiniert*.[1633] Mittels Tracking und Monitoring erhobene Personendaten werden meist aggregiert sowie ausgewertet und in der Folge weiterverteilt sowie publiziert. Durch diese Kombinationen von «Features» verändert und potenziert sich nicht bloss die Quantität sowie Qualität der verarbeiteten Personendaten, vielmehr transformiert sich dadurch die Topografie der Verarbeitungsprozesse. Inhalt und Auswirkungen der Personendatenverarbeitungen verändern sich grundlegend. 1209

Zum anderen stossen keineswegs alle neuen Personendatenverarbeitungstechnologien auf gesellschaftlichen Widerstand. Vielmehr lassen sich solche identifizieren, die von der Gesellschaft weitgehend akzeptiert und gebilligt werden, wohingegen andere technologieunterstützte Praktiken vehement abgelehnt werden. Diese *unterschiedlichen gesellschaftlichen Reaktionen* nutzt Nissenbaum als Metrum, um ihr Konzept «Privacy in Context» zu entfalten.[1634] Die Autorin legt somit eine Studie vor, der es gelingt, transversal die für das Datenschutzrecht relevanten Aspekte der Technologie, Soziologie, Philosophie sowie des Rechts zu inkludieren und vernetzt zu analysieren. 1210

1633 Vgl. Nissenbaum, 62 ff.; vgl. zur Sammlung und Verteilung von Informationen Schwartz, Harv. L. Rev. 2004, 2055 ff., 2055 f.; immerhin ist darauf hinzuweisen, dass z. B. die steigende Speicherkapazität und damit Aggregierung sowie Zirkulation und damit Verteilung bereits in den 1970er Jahren als Strukturwandel bei der Personendatenverarbeitung umschrieben wurde; vgl. hierzu Mallmann, 12 ff.

1634 Dies., 3, 142, 158, 181 ff., 186 ff., 235; dazu, dass Personendatenverarbeitungen bei den einzelnen Individuen unterschiedliche Reaktionen auslösen, Litman, Stan. L. Rev. 2000, 1283 ff., 1284 f.; für den kontinental-europäischen Raum wies Mallmann, 36 ff. auf die Einschlägigkeit der gesellschaftlichen Ausdifferenzierung auch für das Datenschutzrecht hin.

1.1. Drei Kernkapazitäten neuer Datenverarbeitungstechnologien

1.1.1. Tracking und Monitoring

1211 Die Verdichtung der kontinuierlichen Fremd- und Selbstbeobachtung im Rahmen von Tracking- und Monitoring-Technologien lässt sich für die *analoge wie digitale Welt* beschreiben.[1635] Neue Informationsverarbeitungstechnologien operieren multimodal und ubiquitär, indem sie Bilder, Geräusche, Gerüche, Temperaturen, Druck usf. registrieren. So generierte Informationen können miteinander kombiniert werden.[1636] Visuelle Aufnahmen erfolgen mit deutlich besserer Auflösung, Kameras haben markant weitere Aufnahmewinkel mit Schwenk- und Drehköpfen (Rotationen um 360 Grad) und verbesserte Linsen, die Speicherungsmengen sind durch Kompressionstechniken und Digitalisierung potenziert. Multifunktionalkameras integrieren neben Bild- auch Geräuschaufnahmen, haben einen Helligkeits- und Wärmesensor sowie eine Alarmfunktion integriert, wobei die Aufnahmen direkt auf das Notebook oder iPhone gestreamt werden können. Bild- und Tonaufnahmen lassen sich damit in Echtzeit zur Kenntnis nehmen oder über Netzwerke verteilen. Beobachtungen erfolgen einmalig oder kontinuierlich, beispielsweise solange man im «Fokus» eines Instrumentes steht, und/oder systematisch. Es gibt heutzutage kaum einen Raum oder gesellschaftlichen Bereich, in dem solche Technologien nicht zum Einsatz kommen: vom Arbeits- zum Flugplatz, vom Schul- zum Handelsplatz, vom Hauseingang zum Balkon. Namentlich kritische Infrastrukturen wie Energie-, Kommunikations-, Transport- und Finanznetzwerke werden durch computergesteuerte Überwachungssysteme, die Bewegung, Berührung, Licht, Wärme usf. kontrollieren, geschützt.[1637] Jüngst wird der visuellen, auditiven, haptischen, physikalischen (Licht und Wärme) Er-

1635 Vgl. spezifisch für das Webtracking jüngst Wenhold, *passim*; zum Webtracking und den Widerständen dagegen Howe/Nissenbaum, in: Kerr/Steeves/Lucock (Hrsg.), 417 ff.; zum Tracking qua Videoüberwachung öffentlicher Räume Weydner-Volkmann/Feiten, digma 2019, 218 ff., 219 ff., auch mit Hinweis auf eine sog. digitale Tarnkappe, welche eine informationelle Gewaltentrennung ermöglichen soll; Schwartz, Wis. L. Rev. 2000, 743 ff., 746 ff. beschreibt die weitangelegte elektronische Überwachung in der Online- und Offline-Welt als Hauptrisiko für die privacy; vgl. zur irrtümlicherweise angenommenen Anonymität im Internet Bergelson, UC Davis L. Rev. 2003, 379 ff. und 451; zu den digitalen Spuren sowie weiteren Überwachungsprozessen wie Videoüberwachungen auch Schaar, 42 ff.; Monitoring-Technologien wurden allerdings bereits in den 1960er Jahren eingesetzt – und als problematisch beurteilt, vgl. Fried, Yale L.J. 1968, 475 ff., 476 ff.; Solove, Stan. L. Rev. 2001, 1393 ff., 1419 ff. legt dar, warum der Fokus auf den Überwachungsaspekt zu kurz greift, wobei er die Ersetzung der Big-Brother-Metapher durch diejenige von Kafkas Prozess vorschlägt: Das Problem von Datensammlungen liege in der ungenügenden Entscheidungspartizipation mit Blick auf eigene Informationen, womit eine Entmachtung einhergehe; jüngst zum Tracing im Rahmen der digitalen Massnahmen zur Bekämpfung der COVID-19-Pandemie Vokinger, SJZ 2020, 412 ff.; Schuler-Harms, in: Sokol (Hrsg.), 5 ff.

1636 Vgl. Nissenbaum, 22 ff.; vgl. auch Flückiger/Auer, AJP 2006, 924 ff., 925 f.

1637 Vgl. Furrer/Angwert, NZZ vom 25. Februar 2019; zu den Schwachpunkten des Schutzes der kritischen Infrastruktur in der Schweiz jüngst Mäder, NZZ vom 2. Juli 2021.

fassung eine weitere «Sinneskomponente» hinzugefügt mittels sog. chemischer Sensoren, mittels derer Umweltfaktoren analysiert werden können.[1638]

Nicht wenige dieser Monitoring- und Tracking-Instrumente sind durch *Radio-* 1212
frequenzsysteme verbunden. Damit wird ein *Transfer* der erhobenen Daten in Echtzeit möglich. Hieran anschliessend lässt sich umgehend sowie teilweise automatisiert eine Reaktion auslösen.[1639] Radiofrequenztechnologien wurden von den USA bereits im Zweiten Weltkrieg eingesetzt, um eigene Flugzeuge von denen feindlicher Nationen unterscheiden zu können.[1640] Mittlerweile haben sich die Radiofrequenztechnologien stark verbessert und verbilligt. Heute finden sie in weiten Feldern Einsatz. Sie funktionieren über Radiowellen, wobei über Mikrochips sowie Mini-Antennen der Austausch von Signalen zwischen Sender und Empfänger bewerkstelligt wird. Entsprechend konfiguriert sich in aller Regel ein RFID-Transponder aus einem Mikrochip, der zusammen mit einem Koppelungselement, einer Antenne oder Spule auf einem Trägerelement angebracht ist, womit Daten kommunizierbar werden.[1641] Transponder weisen unterschiedliche Speicherkapazitäten auf und können mit Sensoren ergänzt werden, die beispielsweise die Temperatur messen. Folglich lassen sich z. B. Lebensmittel, aber auch Tiere und Menschen sowie deren «Zustand» mittels Radiofrequenzidentifizierungstechnologien berührungslos und automatisch lokalisieren, identifizieren und analysieren.[1642] Eine besondere Rolle kommt ihnen heute bei der Kontrolle von Strassenverkehrsnetzen und der Durchsetzung von Strassenverkehrsregulierungen zu, namentlich in Gestalt von elektronischen Zugangskontrollen, Kraftfahrzeug-Wegfahrsperren oder Mautsystemen.[1643] Zudem wird die Radiofrequenztechnologie im Rahmen von biometrischen Pässen mit ihrem Chip genutzt, die in zahlreichen Staaten eingeführt wurden.[1644] Auch in der Schweiz wird seit 2010 der biometrische Pass emittiert.[1645] Mit diesem wird jüngst die Einführung der E-ID assoziiert, bei der es indes nicht um die staatlichen Identitätsausweise geht.[1646]

1638 Vgl. Nissenbaum, 23; zu den Smart-City-Technologien «Die Stadt bekommt Augen, Ohren, Tastsinn und sogar Geruchsinn», Grassegger, 43: So kann die Luftbelastung gemessen und mit Fahrverboten beantwortet oder die Strassenoberflächentemperatur gemessen und mit einer automatisierten Salzeinstreuung reagiert werden. Das Verkehrs- und Strassennetz kann als illustratives Beispiel für die «transformative» Kraft von Überwachungssystemen gelten.

1639 Schmitt, 19 ff., 83 ff.

1640 Nissenbaum, 31; Schmitt, 1.

1641 Schmitt, 14.

1642 Zum Ganzen Nissenbaum, 31 ff.

1643 Schmitt, 1; hierzu auch Schaar, 66 ff.

1644 Auswärtiges Amt, Häufig gestellte Fragen, Was ist ein biometrischer Pass? Was ist ein ePass?, Berlin 2021, <http://www.auswaertiges-amt.de/DE/Infoservice/FAQ/Reisedokumente/08a-BiometrischerPass.html?nn=383016> (zuletzt besucht am 30. April 2021).

1645 Ch.ch, Pass oder Identitätskarte beantragen (bestellen), Bern 2021, <https://www.ch.ch/de/pass-identitatskarte-beantragen/> (zuletzt besucht am 30. April 2021).

1646 Bundesamt für Justiz, Bundesgesetz über elektronische Identifizierungsdienste, Bern 2018, <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html> (zuletzt besucht am 30. April 2021).

1213 Die Technologie der Radiofrequenzidentifikation ist keineswegs bloss für die Erfüllung staatlicher Verwaltungsaufgaben relevant. Gerade auch für die Forschung und Industrie hat sie hohe Bedeutung. Unternehmen der unterschiedlichsten Branchen versprechen sich von Radiofrequenztechnologien eine gesteigerte Prozesseffizienz, die verbesserte Regalverfügbarkeit von Produkten sowie wirkungsvolle Methoden zur Bekämpfung von Fälschungen.[1647] Im Supply Chain Management eingesetzt, können Güter resp. Produkte entlang ihres Transportes über den gesamten Verteilungskanal hinweg beobachtet werden.[1648] Auf diese Weise werden beispielsweise Medikamente vom Verlassen der Fabrik bis zum «konsumierenden Patienten» getrackt. Die Technologie ermöglicht es, ein bestimmtes Produkt nachzuverfolgen und seinen Verbleib im System resp. Prozess zu eruieren. Im Gesundheitssektor kann sie z. B. dazu nutzbar gemacht werden, schwer kranke Menschen ausfindig zu machen und deren Versorgung wieder sicherzustellen.[1649]

1214 *Tracking- und Monitoring-Technologien* werden somit für mannigfache Zwecke nutzbar gemacht. Sie dienen der Terrorbekämpfung, Aufdeckung und Verhinderung von Straftaten, der Optimierung der Geschäftsgänge und Verbesserung der gesundheitlichen Versorgung.[1650] Längst ist es nicht mehr nur der Staat, der mit gut sichtbaren Videokameras das Treiben der Menschen auf öffentlichen Plätzen registriert, um allfällige Straftaten oder Terroranschläge zu verhindern resp. aufzuklären. Vielmehr ist die Welt gefüllt mit Geräten, Systemen und in Systemen eingebetteten Geräten, die Menschen und ihr Verhalten beobachten.[1651] Technologien mit Beobachtungskapazität sind mittlerweile so klein, dass sie ohne Probleme in Geräte, die eine andere Primärfunktion aufweisen, in Hilfsmittel oder unter die Haut von Mensch und Tier gesetzt werden können. Eine Vielzahl der Sensoren und Detektoren sind für den Menschen kaum mehr wahrnehmbar.[1652]

1215 Obschon klein und in Alltagsgeräte und -prozesse migriert, sind die Datenverarbeitungskapazitäten nicht nur, was die Geschwindigkeit anbelangt, sondern auch, was die Speicherkapazitäten sowie die Vernetzung angeht, hoch effizient. Viele dieser Technologien sind in Netzwerke integriert. Registriert werden können nicht nur Bilder und bewegte Bilder, sondern auch Akustik, Temperaturen, Licht, Berührungen und entsprechend Wellen, Aggregatzustände, Stoffkonzentrationen usf. Menschen, Tiere und Produkte werden oder können heute umfassend, billig, schnell und mit weiteren Angaben abgeglichen und beobachtet werden.

1647 Schmitt, 1 ff.
1648 Vgl. London Economics (Hrsg.), 20 ff.
1649 Schmitt, 14.
1650 Vgl. Schaar, 124 ff.
1651 Nissenbaum, 21.
1652 Dies., 23; vgl. zur Miniaturisierung auch Mattern, in: Mattern (Hrsg.), 11 ff., 11.

Tracking- und Monitoring-Technologien lassen Kategorien sichtbar werden, welche die Subjekt-Objekt-Verhaftung, die das geltende Datenschutzrecht prägt, durchkreuzen. Die Tracking- und Monitoring-Kapazitäten moderner Informationsverarbeitungstechnologien drängen die Kategorien von *Netzwerken und Infrastrukturen*, innerhalb derer Informationsflüsse stattfinden, in den Vordergrund.[1653] Mit einer solchen Betrachtungsweise rücken zugleich die *Grenzstellen* oder auch «Knotenpunkte» resp. Verbindungsstellen sowie die hier «geschalteten» Flüsse von Personendaten in das Zentrum des Interesses auch einer datenschutzrechtlichen Analyse.[1654] 1216

Die Relevanz der Kategorien von Netzwerken und Infrastrukturen, in welchen die Knotenpunkte als die eigentlichen Brennpunkte zu identifizieren sind, sollen anhand *zweier Beispiele veranschaulicht werden*. Von diesen geht ein richtungsweisender Impuls aus, um einen Perspektivenwechsel für das datenschutzrechtliche Regime anzustossen. Das erste Beispiel entstammt der Offline-Welt und nimmt die Überwachung von Strassenverkehrsnetzen in den Blick. Das zweite Beispiel ist das Online-Tracking im Internet.[1655] 1217

Im *Strassenverkehr sind es die sog. Toll-Stations oder Mautstellen*, die auch informationelle Funktionen wahrnehmen. Anders als der Flugverkehr war der Strassenverkehr lange nur beschränkt im Visier der Überwachungstechnologien. Allerdings wird zusehends auch das Strassenverkehrsnetz direkter und indirekter technischer Beobachtung unterstellt. Früher fand eine Beschränkung auf die Kontrolle von Fahr(zeug)ausweisen und Versicherungsdeckungen statt. Heute hat sich das Bild – wenn auch vielleicht weniger in der Schweiz, so doch in den USA – grundlegend verändert.[1656] An sog. Toll-Stations resp. Mautstellen werden Gebühren oft automatisiert qua Kreditkartenzahlung beglichen. Informationell weiter gehen Systeme, die mit Radiofrequenz ausgestattet sind. Bei ihnen werden registrierte Fahrzeuge im Moment ihrer Passage an einer bestimmten Stelle in das System «eingeloggt». In der Folge werden die zurückgelegte Strecke und die entsprechenden Gebühren erhoben. Auch die Geschwindigkeiten 1218

1653 Vgl. zur konnexionistischen Struktur des Internets Vesting, in: Ladeur (Hrsg.), 155 ff., 162 f.; Datenflüsse zum Betrachtungsgegenstand macht Helfrich, 29; zur informationellen Selbstbestimmung in Netzwerken Maisch, *passim*.

1654 Ladeur, Vortrag, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021); Nissenbaum, 23.

1655 Zu diesem auch Bucher, 9 ff.; Heinzmann/Bänziger, digma 2001, 134 ff.; Eifert, NVwZ 2008, 521 ff. auch mit Hinweis auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und die bundesverfassungsgerichtliche Rechtsprechung; Bergelson, UC Davis L. Rev. 2003, 379 ff.; Howe/Nissenbaum, in: Kerr/Steeves/Lucock (Hrsg.), 417 ff.

1656 Hierzu Nissenbaum, 25 ff.; vgl. zu den Entwicklungen den Überblick über die Beiträge zu Personendatenverarbeitungen im Zusammenhang mit der Nutzung von Autos Rudin, digma 2007, 88 f.

der Fahrzeuge auf den jeweiligen Streckenabschnitten werden ermittelt. Zudem werden Strassen, Kreuzungen, Ampeln usf. mittels Videokameras überwacht. Zudem sind die Fahrzeuge selbst heutzutage mit technischen Systemen ausgestattet, die Geschwindigkeiten, Anschnallverhalten, Beschleunigung usf. registrieren und aufzeichnen.[1657] GPS-Systeme, die primär dazu dienen, der Lenkerin den Weg zu weisen, können dergestalt konfiguriert sein, dass sie das Tracking des Fahrzeuges durch Dritte ermöglichen. In den USA wie in Grossbritannien hat sich darüber hinaus ein Modell der automatisierten Fahrzeugnummernerkennung etabliert,[1658] womit täglich mehrere Millionen Bilder von Fahrzeugnummern im nationalen Polizeicomputersystem ausgewertet werden können und Fahrzeuge resp. deren Führer, die in Verbindung mit einem Kriminalfall gebracht werden, identifizierbar werden. In der Schweiz arbeitet namentlich das Grenzwachkorps mit Kameras und einer automatisierten Fahrzeug- und Verkehrsfahndung.[1659] Jüngst ist Belgien dazu übergegangen, seine Grenzen mit entsprechenden Systemen zu überwachen.[1660] Zugleich werden Applikationen entwickelt, die den Autofahrenden umfassende Informationen zu Motor, Staumeldungen, Strassenzuständen, Objekten auf der Strasse, abrupten Beschleunigungen in der Kolonne usf. melden. All dies wird durch dahinterstehende Netzwerke ermöglicht, in denen relevante Daten abgeglichen, ausgetauscht, ausgewertet und übermittelt werden. Mit diesen Entwicklungen lässt sich die Transformation eines Systems beschreiben, das ursprünglich primär auf die Gewährleistung der Strassensicherheit und des Transportes ausgerichtet war, in ein umfassendes System der Überwachung und informationellen Auswertung. Damit wird nicht nur die Rechtsdurchsetzung des Staates – über diejenige der Strassenverkehrsregulierung hinausgehend, z. B. die Fahndung nach Personen, die verdächtigt werden, anderweitige Delikte begangen zu haben – unterstützt. Selbst privatwirtschaftliche Unternehmen machen sich solche Systeme zunutze, indem sie beispielsweise Werbung für Restaurants oder Einkaufszentren in der Nähe des übermittelten Standortes im GPS schalten.

1219 Nicht nur das Strassennetz der Offline-Welt, auch in der Online-Welt werden Aktivitäten, Kommunikationen und Interaktionen der Nutzerinnen und Nutzer

1657 Zu den sog. intelligenten Fahrzeugen mit ihren digitalen Spuren vgl. Arnold, Jusletter IT vom 24. November 2016.

1658 Wikipedia, Automatische Nummernschilderkennung, Februar 2021, <https://de.wikipedia.org/wiki/Automatische_Nummernschilderkennung> (zuletzt besucht am30. April 2021); Nissenbaum, 26.

1659 Das Bundesgericht befand unlängst in diesem Zusammenhang, dass eine Praxis des Kantons Thurgaus unzulässig sei, vgl. BGer 6B_908/2018, Urteil vom 7. Oktober 2019; Gerny, NZZ vom 28. Oktober 2019, Fahrzeugfahndung darf nicht zur totalen Überwachung führen, <https://www.nzz.ch/schweiz/bundesgericht-stellt-automatisch-fahrzeugfahndung-infrage-ld.1517764?reduced=true (zuletzt besucht am 30. April 2021).

1660 <https://www.luxprivat.lu/news/detail/belgien-sichert-grenzen-mit-kameras-luxemburg-> (zuletzt besucht am 20. September 2021).

getrackt und gemonitored.[1661] Paradoxerweise ist es ausgerechnet im *Cyberspace*, wo Nutzende fälschlicherweise davon ausgehen, im «stillen Kämmerlein» des Zuhauses anonym und unbeobachtet zu agieren.[1662] Anders als beim Monitoring im Offline-Bereich, das die Implementierung signifikanter Einrichtungen sowie Prozesse und damit einen beträchtlichen Aufwand bedingt, machen im Internet bereits marginale Anpassungen in vorhandenen Features nahezu sämtliche Aktionen umfassend scannbar: IP-Adressen und Cookies werden in die Systeme integriert und übernehmen die Registrierungsfunktion quasi *en passant*. Zwar werden noch heute beim Surfen regelmässig sog. dynamische IP-Adressen zugewiesen.[1663] Hierbei teilt der Access-Provider dem Internetnutzenden bei jedem Login ins Internet eine IP-Adresse quasi als «Einwegzugangscode» zu. Diese Adresse ist mit anderen Worten temporär, bei jedem Gang ins Internet wird eine neue, andere Adresse zugewiesen. Anders dagegen im «Real Space» mit seiner fixen Häusernummerierung oder dem stabilen Personenidentifikator. Der Internet-Anbieter weiss damit nicht unmittelbar, von wem die Seiten genutzt werden. Diese systembedingten «Nachteile» der dynamischen IP-Adressierung werden durch ein einfaches technisches Instrument mit dem verniedlichenden Namen «Cookie» kompensiert.

Anhand des Einsatzes von Cookies lässt sich eine Datenspur generieren, anhand 1220
derer ein Nutzer wiedererkannt wird und Angaben (Daten) zu seinem Verhalten, seinen Vorlieben und Interessen selbst im dezentral und netzwerkartig strukturierten Internet erhoben werden.[1664] Die Clickstream-Analyse, die schon früh Service/Access-Providern implementiert wurde, ermöglicht es beispielsweise Unternehmen wie Amazon, einer Person anhand einer Analyse ihres Surfverhaltens Kaufempfehlungen zu unterbreiten.[1665] Trotz variabler IP-Adresse ist nicht erst qua Registrierung mit identifizierenden Angaben durch Eröffnung eines Kontos ermittelbar, dass es eine ganz bestimmte Nutzerin ist, die wiederholt eine bestimmte Seite besucht. Es kann ebenso festgestellt werden, welche Inhalte und Unterseiten eines Unternehmens sie konsultiert oder bei welchem Produkt wie lange verweilt wird. Neuerdings kann namentlich auch erhoben werden, zwischen welchen Seiten verschiedener Unternehmen sie sich bewegt, mithin wie

1661 Vertiefend zum Webtracking Wenhold, 32 ff.; weiter hierzu Nissenbaum, 27 ff.; vgl. Web-Surfer mit Masken, Tracker lassen sich austricksen, NZZ vom 3. Juli 2019, 22.

1662 M. w. H. Nissenbaum, 27; zum Irrtum der Internetnutzenden, anonym zu agieren, mit Hinweis auf die berühmte Hunde-Karikatur im New Yorker, vgl. Waidner/Karjoth, digma 2004, 18 ff., 18.

1663 Zu statischen und dynamischen IP-Adressen sowie Spuren im Internet vgl. z. B. Köhntopp/Köhntopp, CR 2000, 248 ff.

1664 Zum Tracking mittels Cookies auch Heuberger, N 103 f.; Heinzmann/Bänziger, digma 2001, 134 ff.; Vesting, in: Ladeur (Hrsg.), 155 ff., 169 ff.; Waidner/Karjoth, digma 2004, 18 ff., 18; zu Cookies und ihrer DSGVO-konformen Verwendung vgl. Kessler/Oberlin, CB 2020, 63 ff., insb. 65 ff., wobei davon auszugehen ist, dass es der Einwilligung des Datensubjektes bedarf und ein Opt-out im Anwendungsbereich der DSGVO nicht rechtsgenügend ist.

1665 Nissenbaum, 29; Vesting, in: Ladeur (Hrsg.), 155 ff., 169 ff.

die «Reise» ausserhalb des Besuches auf der Website des eigenen Unternehmens weitergeht. Zwar können einzelne Anbieter jeweils nur Cookies für ihre eigenen Websites setzen. Allerdings wurden hier Strategien und Geschäftsmodelle entwickelt, um die «Surfhistorie» zu erheben, was durch ein dahinterliegendes Vertragsnetzwerk erreicht wird. Ein Beispiel ist das sog. AD-Netzwerk, das mit Cookies arbeitet und in welchem diverse Unternehmen Verträge schliessen, woraus ein informativer «Zusammenschluss» resultiert. Je grösser die Marktmacht der jeweils kontrahierenden Unternehmen, desto grösser der Datenpool zwecks Analyse.[1666] In diesem (Werbe-)Kontext agieren Dienste wie DoubleClick von Google, die als Vertragspartner das Surfverhalten von Internetnutzern zwischen verschiedenen Homepages registrieren und versprechen, das volle Potential des digitalen Marketings ausschöpfbar zu machen.[1667] Solche Geschäftsmodelle, die im Rahmen der Tracking- und Monitoring-Kapazität im Internet beschrieben wurden, stellen eine Herausforderung für das aktuelle Datenschutzrecht dar – auch wegen der Transformation von Daten in Wirtschaftsgüter.[1668]

1221 Einige Einsatzformen der Monitoring- und Tracking-Technologien, keineswegs aber alle, lösen *erheblichen Widerstand* aus:[1669] In Zeiten von Bedrohungen durch den Terrorismus werden öffentlich überwachte Plätze vom grossen Teil der Menschen hingenommen, um sich sicherer zu fühlen. Anders lösen Technologien wie beispielsweise Google Glasses, aber auch der Einsatz von RFID zur Nachverfolgung beispielsweise eines Medikamentes von der Produktion über das Warenhaus bis zum Endverbraucher Irritation aus. Gerade die Radiofrequenztechnologien, die zwar Verwaltungs- und Handelsprozesse effektuieren, gelten aufgrund ihrer effizienten und häufig nicht erkennbaren und durchschaubaren Trackingkapazitäten als Bedrohung für die Privatheit. Nicht nur, dass ihr Einsatz oft unbemerkt und intransparent geschieht. Die durch multimodale Technologien erhebbaren Angaben aus *diversen Verarbeitungszusammenhängen und Kontexten* lassen sich nahezu unbeschränkt miteinander verknüpfen, womit allem voran die Ausbeutung der mit den Tracking-Technologien generierten Angaben schier unbeschränkte Ausmasse annimmt. Die hier generierbaren (Personen-)Daten lassen sich selbstverständlich mit weiteren, anderweitig angelegten Datenpools anreichern.[1670] Nicht selten werden damit vorab zu einem bestimmten Zweck

1666 Hierzu Nissenbaum, 41 f.; Barocass/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 46; zum Handel mit Personendaten auf primären und sekundären Märkten vgl. auch Schmidt, digma 2019, 178 ff.

1667 Zum Online-Marketing mit seinen Herausforderungen vgl. auch Kollmann/Tanasic, digma 2012, 98 ff.; zum Webtracking durch Werbetreibende Langheinrich/Karjoth, digma 2012, 116 ff.; Solove, Stan. L. Rev. 2001, 1393 ff., 1403 ff., insb. 1412 ff.; Weber, digma 2012, 110 ff.

1668 Vesting, in: Ladeur (Hrsg.), 155 ff., 169 ff.; zur Kommerzialisierung der datenschutzrechtlichen Einwilligung Buchner, DuD 2010, 39 ff.

1669 Zur Relevanz der gesellschaftlichen Reaktionen auf gewisse technologische Möglichkeiten und Instrumente Nissenbaum, 3.

1670 Dies., 34 f.

etablierte Personendatenverarbeitungsprozesse – beispielsweise die Erfassung von Kreditkartenbezügen zwecks Abrechnung – auch zur Erreichung weiterer und anderer Zwecke eingesetzt – beispielsweise die Verhinderung von Delikten im Zusammenhang mit dem Kreditkarteneinsatz, die Unterbreitung von speziellen Angeboten und die passende Bewerbung. Die Varietät der Instrumente, mit denen Personen, ihr Verhalten und ihre Interessen über Raum und Zeit hinweg beobachtet werden, sowie der Informationen, die über sie generiert werden, ist gross. Entsprechende Features und Installationen sind tief in die Gesellschaft eingebettet, weisen diverse Funktionsweisen auf und vermögen diverse Zwecke zu erfüllen.[1671]

Aus einer datenschutzrechtlichen Perspektive stellen einige dieser technologiebasierten Beobachtungssysteme und -praktiken infolge der mit ihnen verbundenen Intransparenz sowie der Unmöglichkeit, diese Prozesse als Datensubjekt nachvollziehen zu können, eine Herausforderung dar. Wird zudem die anhand dieser ersten Kernkapazität der neuen Informationsverarbeitungstechnologien in den Vordergrund gerückte Kategorie der Netzwerkstruktur als zentraler Bezugspunkt der datenschutzrechtlichen Betrachtung identifiziert, zeigt sich die oftmals restriktionsfreie Verteilung an den Knotenpunkten zwischen diversen Systemen bereits *de lege lata* im Lichte des Grundsatzes der Zweckbindung als problematisch. 1222

Der Befund, wonach ursprünglich zu einem bestimmten Zweck generierte Personendaten potentiell beliebigen weiteren Systemen, Bereichen, Zwecken und Personen zugeleitet werden können, wird uns im Rahmen eines Vorschlages zur Rekonzeptionalisierung und Weiterentwicklung des Datenschutzrechts im IX. Kapitel dieses dritten Teils weiter beschäftigen. 1223

Hier soll an die erste Kernkapazität der neuen Informationsverarbeitungstechnologien – das Tracking und Monitoring, das längst im Alltag des Einzelnen angekommen ist – prozesshaft logisch die *zweite Kernkompetenz* angeschlossen werden: Die einmal generierten «Rohdaten» werden nunmehr in Datenbanken *gesammelt und ausgewertet*. 1224

1.1.2. Aggregierung und Auswertung

Die heutigen Aggregierungs-, Speicher-, Organisations- und Analysekapazitäten finden in technischer, zeitlicher, finanzieller sowie personeller Hinsicht kaum Schranken. Einmal erhobene (Personen-)Angaben können infolge digitaler Tech- 1225

1671 Nissenbaum, 20.

nologien effizient, umfassend und langfristig aggregiert werden.[1672] Speichermöglichkeiten sind günstig, Komprimierungstechniken hoch effizient. In der Folge lassen sich massive Datenbestände, -sammlungen und -banken erstellen, die aus diversen Quellen und Pools gespeist werden. Diese sind dynamisch und können beliebig zusammengelegt sowie ausgewertet werden.[1673]

1226 Die «Massivität» von Datenbanken wird anhand *zweier Kriterien* umschrieben. Sie sind kombinierbar:[1674] Unter dem Kriterium *«Weite»* resp. *«Breite»* werden Datensammlungen beschrieben, bei denen es darum geht, die Mitglieder eines Kollektivs so weit wie möglich lückenlos zu erfassen. Beispielsweise werden sämtliche Einwohner eines bestimmten Gebietes – allerdings nur hinsichtlich eines oder weniger Merkmale – registriert. Unter dem Kriterium *«Tiefe»* sind Datensammlungen nicht auf eine Erfassung einer möglichst grossen Anzahl von Personen ausgerichtet, sondern auf die Erfassung möglichst vieler Merkmale und Datenkategorien zu bestimmten Personen: Name, Wohnort, Geburtsdatum, Ausbildung, Beruf, Familienstand, Anzahl der Kinder, Hobbys, Betreibungen usf. Viele Datensammlungen sind sowohl *weit als auch tief* und zugleich dynamisch sowie – eine weitere Entwicklung – in Höchstgeschwindigkeit übertragbar und zusammenlegbar. Datenbestände, die sowohl breit (d. h., es werden sehr viele Personen erfasst) als auch tief sind (d. h., von den betroffenen Personen werden detaillierte, viele und tiefgreifende Angaben erfasst), gelten als besonders kontrovers.[1675]

1227 Das Internet stellt ein unerschöpfliches Reservoir dar, aus dem sich mittels Suchmaschinen Musik, Fotos, personenbezogene Angaben über bestimmte Personen usf. extrahieren lassen. Wie der geschichtliche Rückblick des ersten Teils zeigte, waren es früher Boten zu Fuss und zu Ross, die Informationen in Fuss- oder Reitgeschwindigkeit transportierten. Diese humanoiden Boten und deren animalische Träger mussten Pausen einlegen und stiessen auf manches Hindernis.[1676]

1228 Die Informationsmobilität wurde mit der Fortentwicklung und Standardisierung sowie Harmonisierung von netzwerkartigen Informationsübermittlungssystemen wie dem Internet transformiert: (Personen-)Daten und Informationen sind heute nicht nur von nahezu jedem Ort abrufbar, sondern auch von jedem Ort zu anderen Orten übermittelbar. Sie können in Höchstgeschwindigkeit über den ganzen Globus hinweg (und darüber hinaus) verbreitet und verteilt werden. Gleichzeitig kann von nahezu jedem Ort aus auf Datenbestände zugegriffen werden, die in

1672 Statt vieler vgl. z. B. Mayer-Schönberger, Delete, 64 ff. und 77 ff.; zu den enormen Kapazitäten elektronischer Datenverarbeitungstechnologien bereits Bull, Computer, 34 ff.; zur Aggregierung und Auswertung auch Dörflinger, 37 ff.
1673 M. w. H. Heuberger, N 30 ff.
1674 Vgl. Doug, 1 ff.; Nissenbaum, 36 ff., 41 f.
1675 Nissenbaum, 40 f.
1676 Vgl. erster Teil, I. und II. Kapitel.

Netzwerkknotenpunkten gespeichert sind. Namentlich digitale Informationsbestände lassen sich schnell, billig und in grossen Mengen überall hin verteilen und sind von nahezu überall her abrufbar.[1677]

Diese dynamische Dimension ist sowohl unter dem Titel dieser zweiten Kernkapazität der Aggregierung und Analyse relevant als auch unter der dritten Kernkapazität (dazu sogleich mehr). Mit anderen Worten hängen die zentralen Potenzen neuer Informationstechnologien oft eng zusammen, bedingen und effektuieren sich, bauen aufeinander auf: Je breiter und tiefer Bestände aggregiert, je schneller diese verbreitet und zusammengelegt werden können, desto grösser wiederum sind die resultierenden Datenbestände und das Analysepotential (Stichworte «Big Data» und «big is beautiful»). 1229

Vergleichbar mit der ersten Kernkapazität der neuen Informationsverarbeitungstechnologien, dem Tracking und Monitoring, ist zudem ebenso für die Aggregations- und Analysetechnologien ein Trend zu verzeichnen, der als «Demokratisierung» oder «gesellschaftliche Eigenaufrüstung» beschrieben wird.[1678] Ihr Einsatz ist längst nicht mehr nur staatlichen Organisationen oder Grossunternehmen vorbehalten, die in riesigen Rechenzentren Datenaggregierungen und -analysen durchführen. Vielmehr hat sich der Zugang zu diesen Technologien verbessert in dem Sinne, dass sie auf eine Vielzahl heterogener Nutzer – auch die Apotheke an der Ecke hat ein elektronisches «Treuekartensystem» entwickelt – expandiert sind.[1679] In der Folge haben sowohl die Quellen und Datenkategorien als auch die Nutzerinnen und Nutzer entsprechender Aggregierungs- und Auswertungstechnologien eine Diversifizierung erfahren. 1230

Tracking und Monitoring sowie die Aggregierung stellen den «Rohstoff» bereit, um *Auswertungen* vorzunehmen und Prognosen resp. Informationen zu generieren. Die Fortschritte im Rahmen von statistischen Auswertungen, der Computerwissenschaft, Kryptografie usf. haben dazu geführt, dass die Analysemöglichkeiten von (Personen-)Daten stark an Bedeutung gewonnen haben. Aus den Evaluationen weiter und tiefer Datenbestände lassen sich (mehr oder minder präzise) inhaltliche Folgerungen resp. Prognosen zu Vorlieben, Risiken oder dem (Entscheidungs-)Verhalten von Personen(gruppen) ziehen. Hierbei wird aus bereits beobachteten Verhaltensweisen, Befunden oder Präferenzen der Vergangenheit und Gegenwart auf solche der Zukunft geschlossen.[1680] Aus Daten (digital in Gestalt des Binärcodes) wird Information, aus Information Wissen gewonnen, 1231

1677 Meier, in: Meier/Fasel (Hrsg.), 1 ff.; m. w. H. auch Heuberger, N 30; Nissenbaum, 40 f.; zur Vernetzung sodann Brunner, Jusletter vom 4. April 2011, N 16.

1678 Vesting, in: Ladeur (Hrsg.), 155 ff., 169 ff.; Nissenbaum, 38; vgl. auch Rudin, digma 2001, 126 ff., 127 f.

1679 Nissenbaum, a. a. O; vgl. auch Bergelson, UC Davis L. Rev. 2003, 379 ff., 384 f.

1680 Nabeth, 31; vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff., 7022; Weichert, ver.di 2008, 12 ff., 12.

woraus entsprechende Planungen, Steuerungen und Entscheidungen abgeleitet werden.

1232 Solches, durch Analyseverfahren ermitteltes Wissen lässt sich in vielfacher Weise wirksam einsetzen, beispielsweise zur Prüfung der Bonität eines Kreditnachsuchenden, im Rahmen von Kundenbindungssystemen und personalisierter Werbung, bei der Evaluation von potentiellen gesundheitlichen Vorbelastungen aufgrund bestimmter Merkmale oder zur Wahl der individualisierten medizinischen Behandlung.[1681]

1233 Analysen und Auswertungen von Datenbeständen werden heute namentlich zur *Effizienzsteigerung* eingesetzt – in wirtschaftlicher Hinsicht, aber auch zur Effektuierung jeweils bereichsspezifisch verfolgter Ziele. Die Verfügbarkeit von tiefen und weiten Datenbeständen weckt eine diverse Bereiche durchdringende Nachfrage, die das Angebot an entsprechenden Methoden und Technologien weiter vorantreibt.[1682] Jedes Risiko scheint durch Rationalisierungsprozesse, wozu Daten und Informationstechnologien nutzbar gemacht werden, beherrschbar zu werden, beherrschbar werden zu müssen.[1683]

1234 Verspricht man sich von Aggregierungs- und Analyseverfahren in mehrfacher Richtung Effizienzsteigerungen, die durchaus auch im Interesse der von den Bearbeitungen betroffenen Personen liegen können, werden für diese indes aus einer datenschutzrechtlichen Betrachtung heraus auch Risiken verortet. Namentlich Unternehmen mit Auskunftsservices zur *Bonität* werden datenschutzrechtlich kritisiert.[1684] Problematisiert werden intransparente Prozesse und nicht nachvollziehbare Ergebnisse, aber auch falsche Schlussfolgerungen, beispielsweise aufgrund fehlerhafter «Rohdaten», des Weiterverkaufs an Kriminelle u. a. m. Anlass zu Diskussionen geben anknüpfend an die Nutzung von Aggregierungs- und

1681 Zu den Kundenbindungssystemen vgl. z. B. Eckhardt/Fattebert/Keel/Meyer, 1 ff.; zu den Gesundheitsdaten do Canto, sic! 2020, 177 ff.

1682 Nissenbaum, 49.

1683 Vgl. hierzu auch Rosa, 31; kritisch zur Bedeutung, die quantifizierenden Methoden zugemessen wird, Porter, 11 ff.

1684 Vgl. Buchner, 119 ff. auch zu falschen Kreditauskünften; Strasser, SJZ 1997, 449 ff.; Weichert, DuD 2005, 582 ff.; Wuermeling, NJW 2002, 3508; Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16; Rudin, digma 2007, 50 ff.; vgl. Koprio, Ktipp vom 12. November 2013, Von der Vergangenheit wieder eingeholt, <https://www.ktipp.ch/artikel/d/von-der-vergangenheit-wieder-eingeholt/> (zuletzt besucht am 30. April 2021); Frühauf, Neue Westfälische vom 23. März 2013, Bertelsmann-Tochter Infoscore nimmt Auskunftei vom Netz, <http://www.nw.de/nachrichten/wirtschaft/20412987_Bertelsmann-Tochter-Infoscore-nimmt-Auskunftei-vom-Netz.html> (zuletzt besucht am 30. März 2021); allem voran aber auf die wirtschaftlichen Vorteile verweisend Leisinger, NZZ vom 10. Februar 2014, Hier wohnt der Pleitegeier, <https://www.nzz.ch/finanzen/auskunfteien-bieten-informationen-ueber-kreditwuerdigkeit-und-zahlungsverhalten-1.18239649> (zuletzt besucht am 30. April 2021); beachte auch BGer A-4232/2015 vom 18. April 2017 und den Artikel hierzu in der NZZ <https://www.nzz.ch/schweiz/bundesverwaltungsgericht-engere-grenzen-fuer-moneyhouse-ld.1292276> (zuletzt besucht am 30. April 2021); «Saubanden sind das», vgl. <http://inkasso-abzocke.ch/schwarze-liste/> (zuletzt besucht am 30. April 2021); vgl. zur Furcht vor Registrierungen und den Druck zur Anpassung Forstmoser, SJZ 1974, 217 ff., 220.

Analysetechnologien und darauf basierenden Geschäftsmodellen Effekte (potentieller) Verführungs- und Beeinflussungsmacht, der Manipulation sowie der Ungleichbehandlung bis hin zur Diskriminierung.[1685]

Insofern ist erneut exemplarisch der jüngste Facebook-Skandal zu erwähnen, in welchem (Personen-)Daten von über 85 Millionen Nutzerinnen und Nutzern an Cambridge Analytica «gelangten», woraufhin, wohl basierend auf entsprechenden Auswertungen, der US-amerikanische Wahlkampf gezielt beeinflusst wurde. Mit einem solchen Vorgehen sind es keineswegs nur isoliert die Individuen, die manipuliert und korrumpiert werden, was der Sichtweise eines Rechts entspricht, das im Individualgüterrechtsschutz verankert ist. Vielmehr zeitigt das Vorgehen disruptive Wirkung auf die Integrität des politischen Systems und die Demokratie an sich. Offensichtlich hat sich mit der Entwicklung solcher technischer Kapazitäten zugleich die Landkarte der Bedrohungen verändert.[1686] 1235

1.1.3. Zugriff und Verteilung

Bei der *dritten Kernkapazität* moderner Daten- und Informationsverarbeitungstechnologien, die mit den beiden vorangehenden verknüpft ist, geht es darum, dass (Personen-)Daten und Informationen weitläufig und umfassend zugänglich gemacht, verteilt und umgekehrt wieder aufgefunden sowie abgerufen werden können.[1687] 1236

Erneut sei ein im historischen Teil beschriebener Vorläufer in Erinnerung gerufen: das erste Comptoir im Paris des 14. Jahrhunderts, bei dem Informationen aggregiert wurden und Menschen auf sie quasi vor Ort zugriffen, woraufhin die entsprechenden Informationen unter Umständen weiter verteilt wurden.[1688] 1237

Heute bietet das World Wide Web mit seiner netzwerkartigen Struktur sowie etablierten Suchmaschinen nie zuvor gekannte Möglichkeiten der Informationsverteilung sowie Auffindbarkeit von Informationen, mithin des Informationsaustausches sowie der Kommunikation, von Suchen und Finden auch von Personenangaben.[1689] 1238

1685 Vgl. Buchner, 195 f.; Heuberger, N 28 und N 222; Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff.; zum Risiko von Big Data, diskriminierende und segregierende Effekte zu bringen, Allen, Harv. L. Rev. Forum 2013, 241 ff., 246 f.

1686 Zum Ganzen Nissenbaum, 36 ff.

1687 Zum Suchen und Finden von Informationen sowie Suchmaschinen aus einer geschichtswissenschaftlichen Perspektive Gugerli, 9 ff.; zur Registrierungsfähigkeit von Suchmaschinen wie Google Mayer-Schönberger, Delete, 16 ff., sowie zum leichten Informationszugriff, 89 ff.

1688 Hierzu erster Teil, II. Kapitel.

1689 Nissenbaum, 52; Bergelson, UC Davis L. Rev. 2003, 379 ff., 381; vgl. zu den technischen Grundlagen resp. der Netztechnik in Bezug auf Internetdienste und im Zusammenhang mit haftungsrechtlichen Fragen Rohn, 6 ff.

1239 An dieser Stelle ist das Thema der «Öffentlichkeit» staatlicher Register und Dokumente, insb. auch von Gerichtsurteilen, zu thematisieren. Jüngst zeichnet sich ein Entwicklungstrend ab, Online-Zugriffe auf Register, Dokumente und darin niedergelegte Personenangaben zu implementieren.[1690]

1240 Der Kanton Genf testete 2017 in einem halbjährigen Pilotprojekt ein digitales Handelsregister, das mittels Blockchain-Technologie funktionierte.[1691] Eine längere Tradition hat der sog. Halter-Index, mit dem sich in der Schweiz online Name und Adresse des Fahrzeughalters, dessen Kontrollschild man anvisiert, ausfindig machen lässt.[1692] Die rechtlichen Grundlagen hierfür fanden sich im Strassenverkehrsgesetz und konkretisierend in Art. 126 Abs. 1 der Verkehrszulassungsverordnung. Eine Auskunft erfolgte in der Regel gegen ein Entgelt von CHF 1.00, aus Sicherheitsgründen wurden innert 24 Stunden nur fünf Auskünfte erteilt. Auf Widerspruch des Halters und Datensubjektes hin konnte der Zugriff durch Private auf die entsprechenden Personenangaben blockiert werden. Art. 126 Abs. 1 der Verkehrszulassungsordnung wurde allerdings aufgehoben durch Anhang 4 Ziff. II der Verordnung vom 30. November 2018 über das Informationssystem Verkehrszulassung – mit Wirkung seit dem 1. Januar 2019.[1693] Die Auskünfte aus dem Fahrzeugregister werden nunmehr im Kanton Zürich gratis (E-Autoindex), allerdings nur noch via Online-Formular erteilt. Die Auskunft wird ungeachtet eines Interessennachweises und entsprechend voraussetzungslos erteilt. Das einzige Hindernis resultiert aus einer Sperrung vonseiten des Halters, was einem Widerspruch entspricht.

1241 Im Kern zielen das Fahrzeugkontrollschild und die informationelle Korrelierung des Fahrzeuges mit der Halterin darauf ab, den Regeln des Strassenverkehrs Nachachtung zu verschaffen. Allerdings drängt sich die Frage auf, ob der Zugriff auf Halterinformationen durch Privatpersonen angemessen ist, zumal die Durchsetzung der Strassenverkehrsregulierung eine staatliche, keine private Aufgabe ist. Zudem sind weitere «Zweckentfremdungen» der Angaben denkbar, die

1690 Betr. Gerichtsurteile in der Schweiz vgl. Hürlimann, sui-generis 2016, 83 ff.; Hürlimann/Kettiger, Justice – Justiz – Giustizia 2018, N 20; vertiefend Nissenbaum, 53 ff.; Conley/Datta/Nissenbaum/Sharm, Md. L. Rev. 2012, 772 ff.; zum Zugriff auf Grundbucheinträge und die eingesetzte Plattform Terravis Widmer, AJP 2020, 30 ff.; zur Justizöffentlichkeit im digitalen Zeitalter auch Schindler in: Gschwend/Hettich/Müller-Chen u. a. (Hrsg.), 741 ff., insb. 749 ff. und 752 ff. zur digitalen Publikation von Urteilen.

1691 Bolzli, Blick vom 12. September 2018, Erstes Blockchain-Handelsregister der Schweiz, Maudet modernisiert Genf, <https://www.blick.ch/news/politik/erstes-blockchain-handelsregister-der-schweiz-maudet-modernisiert-genf-id7194124.html> (zuletzt besucht am 30. April 2021); vgl. hierzu auch Sattler, SJZ 2017, 1036 ff. und Ders., BB 2018, 2243 ff.; zum Datenschutz mit Blick auf die Blockchain vgl. z. B. Isler, Jusletter vom 4. Dezember 2017, wobei er unter N 3 auf den Einwand hinweist, dass es um anonymisierte Transaktionen geht, womit der Anwendungsbereich des Datenschutzrechts gerade aufgehoben wird.

1692 Vgl. hierzu auch Rudin, digma 2004, 32 ff.

1693 Vgl. die Verordnung über das Informationssystem Verkehrszulassung (IVZV) vom 30. November 2018.

genuin einer öffentlichen Aufgabe dienen (Gewährleistung der Strassenverkehrsordnung als Element der Strukturierung des Mobilitäts- und Transportsektors mit entsprechenden Infrastrukturen). Besagte Personendaten verlassen ihren ursprünglichen Kontext dann, wenn Private diese ermitteln können. Ebendies kommt bekanntermassen auch zur Anbahnung persönlicher Beziehungen vor. Handelte es sich um einen einvernehmlichen Flirt am Rotlicht, mag die spätere Kontaktaufnahme, die über den Datenzugriff auf den Halter-Index möglich wird, faktisch positiv erscheinen. Wenn allerdings jemand zu später Stunde einen Club verlässt, um sich von einer aufdringlichen Person zu entfernen, in sein Auto steigt und die zurückbleibende Person nun anhand des Autokennzeichens den Halter identifizieren kann, ist die Problematik des voraussetzungslosen (Online-)Zugriffes auf die Angaben offensichtlich.

Das Beispiel und das Konzept löst folglich – trotz in der Schweiz vorhandener gesetzlicher Grundlage für einen weitgehend unbeschränkten Zugang zu Fahrzeughalterangaben – Irritation aus. Es fragt sich, ob der Zugriff auf Halterangaben durch Private materiell zu überzeugen vermag. 1242

Die USA – in Europa gemeinhin dafür kritisiert, den Datenschutz wenig ernst zu nehmen – haben einen vormals nahezu unlimitierten Zugriff auf entsprechende Angaben 1994 mit dem *Drivers Privacy Protection Act* Restriktionen unterworfen. Der Akt limitiert den Zugriff auf diese Angaben und lässt die Eröffnung entsprechender Daten nur zu, wenn ein *enger Konnex zum Kontext des Strassenverkehrs mit den hieran geknüpften Vorgaben, Zielen, Erwartungen usf. besteht*. Die datenschutzrechtliche Gestaltung ist folglich eng an bereichsspezifische Erwägungen und besagte Schutzgedanken gekoppelt. 1243

Ganz anders das Schweizer Regime, in welchem kontextuelle Erwägungen und Erwartungen in diesem Bereich weitgehend ausser Acht bleiben. Das Beispiel des (Online-)Zugangs zu Fahrzeughalterangaben und die unterschiedlichen gesetzlichen Antworten hierauf führen erneut vor Augen, dass es die Anerkennung resp. die Nichtanerkennung der Relevanz des Verarbeitungszusammenhanges und des sozialen Kontextes ist, welche das Gesetzgebungskonzept massgeblich prägt. Gezeigt wurde sodann, dass nicht nur der Transfer von Personenangaben von einem Kontext in einen anderen problematisch sein kann, sondern auch, dass sich mit dem Transfer von bestimmten (Personen-)Angaben ins Internet die Topografie der Personendatenverarbeitung verändert. 1244

Ob Akteneinsichtsrechte und Öffentlichkeitsgebote aus der *analogen Welt* gleichermassen ein Recht auf *Online-Zugang* indizieren, wird kontrovers diskutiert.[1694] Die Verlagerung des Zugangs zu «öffentlichen Akten» ins Netz scheint das Terrain grundlegend zu verändern. Gewisse Autoren beurteilen (Perso- 1245

1694 Nissenbaum, 58.

nen-)Daten durch deren Transfer in das Netz als «öffentlich».[1695] Ebendies, weil mit der Möglichkeit des Online-Zugriffes auf Informationen in staatlichen Dokumenten namentlich auch faktische Beschränkungen, die in der analogen Welt greifen, nicht vorhanden sind. Einsichtsrechte, die offline ausgeübt werden, werden quasi durch die Öffnungszeiten von Ämtern, die Notwendigkeit, diese real aufzusuchen, sowie die analog erfolgenden Informationszugriffe (Einblick in die Dokumente, Auszüge aus Registern in Papierform) beschränkt, was bei Online-Zugriffen entfällt.[1696]

1246 Im Hinblick auf Gerichtsentscheide drängt sich eine differenzierte Beurteilung auf, je nachdem, ob diese in einer Bibliothek real aufgesucht werden müssen, kopiert und in der Folge einzig und allein durch die «menschlichen Informationsverarbeitungskapazitäten» gelesen und studiert werden können, oder ob Urteile online abrufbar sind.[1697] Seit Längerem sind die Entscheide des eidgenössischen Bundesgerichts online abrufbar, wobei sich trotz regelmässiger Anonymisierung der Parteien zahlreiche personenbezogene Angaben, beispielsweise über Berufe, Einkommensverhältnisse, Kinderbetreuungsarrangements usf., finden lassen. Besagte Angaben können heute über das Internet ungefiltert und ohne Kosten sowie Aufwand durch jedwede Person, zu jedwedem Zweck, zu jedweder Stunde, von jedwedem Ort aus abgerufen werden und – ohne weitere Schranken – elektronisch weiterverarbeitet und namentlich mit Angaben aus anderen Quellen und Plattformen des Internets kombiniert werden. Suchmaschinen optimieren die Stichwortsuche. Unbestritten eine Errungenschaft für Anwältinnen, Studierende der Rechtswissenschaft, für Gerichte und Forschende. Dennoch sollten Einsichts- und Zugangsrechte aus der analogen Welt nicht unreflektiert *telle-quelle* für die Online-Welt anerkannt werden, ohne die sich mit dem Transfer ins Netz verändernde informationelle Topografie zu reflektieren.

1247 Für das Internet stösst somit – wie die bisherigen Ausführungen bereits gezeigt haben – namentlich der Befund auf Widerstand, dass in dieser netzwerkartigen Struktur Flüsse von Personendaten nicht nur in zeitlicher, persönlicher und quantitativer Hinsicht nahezu unbeschränkt sind. Zudem wird der Zugriff weitestgehend ohne Restriktion in Bezug auf einen ursprünglichen gesellschaftlichen Kontext möglich – beispielsweise der Bereich der persönlichen und individuellen Beziehungspflege auf sozialen Plattformen. Informationen werden diversen anderen etablierten gesellschaftlichen Kontexten zugeführt und nutzbar gemacht, namentlich auch dem ökonomischen Kontext.

1695 Nissenbaum, 58.
1696 Vgl. Ders., 56.
1697 Zur Publikationspraxis von Gerichtsurteilen Hürlimann, sui-generis 2016, 83 ff.; Hürlimann/Kettiger, Justice – Justiz – Giustizia 2018, N 20.

Vor diesem Hintergrund ist es angezeigt, das *Internet nicht isoliert als Technologie* zu taxieren, stattdessen als eigenständigen Bereich. Gleichwohl bleibt dieser Bereich in eine *Gesellschaft* eingebettet. Eine *Gesellschaft, die in pluralen sozialen Kontexten* strukturiert ist. Von diesem Leitgedanken sollte auch ein Datenschutzrecht der Zukunft durchdrungen sein. 1248

Wie sehr die Möglichkeiten, Informationen und Personenangaben online zu veröffentlichen und ebenda aufzusuchen, die zur Beurteilung stehende informationelle Situation verändern, ersieht sich anhand weiterer Praktiken resp. Dienste: Eine Herausforderung aus datenschutzrechtlicher Perspektive sind private Datenbanken der Ahnenforschung wie Ancestry oder My Heritage.[1698] 1249

Die veränderte Topografie wurde sodann anhand des Dienstes von Google Street View beschrieben. Nehmen sich Menschen auf Strassen, vor Häusern usf. von blossem Auge und gewissermassen *en passant* wahr, unterscheidet sich dies grundlegend von der Situation, in welcher der Dienst Google Street View 360-Grad-Fotografien von Strassen, Häusern, Höfen und unter Umständen ebenda befindlicher Personen usf. ins World Wide Web stellt.[1699] Ebenda sind die Angaben weitestgehend unbeschränkt weiterverarbeitbar, auffindbar, kombinierbar, auswertbar, wobei diese technisch ausgebauten Kapazitäten, Daten und Informationen zu verteilen und zu finden, an etablierte soziale Praktiken rühren, die unter dem Dachbegriff des Privaten eingefangen werden.[1700] 1250

Sodann lösen gerade auch die sozialen Netzwerke wie Facebook kontroverse Debatten unter dem Begriff der Privatheit aus. Solche Internetseiten und -plattformen dienen der Pflege sozialer Beziehungen und des Selbstimages. Obschon heute unzählige Menschen persönliche oder berufliche Beziehungen mittels Online-Netzwerken pflegen (MySpace, Facebook, LinkedIn, Xing usf.; Social Media), verstummen die kritischen Stimmen gegenüber sozialen Netzwerken, abermals unter dem Titel des Privat- und Datenschutzes, nicht.[1701] 1251

Insofern werden *drei Problemfelder* umschrieben. Das erste Cluster bilden Situationen, in welchen eine Person personenbezogene Angaben in Wort, Bild oder anderer Form über sich selbst veröffentlicht, woraus Konsequenzen für die Person resultieren können, wie etwa die Kündigung der Arbeitsstelle oder die Nicht-Ein- 1252

1698 Vgl. hierzu auch Karavas/Burri/Gruber, TA-SWISS 2020, 251 ff.; vgl. zur Änderung des DNA-Profilgesetzes den erläuternden Bericht des Bundesrates, abrufbar unter: <https://www.ejpd.admin.ch/dam/data/fedpol/sicherheit/personenidentifikation/dna/ber-d.pdf> (zuletzt besucht am 30. April 2021).

1699 Die Praxis führte in der Schweiz zu einer Intervention des EDÖB, wobei in letzter Instanz das Bundesgericht mit BGE 138 II 364 entschied; Nissenbaum, 10, 51 f., 192 f., 219 ff.

1700 Nissenbaum, 52.

1701 Zum Ganzen Dies., 58 ff.; zu den Möglichkeiten von Privatpersonen, sich gegen Persönlichkeitsverletzungen auf sozialen Plattformen zur Wehr zu setzen, Rosenthal, Anwaltsrevue 2014, 415 ff.; zu den Risiken von Social Media Coen, *passim*.

stellung wegen nicht opportuner Aussagen oder Darstellungen. Das zweite Cluster bilden Aktivitäten in sozialen Netzwerken, die (auch) andere Personen betreffen, beispielsweise die Publikation von «fremden» Fotos oder von gemeinsamen Fotos, was wiederum Konsequenzen für diese Drittperson zeitigen kann.[1702] Das dritte Cluster resultiert aus der Kombination der beiden Kernkapazitäten neuer Technologien, der nahezu unbeschränkten Verteilungs- und Auffindungsmöglichkeit auf der einen und des Trackings und Monitorings auf der anderen Seite.[1703]

1.2. Synthese und Resümee

1253 Die vorangehende Darstellung hat mit dem «rasanten technischen Fortschritt mit seinen grenzenlosen Verarbeitungskapazitäten» eine die Datenschutzdebatte prägende Chiffrierung aufgeschlüsselt. Die aktuellen Informationsverarbeitungstechnologien wurden anhand *dreier Kernkapazitäten* beschrieben: dem Tracking und Monitoring, der Aggregierung und Analyse sowie der Verteilung und Veröffentlichung resp. umgekehrt dem Auffinden von und Zugreifen auf Personendaten resp. Informationen, was namentlich über das World Wide Web in nahezu unbeschränktem Umfang ermöglicht wird. Die Digitalisierung hat dazu geführt, dass bisherige Limiten, denen die drei Potenzen begegneten, entfallen sind.[1704] Die präzisere Umschreibung der technischen Möglichkeiten anhand dreier Kernkompetenzen erfolgte mit dem Ziel, ein besseres Verständnis für die Ausgangslage, Realitäten und Herausforderungen des aktuellen und künftigen Datenschutzrechts zu gewinnen.

1254 Die technischen Kapazitäten mit ihren drei Kernkompetenzen stellen *kein System gegenseitiger Exklusion dar*. Vielmehr werden diese Funktionen und Möglichkeiten regelmässig miteinander *kombiniert*.[1705] Insofern ist zu attestieren, dass sich durch den vernetzenden Einsatz der drei Kernkapazitäten neuer Informationsverarbeitungstechnologien nicht nur die Verarbeitungslandschaft, sondern auch die Risiko- resp. Bedrohungslandschaft verändert. Dies ist wiederum für den Datenschutz relevant. Isoliert eingesetzt mag z. B. eine transparent durchgeführte Monitoring-Funktion aus einer Datenschutzperspektive wenig Anlass zu Bedenken und Misstrauen geben. Ähnlich kann der Austausch von Informationen auf einer Social-Media-Plattform in einem Design, in welchem die Nutzerinnen und Nutzer selbst kontrollieren, wer zu welchen Angaben Zugang hat, datenschutzrechtlich wenig bedenklich sein (sofern hinreichende Sicherheitsmassnahmen gegen Hacking usf. getroffen wurden). Anders allerdings stellt sich das Bild bei

1702 Problematisiert ebenso bei Loch/Conger/Oz, J. Bus. Ethics 1998, 653 ff., 653.
1703 Nissenbaum, 62 f.
1704 Aufschlussreich insofern auch Mayer-Schönberger, Delete, 64 ff.
1705 Illustrativ hierzu m. w. H. Litman, Stan. L. Rev. 2000, 1283 ff., 1283 f.

einem System dar, in welchem Dritte, beispielsweise Agenten der Informationsindustrie, Zugang zu personenbezogenen Angaben haben. Wenn eine potentielle Arbeitgeberin über Bewerberinnen einen «Anstellungscheck» durchführen lässt, indem sie eine Auskunftei dazwischenschaltet, die personenbezogene Daten auch über die sozialen Plattformen im Internet erhebt, speichert, auswertet und dann in der Folge weiterverkauft, kann das unter Umständen – wurde ein negatives Scoring-Resultat übermittelt – zur Verweigerung einer Anstellung führen.[1706] Die Bedrohungstopografie verändert sich, wenn die drei Kapazitäten miteinander verknüpft werden.

Das bessere Verständnis von Funktionsweisen und Kernkapazitäten neuer Informationsverarbeitungstechnologien drängt zu einem Perspektivenwechsel in der datenschutzrechtlichen Auseinandersetzung. Das tradierte und fragmentierende datenschutzrechtliche Konzept, welches die Person als Datensubjekt und Personendaten als Quasi-Objekte zum Regelungsgegenstand und Basisbezugspunkt macht, bildet die beschriebenen technischen Realitäten und Prozesse nicht ab. Vielmehr macht der Blick auf die Kernkapazitäten der Informationstechnologien sichtbar, dass es um *Personendatenflüsse in Netzwerkstrukturen* geht. Mit dem angeregten Sichtwechsel ist eine an früherer Stelle umschriebene Verantwortungszuweisung, wonach die datenschutzrechtlichen Wirkungsschwächen primär mit der fehlenden Vernunft oder ungenügenden Achtsamkeit und Sensibilität von Nutzerinnen und Nutzern begründet werden, zu relativieren. 1255

Gleichzeitig wurde die Relevanz von *Kontexterwägungen* sichtbar. Hierbei zeigte sich, dass Übertritte von Datenflüssen zwischen verschiedenen gesellschaftlichen Kontexten sowie zwischen der Offline- und der Online-Welt den Datenschutz vor spezifische Herausforderungen stellt. Namentlich für das Internet wurde festgestellt, dass Datenflüsse kaum Restriktionen unterliegen, auch nicht aus kontextuellen Erwägungen. 1256

Im Ergebnis ermöglichen die neuen Technologien und entsprechend fortentwickelte Geschäfts- und Verwaltungspraktiken, dass tiefe, breite und hoch mobile, massive Datenbestände generiert werden, die Personenangaben aus verschiedensten Quellen und Kontexten «poolen», woran verschiedene Analysen anschliessen und wobei die damit generierten Informationen wiederum divers verteilt werden. Es ist diese Zusammenführung, Auswertung und Verteilung von Personendaten zwischen pluralen Quellen und Kontexten – vom Facebook-Profil bis zum LinkedIn-Profil, von öffentlichen Registern bis zu Telefonbüchern – vom Bereich der persönlichen Beziehungspflege in den wirtschaftlichen Kontext und alsdann in den politischen Bereich, die datenschutzrechtlich kritisch ist. Dass das «Zu- 1257

1706 Zum Robot Recruitment vertiefend Glatthaar, SZW 2020, 43 ff., 46 ff.; vgl. bereits Bull, Computer, 57 f.; vertiefend zum Datenschutz im Arbeitskontext vgl. Kasper, *passim*.

sammenziehen» von Personendaten aus verschiedensten Systemen in netzwerkartigen Strukturen, deren Auswertungen und später wiederum diversifizierte Verteilung aus der Perspektive des Datenschutzes auf Widerstand stossen, illustrierte der jüngste Facebook-Skandal, infolge dessen im Mai 2018 der involvierte Informationsbroker Cambridge Analytica Insolvenz anmeldete. Das Beispiel, das die *technischen Möglichkeiten als erste faktische Hauptherausforderung des Datenschutzes* illustriert, leitet zur *zweiten Realität resp. faktischen Entwicklung* über, die das *Datenschutzrecht auf den Prüfstand stellt:* Die neuen Möglichkeiten der (Personen-)Datenaggregation und -analyse haben zugleich eine eigenständige *Industrie*, die Daten- und Informationsindustrie, ein verselbstständigtes Geschäftsfeld und einen eigenen Marktplatz hervorgebracht.

1258 Mit dem Trend zur sog. *Kommerzialisierung von Personendaten* und den damit verbundenen Geschäftspraktiken sowie mit deren Bedeutung für den Datenschutz befasst sich die nachfolgende Analyse.

2. Ökonomische Transformation und Expansion

2.1. Vorbemerkungen

1259 Vergleichbar zum «rasanten technischen Fortschritt mit seinen grenzenlosen Datenverarbeitungen» avancierten Wendungen wie «Personendaten sind das Öl des 21. Jahrhunderts» oder «data is the new currency[1707]» zum Topos dieser Tage.[1708] Apple, Google, Facebook, Amazon und Co. bilanzieren je mehrere Milliarden US-Dollar.[1709] Bemerkenswerterweise machen indes weder Google noch Facebook oder YouTube die Nutzung ihrer Dienstleistungen von einer Bargeldzahlung abhängig. Es handelt sich mit anderen Worten um Dienste und Unternehmen, die kein Geld kosten und gleichwohl nicht unentgeltlich resp. gratis sind.[1710] Erneut sollen zwecks sinnhafter Re-Formulierung des Datenschutzes und seiner Vorgaben mit dem Ziel, diese in Zukunft wirksamer zu gestalten, die hinter diesem Topos stehenden Entwicklungen präziser eingefangen werden.

1707 Bolliger/Féraud/Epiney/Hänni, 34, wohl anlehnend an EU-Kommissarin Reding: «Personal data is in today's world the currency of the digital market», abrufbar unter: <http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm> (zuletzt besucht am 30. April 2021).

1708 Die FAZ vom 18. April 2017, 33, titelt: «Wie wir mit Daten bezahlen»; der Autor, Spehr, geht der Frage nach, was ein Gigabyte wert sei; in der NZZ vom 1. Februar 2016 findet sich ein Beitrag von Flückiger mit dem Titel «Digitale Selbstbestimmung. Daten sind Gold wert – doch für wen?»; vgl. auch Grassegger, 37; zu Recht kritisch zur Analogie zwischen Daten und dem Rohstoff Öl: Hürlimann/Zech, sui-generis 2016, 98 ff., 98; Angwin, The web's new gold mine: Your secrets, WSJ vom 30. Juli 2010; Weichert, in: Bäumler (Hrsg.), 158 ff., 158.

1709 Grassegger, 33 f.; dazu, dass es um Milliardenbeträge geht qua Auswertung von Personendaten im Internet Weichert, in: Bäumler (Hrsg.), 158 ff., 169; Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 198.

1710 Vgl. zur Bezahlung mittels Aufmerksamkeit und Personendaten Kurz/Rieger, 12 ff.

Ein Ausgangspunkt ist, wonach Personendaten resp. die Einräumung von Nutzungsrechten an den Personendaten durch die Betroffenen gegenüber den Dienstanbietern als Gegenleistung für besagte Dienstleistungen figurieren. In der Folge ist deren Verwertung resp. Auswertung das entscheidende Übersetzungs- und Umsetzungskriterium, damit Personendaten einen ökonomischen Wert entfalten. Personendaten sind isoliert betrachtet lediglich eine Art Rohstoff. Gerade im Internet veröffentlichte Personendaten können nahezu beliebig abgerufen und verwertet werden. 1260

Im Prozess der Ökonomisierung von Personendaten spielt ein Phänomen eine wichtige Rolle, das unter dem *Titel der sog. Ökonomie der Aufmerksamkeit* abgehandelt wird: Gemeint ist an dieser Stelle indes nicht die für Juristinnen und Juristen naheliegende Assoziation mit der Thematik der Kommerzialisierung der Persönlichkeit von und durch Prominente und jünger von weniger Prominenten in Formaten wie Reality Shows.[1711] Vielmehr ist die Beschreibung der Aufmerksamkeit als knappes und rares Gut, welches durch gezielte Werbeaktivitäten intensiv ausgebeutet und genutzt wird, für die nachfolgenden Ausführungen von besonderem Interesse.[1712] Für die meisten der Online-Giganten und Internet-Dienstleister bildet die *Werbeindustrie*, die auf der Verarbeitung von Personendaten basiert, eine tragende Säule ihres Geschäftsmodells: 1261

> «Vor genau 20 Jahren haben Larry Page und Sergey Brin Google aus der Taufe gehoben. Inzwischen ist ihr Konzert das zweitwertvollste Unternehmen der Welt. Es erzielt mit der Online-Werbung jedes Jahr Milliardengewinne.»[1713]

Den ökonomischen Wert von Personendaten realisieren heute keineswegs bloss die Internetgiganten für sich. Vielmehr machen sich nahezu sämtliche Unternehmen, Organisationen und Institute den wirtschaftlichen Wert von Personendaten zwecks Effizienzsteigerung, zur Kostensenkung sowie Gewinnsteigerung zunutze. Gekoppelt an einen Trend, wonach neue Daten- und Informationsverarbeitungstechnologien bis in die feinsten Kapillaren der Gesellschaft diffundiert sind, ist die Effektuierung von Geschäfts- sowie Verwaltungsprozessen und damit zugleich deren Optimierung aus wirtschaftlichen Erwägungen unter Nutzung von 1262

1711 Für die Schweiz und rechtsvergleichend zur faktischen wie rechtlichen Kommerzialisierung von Persönlichkeitsrechten Meyer Caroline B., 1 ff.; zur medialen Unterhaltung, zur Erzeugung von Prominenz durch die Medien, zu der in diesem Zusammenhang zu verzeichnenden Ökonomie der Aufmerksamkeit sowie zur Forderung auch nach Anerkennung eines Rechts auf Prominenz mit vermögensrechtlichem Gehalt Ladeur, ZUM 2000, 879 ff.; rechtsvergleichend auch Moskalenko, IJC 2015, 113 ff.

1712 Zur Aufmerksamkeit als ausgebeutetes Gut Wu, Antitrust L.J. 2017, 34 ff.

1713 So steht es auf der Frontseite der NZZ vom Sonntag, 10. September 2017 unter dem Titel «Wie Google den Tod besiegen will»; dazu, dass zahlreiche Dienste im Internet kostenlos, mithin über Werbung finanziert würden, Langheinrich/Karjoth, digma 2012, 116 ff., 116; Meyer, Jusletter IT vom 25. Februar 2016, N 1.

(Personen-)Datenverarbeitungsprozessen längst nicht mehr den grossen Akteuren wie den Internetgiganten oder den Staaten vorbehalten.[1714]

1263 Der Wert personenbezogener Angaben aller Europäer wird für das Jahr 2020 mit einer Billion Euro veranschlagt.[1715] Doch das Datensubjekt, so ein Kritikpunkt, wird monetär exkludiert:

> «250 harte Dollar pro Monat, das ist der Wert Ihrer digitalisierten Persönlichkeit. Wenn sich nichts ändert, werden Sie nie etwas davon sehen. Denn Sie bekommen im Gegenzug für Ihre Daten: einen Facebook-Account.»[1716]

1264 Gezeichnet wird ein *Bild der informationellen Leibeigenschaft des Menschen*.[1717] Die Datensubjekte würden in zweierlei Hinsicht zu Objekten degradiert: erstens, indem sie im Hinblick auf Entscheidungsprozesse nur ungenügend in die Personendatenverarbeitungsprozesse inkludiert würden, und zweitens, weil sie keine wirtschaftlich angemessene Teilhabe erhalten würden.

1265 Die Kognition eines ausschlachtbaren, zum Informationsobjekt herabgewürdigten Subjektes liefert indes keine hinreichend präzise Darstellung des komplexen *Ökonomisierungsphänomens als zweiter faktischen Hauptherausforderung des Datenschutzes*. Mit anderen Worten ist das aktuelle (Privat-)Recht mit seinen etablierten dogmatischen Kategorien des Rechtssubjektes, der subjektiven Rechte, einer ideellen Natur des Persönlichkeitsrechts und der Rechtsobjekte, welche die Hintergrundfolie für das Datenschutzrecht des privaten Sektors bilden, nicht in der Lage, die Herausforderungen, die unter dem Titel der Ökonomisierung von Personendaten beschrieben werden, in sämtlichen Dimensionen zu erfassen.[1718]

1266 Vorauszuschicken ist, dass sich faktisch für wohl sämtliche Kontexte Optimierungsprozesse basierend auf Personendatenverarbeitungsprozessen beschreiben lassen, die auch, aber nicht nur ökonomische Folgen und Vorteile nach sich ziehen: In dem bereits erwähnten Versicherungsbereich, der fortwährend neue Applikationen wie z. B. die beschriebene App testet, finden sich weitere Praktiken, mit denen sich Kosten senken resp. Gewinne steigern lassen: Dazu gehört ebenso das Aufdecken von potentiellen Betrugsfällen durch Observationsmassnahmen, eine Konstellation, die im IX. Kapitel zur Erhärtung der in dieser Arbeit aufgestellten These analysiert wird. Zudem wird der Geschäftsgang optimiert, indem Vertragskonditionen basierend auf Profiling-Analysen und individualisier-

1714 Hierzu z. B. Vesting, in: Ladeur (Hrsg.), 155 ff., 169 ff.
1715 Boston Consulting Group, The Value of Identity 2014, 9 ff.
1716 Grassegger, 39.
1717 Illustrativ hierfür Grassegger: «Das Kapital bin ich. Schluss mit der digitalen Leibeigenschaft».
1718 Eine logische Folge des subjektivrechtlichen Ansatzes ist die Frage nach einem Recht an eigenen Personendaten, vgl. zu dieser Frage z. B. Thouvenin, SJZ 2017, 21 ff.; vgl. zur digitalen Ökonomie, der Bewerbung im Internet basierend auf Webtracking Wenhold, 75 ff.

ten Risikoprofilen gestaltet werden.[1719] Für den Gesundheitssektor ist auf die personalisierte Medizin hinzuweisen, die auf der Auswertung umfassender (auch personenbezogener) Datenbestände beruht.[1720] Sie ermöglicht die verbesserte (weil präzisere und individualisierte) Gesundheitsversorgung des Menschen. Personendatenverarbeitungen leisten ihrerseits einen Beitrag, Ziele und Zwecke des Gesundheitssektors zu erfüllen, indem sie Heilungschancen oder die Linderung von Leiden resp. die Wahl von effektiveren Präventivmassnahmen eröffnen.[1721] Gleichzeitig ziehen solche Prozesse und Praktiken ökonomische Konsequenzen nach sich, die indes auch negativ bewertet werden (Schlagwort «explodierende Gesundheitskosten»).

1267 Optimierungen werden weiter im Verkehrs- resp. Transportkontext erreicht, indem mittels automatisierter Messungen von Strassenzuständen, Wetterverhältnissen oder Verkehrsaufkommen Staumeldungen via GPS abgesetzt werden oder Massnahmen wie die automatisierte Salz-Einstreuung greifen, was Kosten wegen Staus oder Verkehrsunfällen verringert. Finanzinstitute nutzen und werten Personenangaben, die aus dem Einsatz von Kreditkarten generiert werden, nicht nur für die Vertragsabwicklung aus; darüber hinaus lassen sich ungewöhnliche Karteneinsätze feststellen, die auf einen Kartendiebstahl schliessen lassen. Auch aufseiten des Staates effektuieren Personendatenverarbeitungen zunächst die diversen unmittelbar verfolgten Ziele und Zwecke resp. öffentlichen Interessen der jeweiligen Funktionseinheiten. Regelmässig lassen sich hieran anknüpfende Effekte ebenso pekuniär quantifizieren, so offensichtlich für die Bereiche des Steuerwesens oder des Sozialstaats; Straftäter können dank der Auswertung von Handydaten schneller gefasst werden, womit die Gesellschaft effizienter vor Kriminalität geschützt wird, was Kosten unter verschiedenen Titeln, auch dem monetären Titel, reduziert. In ähnlichem Zusammenhang von hoher Relevanz sind Datenerhebungen und -analysen sowie Informationsaustauschsysteme zwecks Bekämpfung des Terrorismus, der unermessliche emotionale, psychische und physische Schäden auf individueller, gesellschaftlicher wie auch wirtschaftlicher Ebene verursacht.

1268 Spätestens in dem Augenblick, in welchem personenbezogene Angaben, Analyseergebnisse und abgeleitete Hypothesen zum Handels- und Marktgut avanciert sind, verschärft sich das Risiko, dass Personendaten aus wirtschaftlichen Moti-

1719 Vgl. Zittel, in: Passadelis/Rosenthal/Thür (Hrsg.), § 12 N 12.1 ff.; allgemeiner zum Profiling, seiner Relevanz im Zusammenhang mit dem Vertragsschluss und dem Datenschutzrecht Heuberger, N 377 ff.

1720 Baeriswyl, digma 2014, 52 ff.; do Canto, sic! 2020, 177 ff.; grundlegend zu Chancen und Risiken der Informations- und Kommunikationstechnologien im Gesundheitsbereich resp. E-Health-Bereich Berger Kurzen, *passim*.

1721 Zum Datenschutz im Gesundheitswesen Uttinger, in: Passadelis/Rosenthal/Thür (Hrsg.), § 10 N 10.1 ff.; vertiefend zur Humanforschung auch mit Blick auf gesundheitsbezogene Personendaten Karavas, Körperverfassungsrecht, 199 ff.; zu einem Bioinformationsrecht Gruber, *passim*.

ven heraus weitgehend schrankenlos verarbeitet werden. Hinter solchen Expansions- und Transformationsprozessen stehen sophistizierte, durch die neuen Technologien erst möglich gewordene Geschäftsmodelle und Vertragsnetzwerke, mit denen Personendaten wirtschaftlich ausgenutzt werden. Anders gewendet gehen neue technologische Kapazitäten, die vorangehend als erste faktische Hauptherausforderung des Datenschutzrechts beschrieben wurden, Hand in Hand mit neuen Geschäftsmodellen.

1269 Eine spezifische Rolle spielt die sog. *Informationsindustrie*. Der Geschäftszweck der in diesem Bereich angesiedelten Unternehmen ist einzig und allein auf den Umgang mit Personendaten ausgerichtet.[1722] Weiter alimentieren diese Unternehmen andere Unternehmen, Organisationen und Institutionen, die zwar oft durchaus auch wirtschaftliche Ziele verfolgen, zugleich indes anderen Zwecken verpflichtet sind und somit in spezifischen Branchen resp. sozialen Kontexten agieren: Spitäler und Pharmaunternehmen sollen, selbst wenn sie gewinnstrebend sind, primär Ziele des Gesundheitsbereiches gewährleisten. Medienunternehmen nehmen Informations- und Unterhaltungsaufgaben wahr, womit sie eine wichtige Funktion sowohl für das demokratische Staatssystem als auch für das sog. Privatleben einnehmen; zugleich sind sie an Wirtschaftlichkeitserwägungen ausgerichtet. Fluggesellschaften agieren im Transportsektor, womit sie wiederum eine quasi doppelte Zielsetzung verfolgen. Privatwirtschaftliche Unternehmen handeln damit regelmässig im Bestreben diverser und facettenreicher Geschäftszwecke, verfolgen indes zugleich ökonomische Interessen – auf die Verwirklichung dieser doppelten Stossrichtungen zielen denn auch (mutmasslich) regelmässige Personendatenverarbeitungen ab. Anders ist für die Unternehmen der Informationsindustrie die (entgeltliche) Zurverfügungstellung von Informationen aus Gewinn- und Profitstreben heraus der Geschäftszweck selbst.

1270 Das Verhältnis von Wirtschaft und Datenschutz ist seit jeher ein ambivalentes und spannungsvolles. Gezeigt wurde dies anhand des Beispiels der Verabschiedung des ersten DSG in der Schweiz.[1723] Auch bezüglich der Totalrevision des DSG erwuchs vonseiten der Privatwirtschaft Widerstand; allerdings handelt es sich nicht zwingend um ein antithetisches Verhältnis.

1271 Dass Personendaten *und* ihrer (rechtskonformen) Verarbeitung auch wirtschaftliche Bedeutung zukommt, das Datenschutzrecht allerdings zugleich weitere Schutzziele und -zwecke zu erfüllen hat, wird eindrücklich von der DSGVO

1722 Vgl. Nissenbaum, 45 ff.

1723 Vgl. zweiter Teil, IV. Kapitel; auch der Totalrevision des DSG wurde von wirtschaftlicher Seite her Widerstand entgegengesetzt, vgl. EJPD, Zusammenfassung, 7; vgl. illustrativ insofern <https://www.mll-news.com/totalrevision-dsg-bundesrat-veroeffentlicht-gesetzesentwurf-und-botschaft/> (zuletzt besucht am 30. April 2021); dazu, dass auch die 2008 in Kraft gesetzte Teilrevision auf Widerstand vonseiten der wirtschaftsnahen Kreise stiess, m. w. H. Wermelinger/Schweri, Jusletter vom 3. März 2008, N 2; vgl. auch Baeriswyl/Rudin, Jusletter vom 28. Juni 2004.

in ihren Erwägungen artikuliert.[1724] Sie dient dem Schutz des Menschen bei der Verarbeitung persönlicher Daten, wobei sie gemäss Erwägungsgrund 2 zur Vollendung eines Raumes der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarktes sowie zum Wohlergehen natürlicher Personen beitragen soll. Gemäss Erwägungsgrund 7 soll die DSGVO eine Vertrauensbasis schaffen, welche die digitale Wirtschaft dringend benötige. Zugleich soll die Verarbeitung von Personendaten im Dienst der Menschheit stehen.

1272 Allem voran im Internet ist indes eine expansive Kraft ökonomischer Rationalitäten im Zuge von Personendatenverarbeitungen zu verzeichnen, welche andere, ebenso schutzwürdige Rationalitäten und Leitprinzipien durchkreuzen kann. Es würde zu kurz greifen, von der Kommerzialisierung oder Ökonomisierung von Personendaten zu sprechen; vielmehr geht es um die expansive Kraft ökonomischer Rationalitäten zulasten anderer gesellschaftlicher Ziele und Zwecke.[1725]

1273 Die anschliessende Analyse ist anhand eines *Stufensystems aufgebaut*. In einer ersten Stufe wird isoliert eine klassische Konstellation der Kommerzialisierung personenbezogener Angaben offline mit sog. CRM-Modellen dargestellt. Das Bild wird sogleich ergänzt und verdichtet, indem sich in einer zweiten Stufe der Fokus auf Kommerzialisierungspraktiken im Internet richtet. Hierbei wird gezeigt, inwiefern eine Praxis wie das CRM im Online-Bereich eine neue Dimension erlangt. Gleichzeitig wird sichtbar, wie die Verarbeitungspraktiken und -techniken ineinandergreifen. Ein Höhe- und Kulminationspunkt auf der dritten Stufe bildet die Etablierung einer Datenindustrie. Charakteristisch für diese ist, dass sie in dichten Vertragsnetzwerken operiert sowie vernetzend zwischen Online- und Offline-Bereichen agiert. Damit wird die dem aktuellen Datenschutzrecht zugrunde liegende Fokussierung auf das Datensubjekt sowie Personendaten als Quasi-Objekte herausgefordert. Gerade auch mit und über das Internet wird ein Bereich resp. eine Realität konstituiert, die weitestgehend von *ökonomischen Rationalitäten* beherrscht wird.

1724 Vgl. vertiefend dritter Teil, XIII. Kapitel, A.2.2.

1725 Dafür, dass sich der Wert von Personendaten nicht isoliert ökonomisch erschliessen lässt, stattdessen kontextuelle Erwägungen einschlägig sind, vgl. Karg, digma 2011, 146 ff., 148 ff.

2.2. Der Trend der Ökonomisierung

2.2.1. Im Offline-Bereich

2.2.1.1. Darstellung faktischer Prozesse

1274 Den Ausgangspunkt der Betrachtung bilden Verarbeitungs- und Geschäftspraktiken der analogen Welt. Heute setzen viele Unternehmen, die Waren und Dienstleistungen anbieten, auf sog. *Treuebindungsprogramme*, wobei in der Regel elektronische Kundenkarten zum Einsatz kommen. Elektronische Kundenkarten sind ein Element neuerer Marketinginstrumente und -möglichkeiten, namentlich des sog. *Customer Relationship Management* (CRM). Für das CRM findet sich in der umfangreichen Literatur keine einheitliche Definition.[1726] Das CRM und die zum Einsatz kommenden Datenverarbeitungsprozesse sowie Analysemethoden dienen den Unternehmen dazu, ihre Effizienz zu optimieren, Kundenbeziehungen zu generieren und zu pflegen, direkt und indirekt den Gewinn zu steigern, Fehl- und Überproduktionen zu minimieren und einen strategischen Wettbewerbsvorteil zu erlangen.[1727] Im Finanz- und Bankenbereich tritt die Funktion der Erfüllung des Know-Your-Costumers-Prinzips hinzu. Damit wird branchenspezifischen regulatorischen Vorgaben Rechnung getragen. Verarbeitungspraktiken im Rahmen des CRM verfolgen somit plurale Zwecke.[1728] Regelmässig werden unternehmensweite CRM-Gesamtsysteme mit integrierten Personalisierungs- resp. Individualisierungsprozessen aufgesetzt.[1729]

1275 Betreffend den bedeutsamen Aspekt der *Kundenbindung* sollen durch diverse Strategien neue Kunden gewonnen, bestehende Beziehungen günstiger gepflegt, der Verkauf weiterer oder ähnlicher, aber höherwertiger Produkte (Cross-Selling und Up-Selling) erreicht werden oder eine Konzentration auf besonders umsatzfreudige Konsumentinnen stattfinden. Gleichzeitig soll das Image des Unternehmens verbessert und die Effizienz gesteigert werden.[1730]

1276 Eine Kundenbindung wird mehr oder minder freiwillig erreicht. Sie kann auf der Nähe sowie Zufriedenheit der Kundinnen auf der Grundlage der Freiwilligkeit basieren oder auf Wechselbarrieren erzwungener Gebundenheit gründen.[1731]

1726 Schweizer, CRM, 33; Räuchle, 11; Haag, 11; Leusser/Hippner/Wilde, 19 f.; Eckhardt/Fattebert/Keel/Meyer, 39 ff.; zum Umgang mit Kundendaten durch KMU aus datenschutzrechtlicher Perspektive vgl. Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 159 ff.

1727 Buchner, 157.

1728 Zum Beispiel die Verhinderung von Klumpenrisiken im Zusammenhang mit Kreditvergaben oder aber die Verhinderung von Geldwäscherei.

1729 Schweizer, CRM, 45 ff.; Räuchle, 13 ff.

1730 Räuchle, 9 ff.; Haag, 12; Schweizer, CRM, 8 ff.; Schwenke, 43 und 112; zu den Kundenbindungssystemen auch Weichert, DuD 2003, 161 ff.

1731 Haag, 13 ff.; Schwenke, 43.

Mittels sog. *Direktmarketing* soll eine gemeinhin als so bezeichnete persönliche, direkte und dauerhafte Beziehung zur Kundin gepflegt werden. Anstelle unspezifischer Massenwerbung an eine wenig selektive und ausdifferenzierte Kundschaft wird die Kundin individualisiert in ihren persönlichen Bedürfnissen und Interessen angesprochen. Mutmasslich naheliegende Bedürfnisse werden geweckt; durch ihre Befriedigung und das Einräumen von Rabatten usf. soll eine langfristige Bindung an das Unternehmen erreicht werden.[1732]

Unter dem Begriff *Customized Marketing* wird die Kundin hinsichtlich der nachgefragten Leistungen individualisiert adressiert. Durch das sog. *Relationship Marketing* wird die gesamte Kommunikation und Kundenbeziehung persönlich ausgestaltet.[1733] Der Begriff des *Customer Relationship Managements* bringt zum Ausdruck, dass die Beziehung zwischen Unternehmen und Kundin resp. Konsumentin in das Zentrum der Aufmerksamkeit gestellt wird.[1734] Folglich sind Informationen über die jeweilige Kundin von herausragender Bedeutung. 1277

Die im Rahmen des sog. *operativen CRM* erhobenen, über die Kundenkarten gewonnenen Kundendaten werden vorab in das sog. Data Warehouse, eine Datenbank, eingepflegt.[1735] Die Auswertung erfolgt im Zuge des sog. *analytischen CRM*. Einer dieser Analyseprozesse ist das sog. *Data Mining*, mittels dessen im Data Warehouse automatisch neue, zuvor unbekannte Muster, Interdependenzen und Kausalitäten eruiert werden.[1736] Das analytische CRM erhöht die Effektivität des CRM, indem detaillierte Angaben über vorhandene und potentielle Kunden ausgewertet und hieraus Hypothesen abgeleitet werden. In diesem Zusammenhang werden sog. *Potentialdaten generiert*.[1737] Abgezielt wird auf die präzisere Antizipation von künftigen Verhaltensweisen der Konsumentinnen und Konsumenten. Die generierten Daten werden mittels analytischem CRM zu Kundenprofilen verarbeitet, analysiert, angereichert und fortlaufend aktualisiert.[1738] Die auf Kundendatenbasis zu Kundenprofilen erweiterten Informationen werden schliesslich zur Unterstützung von Geschäftsprozessen in Marketing, Vertrieb und Service, insb. zwecks personalisierter Werbung, eingesetzt.[1739] 1278

1732 Buchner, 147 ff.; Vesting, in: Ladeur (Hrsg.), 155 ff., 165 f.
1733 Scheja, 31 ff.; Haag, 7 ff.; Schwenke, 40 f.
1734 Vesting, in: Ladeur (Hrsg.), 155 ff., 165; zum Customer Relationship Marketing mit seinen datenschutzrechtlichen Herausforderungen Sachs, 28 ff.
1735 Zur Architektur und Entwicklung sowie Anwendung von Data-Warehouse-Systemen vgl. Bauer/Günzel (Hrsg.), *passim*; Eckhardt/Fattebert/Keel/Meyer, 41 ff.; Fasel, 11 ff.; vertiefend zum Data Warehousing sodann die zahlreichen Beiträge in Jung/Winter (Hrsg.).
1736 Vgl. Dittrich/Vavouras, digma 2001, 116 ff.; Bartuschka, CB 2019, 340 ff., 342; vgl. Linoff/Berry, 2 ff.
1737 Haag, 17 f. und 58 ff.; Räuchle, 14 f.; Schweizer, CRM, 139 ff.
1738 Schweizer, CRM, 401 f. und 407; EDÖB, 5. Tätigkeitsbericht, 62.
1739 Haag, 16 ff.

1279 Die beschriebenen Strategien beruhen auf der Annahme, dass sie umso effizienter sind, je breiter und tiefer die Datenbestände sind. Es geht um die Maximierung und Detaillierung des Datenbestandes. Angestrebt wird die Verdichtung von personenbezogenen Daten, woraus ein sog. «umfassendes Kundenprofil» – also Tiefe – generiert werden soll.[1740] Zugleich wird die maximale Breite anvisiert, indem möglichst viele Konsumierende zum Einsatz der Kundenkarte gewonnen werden sollen. Auch dieses Ziel wird unter Einsatz von Datenanalysen verfolgt. Betreiben zudem mehrere Unternehmen – bestenfalls verschiedener Branchen – gemeinsam ein Bonusprogramm, können noch präzisere und komplexere Rückschlüsse auf Vorlieben, Interessen und Verhalten eines Kunden getroffen werden.[1741]

1280 Hinter den elektronischen Kundenkarten eröffnet sich folglich in der Regel eine *netzwerkartige Struktur von Datenverarbeitungsprozessen*, wobei Anbietende unzählige Partnerverträge eingehen, um ihren Datenpool zu verbreitern und zu vertiefen. Vor dem Hintergrund der Funktionsweisen solcher Geschäfts- und Personendatenverarbeitungspraktiken erscheint die gegenüber dem konsumierenden Datensubjekt verwendete Beschreibung als «Treueprogramm», sobald elektronische Kundenkarten zum Einsatz kommen, als teilweise irreführend.

1281 Für die Schweiz sollen die Modelle und Dimensionen der Programme anhand derjenigen der beiden Grossisten Migros und Coop veranschaulicht werden. Die Migros bewarb ihr Cumulus-Programm mit den Worten «Das Cumulus-Bonusprogramm – unsere Art, Ihnen für Ihre Treue zu danken». Mittlerweile wurde das Wording angepasst. Das Programm wurde im Herbst 1997 lanciert. Nur drei Jahre später profitierten rund 3,5 Millionen Migros-Kundinnen und -Kunden in zwei Millionen Haushalten vom M-Cumulus-Programm. Hierbei liefen etwa 60 Prozent des Umsatzes über M-Cumulus, wobei sich seit dem Programmstart wöchentlich rund 5000 Personen neu anmeldeten. Das Papier-Cheque-Heft, in das man Wertmarken einklebte, wurde im Jahr 2000 aufgegeben. Heute dürfte die Teilnehmerquote um einiges höher liegen und die Migros hat ihre Partnerschaften und Unternehmenskooperationen markant ausgebaut. Auch Coop bietet eine elektronische Kundenkarte, die Supercard, an, die sie ebenso als Element ihres «Kundenbindungssystems» bezeichnet. Bei Coop können die per Supercard gesammelten Punkte teilweise quasi als «Entgelt» (z. B. während der sog. Supercash-Aktionen) wie ein anerkanntes Zahlungsmittel eingelöst werden, womit die Transformation von (Personen-)Daten in Entgelt besonders anschaulich wird.

1282 Dass es den Anbietern von elektronischen Kundenkarten (ggf. mit Zahlungsfunktion) nur punktuell um die Belohnung der «Treue» geht, bestätigt eine Gegenüberstellung ebendieser mit reinen «Stempelkarten», die teilweise ausschliesslich,

1740 Zur Anlehnung an das umfassende Persönlichkeitsprofil und zur Schwäche einer solchen kognitiven Annahme Vesting, in: Ladeur (Hrsg.), 155 ff., 167 ff.
1741 Haag, 24 ff.; vgl. Buchner, 150.

teilweise parallel zur elektronischen Karte angeboten werden.[1742] Die vielleicht altmodisch anmutenden – weil analog und auf Papier basierenden – Systeme tragen den Titel «Treuekarte» zu Recht, wird doch mit ihnen einzig und allein das treue Einkaufsverhalten belohnt. Anders bei elektronischen Kundenkarten wie beispielsweise M-Cumulus, bei denen keineswegs bloss das registrierte Kumulieren von Einkäufen mit Treuerabatten valorisiert wird. Gewiss, je öfter in einem bestimmten Geschäft eingekauft wird, desto mehr Bonuspunkte lassen sich anhäufen. Das Interesse des Unternehmens zielt indes in erster Linie auf die Sammlung von Angaben über das Einkaufsverhalten der Kundschaft. Je breiter und je regelmässiger der Einsatz von elektronischen Kundenkarten erfolgt, desto genauer lässt sich das Konsumverhalten ermitteln, woraus sich für das Geschäft prognostische, planerische und strategische Entscheidungen für die Zukunft ableiten lassen. In diesem Sinne ist der Slogan, mit dem Coop seine Supercard bewirbt, obschon mehrdeutig, durchaus aussagestark. Er lautet: «Ihre Supercard. Überraschend vielseitig».[1743]

Vielseitig sind nicht nur die geldwerten Vorteile wie Rabatte und Prämien, die 1283
sich weit über das Angebot von Coop hinaus erstrecken, indem beispielsweise Dienstleistungen der SBB, Eventbesuche wie Zirkus- und Zooeintritte als Gegenleistung angeboten werden. Selbst der Charity-Gedanke findet Integration, da gesammelte Punkte zu einem guten Zweck gespendet werden können.

Kundinnen und Kunden, die der Verarbeitung von Personendaten durch den 1284
Einsatz von elektronischen Kundenkarten zustimmen – allgemein im Rahmen des Kartenantrages, für jeden einzelnen Einkauf durch Vorlegen der Karte – erlangen somit eine Gegenleistung, namentlich für ihre Personendaten. Die Praktiken sind in juristischer Terminologie als Eigenkommerzialisierung zu qualifizieren. Auf der anderen Seite haben die entsprechenden Personendaten und die dadurch ermöglichten Analyse-, Steuerungs-, Planungs- und Prognosemöglichkeiten für die Unternehmen beträchtlichen ökonomischen Wert.

Mittels Generierung und Auswertung der gesammelten Angaben über das Kon- 1285
sumverhalten lassen sich in diverser Hinsicht *Effizienzsteigerungen* erreichen,

1742 Coop beispielsweise sieht, seit die Supercard mit «Datenauswertungsfunktion» gestaltet wird, weiterhin das sog. Trophy-System vor. Coop sieht für seine Kunden im Rahmen des Märkli-Sammelns weiterhin ein «exklusives» Treuesystem mit Klebemarken vor, das vollkommen ohne Registrierungen auskommt. Das Programm läuft unter dem Namen «Trophy». Anonym kann man bei jedem Einkauf Marken sammeln, um bei einem (Marken-)Produkt dank Marken eine Prämie zu erlangen. Interessant zu wissen wäre nun, ob das System der Trophy und das der Supercard äquivalente «Gegenleistungen» verschaffen oder ob nicht das System der Supercard, weil hier sowohl Treue als auch Datenspende bezahlt werden, attraktivere Gegenleistungen verspricht. Im Vergleich und im Nebeneinander der beiden unterschiedlichen Systeme wird deutlich, dass die Namensgebung «Treuekarte» den Kommerzialisierungsmechanismus kaschiert.

1743 Coop, Supercard, Basel 2021, <https://www.supercard.ch/de.html> (zuletzt besucht am 30. April 2021).

so anhand der bereits erwähnten profitversprechenden, individualisierten Werbeansprache und Belohnungsstrategie (Stichworte «Customer Relationship Management» resp. «Customer Relationship Marketing»). Mittel- und längerfristig ergeben die Angaben und deren Auswertung wertvolle Hinweise für die Planung und Gestaltung des Sortiments. Wann wird an welchem Ort durch wen welches Frischprodukt nachgefragt, ein anderes hingegen nicht?

1286 Eine zeit- und ortsspezifische Optimierung der Frischeprodukte erfolgt keineswegs bloss im wirtschaftlichen Interesse des Unternehmens. Indem Fehlproduktionen und Überangebote minimiert werden, können Lebensmittelressourcen nachhaltiger und schonender eingesetzt werden. Die Reduktion von Lebensmittelverschwendungen («Food Waste») ist als erstrebenswertes Ziel und allgemein anerkannte gesellschaftliche Erwartung unbestritten. Zugleich wird ein individuelles Bedürfnis der Kundinnen sowie Kunden befriedigt, dürfen diese – zusätzlich zu ihren Rabatten und Boni – eher auf das Vorhandensein der nachgefragten Frischprodukte zählen.

1287 Die Auswertung personenbezogener Angaben zum Konsumverhalten hat damit *zahlreiche Vorteile nicht nur für die Unternehmen, sondern auch für die Datensubjekte*. Sie profitieren von präziseren Angeboten sowie einer Gegenleistung für ihre Personendaten. Die Entscheidungsfreiheit wird respektiert, indem die Konsumentinnen und Konsumenten selbst entscheiden, ob sie entsprechenden Treueprogrammen beitreten oder nicht; die Wahlfreiheit wird dort wirksam abgesichert, wo parallel als Alternative Markenheftchen oder Stempelkarten zur Verfügung gestellt werden. Die Entscheidungsfreiheit wird zudem gewährleistet, da Karteninhaberinnen stets selbst entscheiden, ob sie im Einzelfall die elektronische Karte vorlegen wollen oder nicht. Und die Karteninhaber und Datensubjekte werden wirtschaftlich integriert.

2.2.1.2. Reflexion und Evaluation

1288 Von einer Degradierung des Datensubjektes zum Datenobjekt kann hier kaum gesprochen werden. Was ist aus datenschutzrechtlicher Perspektive – ohne auf dogmatische Einzelfragen einzugehen – kritisch an besagten Programmen?[1744]

1289 Zunächst mag einem die irreführende Titulierung entsprechender Geschäftsmodelle als Treueprogramme missfallen. Sie verschleiert partiell, dass die Belohnung primär eine Gegenleistung für Personendaten darstellt. Im weitesten Sinne geht es um die datenschutzrechtliche Transparenz. Die Migros hat seine Terminologie angepasst.

1744 Zu Treueprogrammen aus einer betriebswirtschaftlichen, wettbewerbsrechtlichen sowie datenschutzrechtlichen Perspektive grundlegend Seischab, *passim*.

Problematisieren lassen sich der Druck bzw. Zwang durch Manipulation und Übermacht der Massen (Gruppenzwang) im privaten Sektor sowie allfällige, aus Analyseverfahren resultierende Ungleichbehandlungen oder Beeinflussungen. Allerdings sind diese Praktiken weder was die «demokratische» noch was die ökonomische Partizipation anbelangt kritisch. Beschränkt auf den Online-Bereich und strikt angebunden an die deklarierten und beschriebenen Zwecke lösen sie aus einer Datenschutzperspektive wenig Widerstand aus. 1290

Anders dürfte die Bewertung ausfallen, wenn im Antragsformular und einer Datenschutzerklärung deklariert würde, dass die über die Kundenkarte gesammelten Personendaten zum Warenkonsum an Versicherungsgesellschaften weitergegeben werden. Wie eingangs gezeigt, sind auch diese darauf bedacht, über Personendatenverarbeitungen ihr Geschäftsgebaren zu optimieren – und je weiter und breiter die Personendatenbestände, desto «besser» die Analyseergebnisse. Informationsbegehrlichkeiten bezüglich Angaben zum Konsumverhalten dürften in Anbetracht der heutigen Erkenntnisse zu gesunden resp. ungesunden Ernährungs- und Lebensweisen auf der Hand liegen. Die vorliegende Arbeit will Antworten auf die Frage skizzieren, ob ein solcher Datentransfer im Lichte datenschutzrechtlicher Zweckerwägungen und Zielsetzungen zugelassen werden soll oder ob es Argumente gibt, die dagegensprechen. Mit anderen Worten geht es um die Frage, ob und inwiefern der Transfer von Personendaten, die in einem gewissen Kontext erhoben wurden – hier im Bereich des Verbrauchsgüterkonsums – in andere Bereiche aus einer Datenschutzperspektive zugelassen werden soll. 1291

An dieser Stelle zeigt sich einmal mehr, dass es um komplexe Prozesse und Datenflüsse in (Vertrags-)Netzwerkstrukturen geht, was eine datenschutzrechtliche Ausrichtung an der Subjekt-Objekt-Kategorisierung auf den Prüfstandstellt. Eine potenzierte Verdichtung erfährt die Netzwerkstruktur selbstredend durch das *Internet*. Längst sind Unternehmen wie Migros und Coop im Online-Geschäft tätig, womit sich über die elektronische Treuekarte hinaus weitere informationelle Welten erschliessen lassen. Für die Schweiz geht man von einem Online-Kaufvolumen von über einer Milliarde Franken aus.[1745] Wurden Datenverarbeitungsprozesse im Internet bereits im Rahmen der Thematisierung der technischen Kernkapazitäten nachgezeichnet, sollen diese nunmehr weiter vertieft werden: Denn im *Internet findet die Kommerzialisierung personenbezogener Daten eine neue, eigene Dimension*. Das Internet, so Vesting, forciert die Transformation von Personendaten in Wirtschaftsgüter.[1746] 1292

1745 Vgl. Verband des Schweizerischen Versandhandels, Medienmitteilung, Schweizer Online-Konsum wächst 2019 um 8.4 Prozent, Zug 2020, <https://www.vsv-versandhandel.ch/wp-content/uploads/2020/03/DE-2020.03.11-Medienmitteilung_VSV-GfK_Online_und_Versandhandel-2019.pdf> (zuletzt besucht am 30. April 2021).

1746 Vesting, in: Ladeur (Hrsg.), 155 ff., 164.

2.2.2. *Im Online-Bereich mit seinen Vernetzungen*

2.2.2.1. *Darstellung faktischer Prozesse*

1293 Für das Direktmarketing im Internet, das auf die kundenbezogene Individualisierung – wenn vielleicht nicht als Person mit dem Namen NN, so doch aufgrund einer IP-Adresse – abzielt, hat sich der Anglizismus der «Customization» durchgesetzt.[1747] Die Tatsache, dass sich für den Online-Bereich eine eigenständige Bezeichnung etabliert hat, ist indikativ. Es handelt sich um ein gegenüber dem Direktmarketing im Offline-Bereich unterscheidbares Phänomen. Die Migration eines Verarbeitungsprozesses von offline zu online verändert, wie bereits unter dem Titel der technologischen Potenzen beschrieben, seinen Charakter substanziell. Das gilt auch für das Direktmarketing.[1748] Besagte Veränderung allerdings wird erst in Ansätzen zur Kenntnis genommen.

1294 Fest steht, dass im Internet aktuell der grösste Teil der Angebote durch die Betroffenen nur im Austausch gegen Personendaten erlangt werden kann.[1749] Sämtliche Dienste von Google, Facebook kosten zwar keinen Rappen.[1750] Gleichwohl werden sie nicht ohne Gegenleistung angeboten: Die Nutzerinnen und Nutzer erklären sich i. d. R. damit einverstanden, dass die Unternehmen ihre personenbezogenen Daten nutzen, namentlich auch, um der Werbewirtschaft einen hochdifferenzierten Markt offerieren zu können.

1295 Die gesamte Internetwirtschaft basiert auf sog. Cookies, kleinen Textdateien, die auf der Hardware des Nutzers platziert werden und die eine eindeutige Kennung desselben ermöglichen.[1751] Allerdings können Unternehmen stets nur eigene Cookies setzen, um die ihre Homepage besuchende Person anhand der IP-Adresse zu identifizieren sowie deren Surfverhalten innerhalb der eigenen Seite zu beobachten. Weiter von Interesse ist die Frage: Von woher kommt die besuchende Person und auf welche Website browst sie weiter? Selbstständig und direkt kann

1747 Ders., a. a. O., 155 ff., 165.

1748 Barocas/Nissenbaum, 1 ff.; Nissenbaum, Vortrag, What is wrong with behavioral advertisement?, abrufbar unter: <https://www.youtube.com/watch?v=z3fbcEsR6Lw> (zuletzt besucht am 30. April 2021).

1749 Radlanski, 24.

1750 Immerhin wollen Medien neu vermehrt auf Bezahlschranken anstelle von Werbeeinnahmen setzen, vgl. NZZ vom 8. Juni 2019, 9.

1751 Vgl. Vesting, in: Ladeur (Hrsg.), 155 ff., 165 ff., insb. 171 ff.; m. w. H. Heuberger, N 104 ff.; beachte mit Blick auf die Vorgaben und Informationen EuGH, C-673/17, Urteil vom 1. Oktober 2019 – «planet49» –; zur e-Privacy-Verordnung, <https://datenrecht.ch/e-privacy-verordnung-neuer-vorschlag/> (zuletzt besucht am 30. April 2021); Council of the European Union, 5979/20, Brüssel 2020, <https://data.consilium.europa.eu/doc/document/ST-5979-2020-INIT/en/pdf> (zuletzt besucht am 30. April 2021); beachte sodann auch Art. 3 lit. o UWG; Bucher zur (teilweise geheimen) Observation im Internet und zum gigantischen Volumen des wirtschaftlichen Wertes eines E-Commerce-Marktes, 100 f.; zur Relevanz des Datenschutzrechts für den E-Commerce bereits Reding, digma 2001, 124.

das Unternehmen nicht eruieren, welchen «Weg» die surfende Person *zwischen verschiedenen Seiten* zurückgelegt hat.[1752]

Obschon der Besuch einer einzigen Homepage dazu führen kann, dass dutzende Cookies gesetzt werden, hat der isolierte Einsatz von Cookies Grenzen, was die Datengenerierung anbelangt. Erst eine netzwerkartige Vertragsstruktur im Hintergrund vermag Lücken zu schliessen, womit es für einmal *soziale Praktiken sind, die technische Grenzen überwinden*. Über Kooperationen zwischen Unternehmen mit Homepages, Online-Werbegesellschaften und sog. Werbenetzwerken wird die exakte «Spurenermittlung», die Nachzeichnung des Surfverhaltens, der Interessen, die Spur eines Individuums im Netz erfassbar und auswertbar. 1296

Als Resultat lässt sich das Individuum noch gezielter ansprechen, insb. mittels Werbung. Ein Individuum, das – wenn auch nicht als Person mit Namen, so doch aufgrund seiner IP-Adresse – identifizierbar wird und über welches exakt ermittelt werden kann, für welche Inhalte es sich in welcher Reihenfolge interessiert. 1297

Zur Illustration: Gelangt man über einen Browser auf die Homepage der FAZ, stösst man auf Werbung im klassischen Sinn. Es handelt sich um einen Werbeplatz, den die FAZ an verschiedene Unternehmen verkauft hat. Die platzierte Werbung entspricht derjenigen in der Printausgabe. Online gibt es eine weitere Art der Werbung. Auf Unternehmenshomepages finden sich «leere Felder», die alsdann mittels individualisierter, sog. interessenbasierter Werbung resp. Bannerwerbung gefüllt werden.[1753] 1298

Die individualisierte Bewerbung resultiert aus einem *Tracking und Monitoring* des Surfverhaltens der Person,[1754] die über die besagten Leerplätze alsdann mit spezifizierten und massgeschneiderten Werbungen konfrontiert wird. DoubleClick war eine der ersten Online-Werbegesellschaften, die in den Markt trat. Google stieg auffallend spät in das Online-Werbegeschäft ein und betonte stets, dass seine Praxis «interessenbasierte Werbung» und nicht «Werbung infolge einer Verhaltensanalyse» sei. DoubleClick, AdSense und weitere Unternehmen betreiben einen Server und agieren in einem Werbenetzwerk.[1755] 1299

Mit diesen und anderen Online-Werbegesellschaften kontrahieren nun Unternehmen wie die FAZ. Durch diese Verträge zwischen werbeinteressierten Unternehmen und Online-Werbegesellschaften wird letzteren die Präsenz durch deren 1300

1752 Vgl. zum sog. Cross-Site-Tracing Langheinrich/Karjoth, digma 2012, 116 ff., 122 ff.

1753 Die englische Bezeichnung für besagte Praxis, Online Behavorial Advertising, kurz OBA, ist aussagekräftig: vertiefend Barocas/Nissenbaum, 1 ff.; Nissenbaum, Vortrag, What is wrong with behavioral advertisement?, abrufbar unter: <https://www.youtube.com/watch?v=z3fbcEsR6Lw> (zuletzt besucht am 30. April 2021); vgl. auch Wenhold, 75 ff.; Langheinrich/Karjoth, digma 2012, 116 ff.

1754 Hierzu dritter Teil, VII. Kapitel, B.1.1.1.

1755 Zu den Werbenetzwerken im Internet und dem ebenda etablierten Ökosystem Langheinrich/Karjoth, digma 2012, 116 ff.; Weber, digma 2012, 110 ff.

Cookies auf den Homepages der ersteren erlaubt. Je mehr werbende Unternehmen mit einer oder mehreren Online-Werbegesellschaften kontrahieren, desto dichter verwoben ist das sich im Hintergrund entspinnende Netz des Datenaustausches. Das Ad-Network setzt Cookies und kann in der Folge eine Verknüpfung der Angaben vornehmen, also den Besuch des Nutzers auf beiden resp. mehreren Homepages tracken und diese Informationen auswerten. Ob die sodann differenziert zugeschaltete Werbung und das früher betrachtete Produkt nun aufgrund der Direktbewerbung genauer betrachtet wird, dient als Kriterium für die Ausgestaltung des Abrechnungssystems.[1756]

1301 Für das Illustrationsbeispielheisst dies: Besucht ein Internetnutzer die Homepage der FAZ, wird er hier nicht nur standardisierte Werbung erhalten, sondern auch individualisierte Werbung für Waren oder Dienstleistungen, die im Laufe früheren Surfverhaltens angesehen wurden. Die so individualisierte Werbung wird durch die Online-Werbenetzwerkgesellschaft geschaltet. Das Surfverhalten des Nutzers kann und wird hinsichtlich der Bewerbung keineswegs bloss von der FAZ und dem oder den mit ihr verbundenen Online-Werbeplattformen registriert, sondern auch von den kontrahierenden Unternehmen.

1302 Die jeweilige Marktbeherrschung der im Hintergrund agierenden Online-Intermediäre und Werbenetzwerktools wie AdSense, DoubleClick usf., die von Unternehmen wie Google, Microsoft oder Yahoo betrieben werden, ist ein einschlägiges Kriterium für die Effizienz der Tracking-Funktion: Je mehr Unternehmen mit einem Werbenetzwerkbetreiber vertraglich verbunden sind, desto grösser wird der Pool der eingespeisten und auswertbaren Angaben, desto lückenloser die Rekonstruktion des Surfverhaltens und desto treffsicherer – so die Erwartung – die Werbeansprachen.

1303 Der grösste Teil der Seiten, die im Internet, ggf. über eine Suchmaschine wie Google, besucht werden, werden einem Monitoring unterzogen.[1757] Durch Kontrahierungen zwischen online aktiven Unternehmen mit Werbenetzwerkanbietern als (nicht subjekthaft verstandene) Intermediäre mit Marktbeherrschung kann ein weiter detailliertes und granulares *Tracking und Monitoring des Surfverhaltens vorgenommen werden.*[1758]

1304 Die Ausgangssituation zeigt sich wiederum in Gestalt von verästelten und dichten netzwerkartigen informationstechnischen und vertraglichen Strukturen, in-

1756 Vgl. Wu, Antitrust L.J. 2017, 34 ff.; in der Praxis finden sich verschiedene Abrechnungsmethoden, wobei namentlich unterschieden wird, ob auf die Aufschaltung der Werbung an sich abgestellt wird oder auf das Anklicken der personalisierten Werbung.

1757 Vgl. bereits z. B. Basho, Calif. L. Rev. 2000, 1507 ff.; zu den Log Retention Policies und der Umsetzung von Aufbewahrungsschranken von Google kritisch Toubiana/Nissenbaum, J. Priv. Confid. 2011, 3 ff.

1758 Barocas/Nissenbaum, 1 ff.; Nissenbaum, 27 ff.; zur Netzwerkstruktur des Internets Tinnefeld/Buchner/Petri, 18 ff.

nerhalb derer Datenflüsse in die verschiedensten Richtungen zwischen diversen Agenten – Unternehmen diverser Branchen und Werbenetzwerke – stattfinden. Für die Nutzerinnen und Nutzer bleiben diese Prozesse und Praktiken – jeglicher Erhöhungen der Transparenz und deren Vorgaben zum Trotz – weitgehend opak und nicht nachvollziehbar. Zwar registriert eine Person die passgenaue Bannerwerbung. Allerdings, so scheint es, ziehen Vorgaben und Massnahmen zur Erhöhung der datenschutzrechtlichen Transparenz und zur Verstärkung der Integration von Datensubjekten qua Einwilligungserfordernis – beides Kernstrategien jüngster datenschutzrechtlicher Entwicklungen – primär in formeller Hinsicht Effekte für den Datenschutz nach sich.[1759]

So komplex die Prozesse und Praktiken sind, so undurchschaubar sind die sie 1305
abbildenden privacy policies, mit denen der Datenschutz gewährleistet werden soll. Kritische Worte hierzu in der New York Times:

> «We read 150 privacy policies. They were an incomprehensible disaster.»[1760]

Dasselbe Medium, die New York Times, liefert mit ihrer privacy policy die 1306
Probe aufs Exempel, um die Strategie der (versuchten) Transparenz und deren Problematik zu illustrieren:

> «Please click here to see a list of third parties that may be using cookies to serve advertising on our websites or in our apps. For example, we use Google to serve advertisements onto the NYT Services, which use the Google DoubleClick cookie, and in some cases, a unique device identifier, to show you ads based on your visit to NYTimes.com and other sites on the internet. You may opt out of the use of the Google DoubleClick cookie by visiting the Google ad and content network privacy policy.»[1761]

Wer diesen Klick wagt und sich die Mühe macht – weil man nicht Zeitung 1307
lesen will, stattdessen eine wissenschaftliche Arbeit zum Datenschutz verfasst –, stösst auf eine Liste von rund siebzehn «Werbenetzwerkagenten», mit denen die NYT kooperiert – die NYT, ein Unternehmen, das in erster Linie aufgrund seiner höchsten Qualitätsstandards im Medienkontext internationale Reputation geniesst und weniger für seine Rolle im Waren- und Dienstleistungsmarkt.[1762]

Ein ähnliches Bild findet man bei der Zeit und deren Datenschutzerklärung. Hier 1308
ist unter dem Schlagwort «Werbedienste» zu lesen:

1759 Buchner/Kühling, Beck-Komm.-DSGVO, Art. 7 N 10; Radlanski, 18; kritisch zur Einwilligung auch Rosenthal, Jusletter vom 27. November 2017, N 35; früh auf die Untauglichkeit der Zustimmung sowie die Unredlichkeit, sich hinter der Freiwilligkeit einer Informationserteilung zu verschanzen, hingewiesen hat Simitis, in: Schlemmer (Hrsg.), 67 ff., 77.

1760 Litman-Navarro, Opinion, New York Times vom 12. Juni 2019, abrufbar unter: <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html> (zuletzt besucht am 13. Juni 2019).

1761 So der Text am 13. Juni 2019; mittlerweile allerdings eine neue Version abrufbar unter: <https://www.nytimes.com/subscription/privacy-policy#/cookie> (zuletzt besucht am 30. April 2021).

1762 Vgl. auch Weichert, in: Bäumler (Hrsg.), 158 ff., 168.

> «Wir verwenden zudem Werbedienste von Drittanbietern. Diese Dienste werden unter Verwendung von Cookies von den nachfolgenden Unternehmen angeboten. Der Datenerhebung und -speicherung kann jederzeit mit Wirkung für die Zukunft widersprochen werden. Beachten Sie dazu bitte die allgemeinen Hinweise zu Cookies und die Opt-Out-Lösungen der einzelnen Anbieter: Wir nutzen DoubleClick von Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA). DoubleClick verwendet Cookies, um Ihnen für Sie relevante Werbeanzeigen zu präsentieren. Dabei wird Ihrem Browser eine pseudonyme Identifikationsnummer (ID) zugeordnet, um zu überprüfen, welche Anzeigen in Ihrem Browser eingeblendet wurden und welche Anzeigen aufgerufen wurden. Die Verwendung der DoubleClick-Cookies ermöglicht Google und seinen Partner-Webseiten die Schaltung von Anzeigen auf Basis vorheriger Besuche auf unserer oder anderen Webseiten im Internet […]. Wir nutzen Google AdWords Conversion Tracking. Dabei wird von Google AdWords ein Cookie auf Ihrem Rechner gesetzt, sofern Sie über eine Google-Anzeige auf unsere Webseite gelangt sind. Diese Cookies verlieren nach 30 Tagen ihre Gültigkeit und dienen nicht der persönlichen Identifizierung. Besuchen Sie bestimmte Seiten von uns und das Cookie ist noch nicht abgelaufen, können wir und Google erkennen, dass jemand auf die Anzeige geklickt hat und so zu unserer Seite weitergeleitet wurde. Jeder AdWords-Kunde erhält ein anderes Cookie. Cookies können somit nicht über die Webseiten von AdWords-Kunden nachverfolgt werden. Die mithilfe des Conversion-Cookies eingeholten Informationen dienen dazu, Conversion-Statistiken für AdWords-Kunden zu erstellen, die sich für Conversion-Tracking entschieden haben. Die AdWords-Kunden erfahren die Gesamtanzahl der Nutzer, die auf ihre Anzeige geklickt haben und zu einer mit einem Conversion-Tracking-Tag versehenen Seite weitergeleitet wurden. Sie erhalten jedoch keine Informationen, mit denen sich Nutzer persönlich identifizieren lassen […]. Wir nutzen Microsoft Bing Ads Conversion Tracking, […].»[1763]

1309 Es folgt eine Liste mit diversen weiteren grossen Vertragspartnernetzwerken mit Hinweisen und Links auf deren jeweilige Datenschutzerklärungen, die im Anschluss ebenso zu studieren wären, um sich datenschutzrechtlich ein Bild zu machen und um die für eine gültige Einwilligung geforderte Informiertheit zu erlangen – sofern dies in Anbetracht der Komplexität der beschriebenen Prozesse überhaupt möglich ist. Die beschriebenen Prozesse lassen sich im Lichte des Datenschutzes unter mehreren Aspekten kritisch reflektieren.

2.2.2.2. Reflexion und Evaluation

1310 Aus Privatheits- und Datenschutzerwägungen steht im Vordergrund des Unbehagens *zunächst* die *Tracking-Funktion*, also die im Hintergrund laufende, weitgehend lückenlose Beobachtung, Registrierung und Auswertung des Surfverhaltens in einer für Internetnutzer undurchschaubaren Weise, und dies einzig «zwecks

1763 Die Zeit, Datenschutzerklärung, <https://abo.zeit.de/datenschutzerklaerung/> (zuletzt besucht am 30. April 2021); weiter aufschlussreich auch der Bericht von Bouhs, Deutschlandfunk vom 2. August 2014, Datenerfassung, Der gläserne Internetnutzer, <https://www.deutschlandfunk.de/datenerfassung-der-glaeserne-internetnutzer.761.de.html?dram:article_id=293516> (zuletzt besucht am 30. April 2021).

Bewerbung».[1764] Problematisiert wird in der Literatur das intransparente und zugleich systematische Beobachten von Online-Aktivitäten. Das Tracking zwecks Direktmarketings geht weit über eine Analyse des Online-Shopping-Verhaltens hinaus: Registriert werden Besuche von sozialen Plattformen, medizinischen Informationsportalen usf. Damit ist der *zweite Vorwurf*, dem die Online-Bewerbung ausgesetzt ist, das Fehlen der Proportionalität, wird doch einzig und allein wegen der wirtschaftlichen Gewinnsteigerung der im Internet agierenden Unternehmen das Verhalten einer Person im Internet umfassend überwacht.[1765] Neuere datenschutzrechtliche Lösungsansätze, wie sie im Zuge der DSGVO, der geplanten Cookie Policy sowie der Totalrevision des DSG gewählt werden, beruhen massgeblich auf dem Ausbau der Transparenz- und Einwilligungsvorgaben.[1766]

Die *Targeting-Funktion* wird *erstens* mit der Beschneidung der Autonomie in Zusammenhang gebracht, vorab in dem Sinne, dass es nicht mehr die Subjekte selbst sind, die bestimmen, was sie zu sehen bekommen, sondern andere. Letztere sind es, die das unterbreitete Angebot definieren. Problematisiert wird eine Interferenz mit der «Identität», indem Dritte im Rahmen dieser Vorgänge über konstituierende Elemente der Identitätsbildung mitbestimmen. So bleibt eine Person unter Umständen gefangen in Gewohnheiten, die sie längst ablegen wollte, oder sie wird zu Verhaltensweisen verführt, denen sie bislang widerstehen konnte. Anders gewendet stellt sich die Frage, wo die legitime Einflussnahme endet und wo Manipulation resp. seduktive Manipulationstechniken beginnen.[1767] 1311

Hinsichtlich der Targeting-Funktion wird *zweitens* unter dem Terminus des «Panoptic Sort» das Thema der (statistischen) Diskriminierung aufgegriffen. Gemeint ist das Risiko, aufgrund eines bestimmten Kriteriums und seiner Bewertung – «falsche» Hautfarbe, Geschlecht, «falscher» Wohnort, «falscher» Beruf, wobei entsprechende Informationen unter Umständen aus unterschiedlichen Kontexten gesammelt werden – ggf. inakkurat kategorisiert zu werden («zahlungsunfähig», «spendierfreudig», «übergewichtig», «sportlich», «ungebildet», «krank») und folglich gewisse Angebote (nicht) zu erhalten.[1768] 1312

1764 Nissenbaum, Vortrag, What is wrong with behavioral advertisement? abrufbar unter: <https://www.youtube.com/watch?v=z3fbcEsR6Lw> (zuletzt besucht am 30. April 2021).

1765 Nissenbaum, Vortrag, What is wrong with behavioral advertisement? abrufbar unter: <https://www.youtube.com/watch?v=z3fbcEsR6Lw> (zuletzt besucht am 30. April 2021); Dies., 27 ff.; Barocas/Nissenbaum, 1 ff.; Buchner, 156 f.

1766 Vgl. betr. DSGVO Kraska, Datenschutz-Aufsichtsbehörden: Webtracking und EU-DSGVO, München 2018, <https://www.datenschutzbeauftragter-online.de/datenschutz-aufsichtsbehoerden-webtracking-eu-dsgvo/11209/> (zuletzt besucht am 30. April 2021); Botschaft DSG 2017–1084, 17.059, 6941 ff., 6972 ff.

1767 Barocas/Nissenbaum, 1 ff., 3 f.

1768 M. w. H. Heuberger, N 27 f.; zum «panoptic sort» auch Regan, 2 und 257 unter Hinweis auf Oscar Gandy; zur statistischen Diskriminierung vgl. Weber, SZW 2020, 20 ff.; Dickenson/Osaca, Digital Commons@USU; Parris/Dougoud/Diallo/Pfaffinger, Diversity and Inclusion: An AI-Formula for HR-success, European Data Protection Intensive Online, IAPP, 23. April 2021;

1313 *Drittens* werden automatisierte Entscheidungen aufgrund von Algorithmen und einer fehlenden Involvierung des Menschen in die Entscheidungsprozesse kritisch reflektiert.[1769] Eine Herausforderung, die in der jüngsten datenschutzrechtlichen Neuerungswelle Beachtung gefunden hat.[1770]

1314 Der vorangehende Beschrieb erhellt sodann, dass das für den Offline-Bereich beschriebene CRM als Dachbegriff mit seiner Teilstrategie des Direktmarketings sowie dem Prozess der individualisierten Pflege von Kundenbeziehungen im Online-Bereich einen neuen Charakter erlangt: Just die gemeinhin als anonym wahrgenommenen Prozesse im Internet und am Computer, die man vermeintlich unbeobachtet im «stillen Kämmerchen» ausführt, werden zu Prozessen, in denen Verhalten und Interessen detailliert analysiert werden. Das im Internet unter Einsatz neuer Informationsverarbeitungstechnologien sowie Vertragsnetzwerke vorgenommene Monitoring des Surfverhaltens mit seinen hieraus generierten Datenbeständen hat nicht mehr viel mit dem Prozedere von Unternehmen in der Offline-Welt zu tun, selbst wenn sich letztere im Rahmen von Treueprogrammen in Kooperationen zusammenschliessen.

1315 In der Online-Welt wird m. E. *weit mehr* erstellt als ein «umfassendes Kundinnen- resp. Konsumentenprofil». Vesting thematisiert und kritisiert in seinem Beitrag zum Internet und der Notwendigkeit der Transformation des Datenschutzrechts den Begriff des umfassenden Kundenprofils, zumal mit dieser Begriffsschöpfung eine Assoziation zum «vollständigen Persönlichkeitsprofil», wie es für den Kontext staatlicher Verarbeitung geprägt wurde, einhergehe. Er tritt dafür ein, Risiken und Leitbilder, wie sie für den öffentlichen Bereich beschrieben wurden, nicht *telle-quelle* in den privaten Bereich zu transferieren. Analoge Begrifflichkeiten wie das umfassende Kundenprofil würden indes exakt die Vergleichbarkeit von Risiken suggerieren.[1771] Der Autor plädiert dafür, datenschutzrechtlich die Notwendigkeit einer Differenzierung zwischen der Preisgabe sowie Verarbeitung von Personendaten im Bereich von Geschäftsbeziehungen und Verträgen über alltägliche Güter und solchen durch den Staat anzuerkennen.

1316 Gleichwohl ist ein solches Paradigma umgehend weiter zu entfalten: Weder der private Bereich noch der Online-Bereich ist ein einheitlicher, monolithischer Bereich, in dem einzig und allein die Logiken und Rationalitäten des ökonomischen Kontextes herrschen sollen. Es greift zu kurz, das Ergebnis der beschriebenen Online-Datenverarbeitungsaktivitäten isoliert in einem «Kundenprofil» aus-

Wildhaber/Lohmann/Kasper, ZSR 2019, 459 ff.; zur Diskriminierungsproblematik aufgrund des Scoring Weichert, ver.di 2008, 12 ff.

1769 Vgl. Nissenbaum, 44; mit Blick auf den Adresshandel vgl. kritisch zur ungenügenden Transparenz und Integration des Datensubjektes Buchner, 156 ff.; aufschlussreich auch Radlanski, 26 f.

1770 Zum Ganzen und vertiefend zu automatisierten Einzelfallentscheidungen und Profiling Heuberger, *passim*.

1771 Vesting, in: Ladeur (Hrsg.), 155 ff., 165 ff.

zumachen. Von einem Kundenprofil könnte mit Fug und Recht dann gesprochen werden, wenn z. B. einer Amazon-Besucherin einzig und allein aufgrund ihrer Suchanfragen auf Amazon Buchvorschläge unterbreitet würden. Ein solches Prozedere käme der Beratung in der Buchhandlung nahe. Die beschriebenen Tracking- und Targetingprozesse im Internet allerdings haben damit nur wenig gemein.

Mit besagten Tracking- und Targetingprozessen werden Angaben über den Besuch von Homepages aus *diversen Kontexten* zusammengetragen und ausgewertet. Diese Angaben werden wegen der Bedeutung von Personendaten zur Effizienzsteigerung in diversen Kontexten in verschiedenste Bereiche weiterveräusserbar.[1772] Im Rahmen der beschriebenen Prozesse und Praktiken rückt das Ziel, ein wirtschaftlich vorteilhaftes Matchmaking zu erreichen, in den Vordergrund. Darin ist ein für den Datenschutz relevanter Aspekt zu verorten, dessen Tragweite mit der Wendung der «Kommerzialisierung personenbezogener Angaben» nur ungenügend beschrieben wird. 1317

Es geht nicht, wie im Rahmen von Treueprogrammen mit elektronischen Kundenkarten, darum, im Konsumkontext Angaben über Einkäufe zu scannen, auszuwerten und im Gegenzug Rabatte usf. zu gewähren. Es geht darum, dass im Internet nahezu sämtliche *Aktivitäten ökonomischen Interessen, Zielen und Zwecken zugeführt und auf das Datensubjekt zurückgespielt werden* – ungeachtet der Frage, ob sich das Datensubjekt selbst im Konsumkontext online Waren bestellt, ob es sich über Krankheiten oder politische Geschehnisse informieren will, ob es Zeitung lesen möchte oder mit Freunden und Familienangehörigen Beziehungen pflegen will usf. 1318

Alles ist Markt – so erscheint es für das Internet. Das ist, was mit dem Titel der *expansiven Kraft des wirtschaftlichen Kontextes* gemeint ist und worin eine Kernherausforderung des Datenschutzrechts verortet wird. Es geht um die Problematik der Absorption sowie ungenügenden Adressierung pluraler resp. facettenreicher Kontexte, wobei das Datenschutzrecht die Robustheit und Integrität der jeweiligen Bereiche und Institutionen mitgarantiert. Namentlich für das Internet lässt sich im Zusammenhang mit dem Umgang mit Personendaten die Unterminierung von Zielen und Zwecken spezifischer Gesellschaftsbereiche – beispielsweise des familiären oder freundschaftlichen Bereiches oder des Gesundheitsbereiches – durch Marktlogiken nachweisen. Darin liegt ein Argument gegen die übertrumpfende Anerkennung eines Eigentums an Personendaten, welches 1319

1772 Entsprechend ist nicht auszuschliessen, dass im jüngsten Facebook-Skandal zur Manipulation des politischen Geschehens weitergereichte Personenangaben gegen Entgelt zur Verfügung gestellt wurden.

den Datenschutz gänzlich den Marktlogiken anheimstellen würde, unter Übergehung der anderen Schutzaufgaben des Rechtsgebietes.[1773]

1320 Wenn auch das Internet – hier anhand von CRM-Systemen für die Online- und die Offline-Welt beschrieben – die Topografie einer Datenverarbeitung grundlegend verändert, genügt es nicht, das Internet isoliert als eigenständigen und einheitlichen Kontext zu beschreiben. Vielmehr ist die Online-Welt, spiegelbildlich zur Offline-Welt, eine gesellschaftlich gleichermassen ausdifferenzierte Welt.[1774]

1321 Das «Netz» allerdings, so Nissenbaum, wird bis heute regelmässig als ein einheitlicher Kontext betrachtet und behandelt. Ein Kontext, in welchem ökonomische Logiken die Rationalitäten anderer Bereiche – medizinische Informierung, politische Informierung, familiäre und freundschaftliche Kommunikation, um nur einige Subsysteme zu nennen – dominieren, ja absorbieren.[1775] Der Online-Bereich ist jedoch, so wenig wie dies die Offline-Welt ist, keineswegs ein einziger grosser Markt- und Handelsplatz.[1776] Im Internet werden Freundschaften und Familienbeziehungen, zudem Berufsbeziehungen gepflegt, Zeitungen gelesen oder Waren bestellt. Dieser Befund ist für das Datenschutzrecht relevant.

1322 Für Geschäftsmodelle und -praktiken im Online-Bereich lässt sich von einer «radikalen» Überwachung sprechen, die keineswegs zum Zweck der Terrorbekämpfung, stattdessen in erster Linie zur Bewerbung und Markteffektuierung erfolgt. Sie wird gegenüber Personen vorgenommen, die als Internetnutzende zwar manchmal im Rahmen des digitalen Handels als Konsumentinnen und Konsumenten von Waren agieren. Wenn sie allerdings – wie in den Illustrationsbeispielen – beispielsweise online Zeitung lesen, dann primär in der Rolle der Sachinformation und ggf. Unterhaltung nachfragenden Person im Medienkontext.[1777]

1773 Jüngst zur Forderung eines kommerzialierungsrobusten Datenschutzrechts Bijok, 5 ff.

1774 Nissenbaum, 195 ff.

1775 Ders., 27 ff.

1776 Illustrativ für eine markdominierende Perspektive der von Engert an der Tagung der Zivilrechtslehrervereinigung in Zürich vom 10.-12. September 2018 präsentierte Beitrag. Die Konferenz stand unter dem Titel «Digitalisierung und Privatrecht», der Vortrag widmete sich digitalen Plattformen; vgl. Engert, AcP 2018, 304 ff.; der Beitrag stellte in sein Zentrum Plattformen, deren Geschäftszweck primär im Austausch von Gütern steht – Vermietung von Ferienwohnungen, Verkauf von Waren usf. sowie die Haftungsfragen. Im Hintergrund dagegen blieben digitale Plattformen wie namentlich Facebook, Gesundheitsplattformen mit Chat-Funktionen oder Partnervermittlungsplattformen, wo es an erster Stelle gerade nicht um wirtschaftliche Kommunikation geht. Unbestritten nimmt die digitale Wirtschaft einen heute bedeutsamen Platz im Netz ein. Das Netz allerdings ist weit mehr als ein Warenumschlagplatz. Wenn auch die Online-Welt eine andere ist als die Offline-Welt, beinhaltet sie durchaus ähnlich facettenreiche Lebens- und Kommunikationsbereiche und bildet ein ausdifferenziertes Milieu. So wenig man sich im analogen Leben nur als «Konsumentin» bewegt, sondern auch als «Patientin», als «Berufsfrau», als «Mutter», als «Freundin», so wenig ist das Verhalten im Netz eines des puren Marktverhaltens. Vielmehr agieren Netzbesucherinnen und Netzbesucher in *diversen Rollen*.

1777 Nissenbaum, Vortrag, What is wrong with behavioral advertisement? abrufbar unter: <https://www.youtube.com/watch?v=z3fbcEsR6Lw> (zuletzt besucht am 30. April 2021).

Ein solches Informationsinteresse kollidiert *zum einen* mit dem Datenschutzinteresse, wenn letzteres aktuell mit der Lösungsstrategie der Transparenz und informierten Einwilligung eingefangen wird. Statt Zeitung zu lesen, sind seitenlange privacy policies zu studieren. Ungeachtet der Technikaffinität, Rechtskenntnis und Sorgsamkeit im Umgang mit eigenen Daten:[1778] Das Individuum, also der Nutzer oder die Nutzerin, bleibt – jeglichen einleitenden Bekundungen wie «Der Zeit-Verlag nimmt den Schutz Ihrer personenbezogenen Daten sehr ernst. Wir möchten, dass Sie wissen, wann wir welche Daten erheben und wie wir sie verwenden»[1779] zum Trotz – ratlos, beunruhigt und uninformiert zurück. Das Studium der privacy policies nimmt Zeit und Aufmerksamkeit in Anspruch und führt dennoch im Ergebnis nur selten zu einem wesentlichen Erkenntnisgewinn, geschweige denn zu einem effizienten Datenschutz.[1780] 1323

Paradoxerweise lösen die Dokumente, die Transparenz und damit ein zentrales datenschutzrechtliches Anliegen nicht nur in Bezug auf die Gültigkeit einer allfälligen Einwilligung gewährleisten wollen – die Informiertheit –, bei der lesenden, datenschutzrechtlich sensibilisierten und aufmerksamen Person ein antikes geflügeltes Wort in Erinnerung: «Ich weiss, dass ich nichts weiss». 1324

Zum anderen wird die Aufmerksamkeit aufgrund der beschriebenen Geschäftsmodelle und -praktiken durch die Werbeansprachen «beschlagnahmt» und absorbiert.[1781] Auch deshalb wird von der expansiven Wirkung ökonomischer Interessen gesprochen. Die im Internet angebotenen Dienstleistungen sind zwar regelmässig kostenlos. Dennoch gibt es eine Gegenleistung in Gestalt von Personendaten, die in der Folge ausgewertet werden. Zusätzlich wird mit der Aufmerksamkeit der Personen bezahlt, die einer «Dauerbewerbung» anheimgestellt wird. 1325

Ob entsprechende Modelle als Ausdruck der Selbstbestimmung des Individuums und als Garanten des Datenschutzes gelesen werden dürfen, wird damit zur Debatte gestellt. In eine solche Diskussionsrichtung verweist der «Vater» des World Wide Web. Er hinterfragt die Idee, wonach es für das Web nur ein Geschäftsmo- 1326

1778 Vgl. zur Technik-Faszination und Technik-Angst Bull, Computer, 19 ff.; hierzu auch Brosette, 149 ff.

1779 So der Text der Datenschutzerklärung mit Stand am 13. Juni 2019; auch dieser Text wurde unterdessen geändert und lautet mit Stand am 25. Mai 2020: «Der Schutz Ihrer Daten ist uns ein besonderes Anliegen, selbstverständlich beachten wir sämtliche für Deutschland geltenden Datenschutzbestimmungen.»

1780 Litman-Navarro, Opinion, New York Times vom 12. Juni 2019, abrufbar unter: <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html> (zuletzt besucht am 13. Juni 2019); kritisch insofern mit Hinweis auf Lessig vgl. auch Schwartz, Wis. L. Rev. 2000, 743 ff., 748 f.; kritisch ebenso Solove, Stan. L. Rev. 2001, 1393 ff., 1459, der weder Einwilligungserklärungen noch privacy policies als taugliche Instrumente beurteilt, um Menschen Kontrolle zu verleihen.

1781 Wu, Antitrust L.J. 2017, 34 ff.

dell gäbe – dasjenige, das auf der Finanzierung durch Werbung basiere.[1782] Und vonseiten der Medien wird für das Lesen im Netz künftig vermehrt auf Bezahlschranken denn auf Werbeeinnahmen gesetzt.[1783] In Anbetracht des Volumens der Online-Werbung hat das Bundeskartellamt im Jahr 2018 eine Untersuchung des Phänomens veranlasst.[1784]

1327 Bevor über datenschutzrechtliche Strategien zur Lösung der Herausforderungen vertieft nachgedacht wird, soll das Bild mit Blick auf die aktuellen Kommerzialisierungspraktiken um eine weitere Stufe verdichtet werden.

2.2.3. Datenindustrie

2.2.3.1. Vorbemerkungen

1328 Die Expansionstendenz ökonomischer Rationalitäten wird durch die *Datenindustrie* mit ihren Informationsvermittlern, Datenagenturen oder Auskunfteien angetrieben und akzentuiert.[1785] So haben sich eigene Märkte herausgebildet, die auf den Handel von personenbezogenen Angaben und Informationen ausgerichtet sind.[1786] Eine Hauptrolle spielen die sog. Adress-, resp. Bonitäts- und Kreditauskunfteien, aber auch sog. Omnibus-Information-Broker, deren Geschäftszweck und -aktivität im Handel mit personenbezogenen Angaben selbst liegen. Die hier als Anbieter agierenden Unternehmen generieren mit anderen Worten ihren Umsatz sowie Profit einzig und allein aufgrund des Umschlags von (Personen-)Daten, deren Sammlung, Auswertung und Verkauf.

1329 Beim informationellen Marktplatz, auf dem die Berufsgattung der «Informationsprofessionisten»[1787] agiert resp. auf dem sog. «Informationszentralen»[1788] gegen Entgelt Informationen sowie Angebot und Nachfrage miteinander korrelie-

1782 Vgl. Berners-Lee, Wie das World Wide Web weiter wachsen kann, NZZ vom 7. November 2018, wobei er auch auf den fehlenden Datenschutz sowie die beherrschende Stellung von Google sowie Facebook hinweist.
1783 Simon, Wer liest, soll auch im Netz bezahlen, NZZ vom 8. Juni 2019, 9.
1784 Vgl. <https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2018/01_02_2018_SU_Online_Werbung.html> (zuletzt besucht am 20. September 2021).
1785 Vgl. Bibas, Harv. J.L. & Pub. Pol'y 1994, 591 ff., 592, wonach die Informationsökonomie grosse Vorteile bringe, allerdings kein Konsens bezüglich der Bedeutung von Herausforderungen unter dem Titel der Privacy bestünden. Der Autor plädiert für einen kontraktuellen Ansatz im privaten Bereich. Die Herausforderungen für diesen seien anders als diejenigen für den öffentlichen Bereich; zu den Informationsbrokern auch Eckhardt/Fattebert/Keel/Meyer, 34; vgl. dazu, dass die Kommerzialisierung und der Personendatenhandel ein Risiko für die privacy darstellen, Schwartz, Harv. L. Rev. 2004, 2055 ff., 2072 ff.
1786 Hierzu auch Bergelson, UC Davis L. Rev. 2003, 379 ff., 381 f.; mit illustrativen Beispielen zum Datenhandel Schwartz, Harv. L. Rev. 2004, 2055 ff., 2060 ff.
1787 Tantner, Suchmaschinen, 7.
1788 Der Begriff stammt von Krajewski, 164, 186, 209, 463.

ren, handelt es sich um kein (post-)modernes Phänomen.[1789] Bereits die Comptoirs des 13. Jahrhunderts in Paris, die Londoner Offices of Intelligence sowie das preussische Intelligenzwerk dienten dazu, Informationen betreffend Waren- resp. Dienstleistungsangebote sowie -nachfragen zu koordinieren. Sie koordinierten punktuell Informationen, die sich ihrerseits – anachronistisch gesprochen – auf spezifische Gesellschaftsbereiche zurückführen liessen: Die Information über eine stellensuchende und zuverlässige Magd im «Arbeitskontext», die Information über Namen und Adresse eines kompetenten Arztes oder Apothekers im «Gesundheitsbereich», das Angebot eines Buches im «Gütermarkt». Der Handel mit Informationen und auch Personendaten hat mit diesen Adress-, Auskunfts- und Frageämtern eine lange Tradition.

Wie aber lässt sich dieses eigenständige Geschäftsfeld aktuell genauer charakterisieren? Nachfolgend werden vorab die Auskunfteien im Allgemeinen beschrieben, um alsdann spezifisch auf die Praxis der Kreditauskunfteien einzugehen. Dabei werden erneut die Herausforderungen aus einer Datenschutzperspektive benannt. 1330

2.2.3.2. Auskunfteien im Allgemeinen

2.2.3.2.1. Darstellung faktischer Prozesse

Eine *Auskunftei* ist ein Unternehmen, das gewerbsmässig Auskünfte über private oder geschäftliche Verhältnisse anderer erteilt, beispielsweise über deren Kreditwürdigkeit.[1790] Kaum eine Auskunftei beschränkt sich unserer Tage auf die Vermittlung einer bestimmten Kategorie von Angaben wie z. B. Bonitätsauskünfte oder Adressen.[1791] Der Begriff «Adresshandel» steht daher für den Umgang mit der «Handelsware Adresse und anderen personenbezogenen Angaben».[1792] Die Grossmehrheit der Auskunfteien agiert aktuell als sog. *Omnibus-Information-Broker*.[1793] Sie wecken, bedienen und befriedigen unter Ausschöpfung umfassender Datenbestände verschiedenste Informationsbedürfnisse. 1331

1789 Hierzu erster Teil, II. Kapitel und III. Kapitel; Buchner/Kühling, Beck-Komm.-DSGVO, Art. 7 N 10; Radlanski, 18; kritisch zur Einwilligung auch Rosenthal, Jusletter vom 27. November 2017, N 35.

1790 So die Definition gemäss Duden.

1791 Hierzu illustrativ bereits BGE 97 II 97; zu Bonitätsdaten, Auskunfteien und Detekteien als Erscheinungsformen der ökonomischen Verwertung von Personendaten vgl. Weichert, in: Bäumler (Hrsg.), 158 ff., 161 ff.

1792 Buchner, 153.

1793 Vgl. Nissenbaum, 45 ff., 201 f., 204 ff.; zum Adresshandel auch Weichert, wrp 1996, 522 ff.; Hermerschmidt, MMR 2005, 155 ff.; zu Informationsmittlern resp. Infomediären weiter Weber, in: Becker/Hilty/Stöckli/Würtenberger, 405 ff., 412 ff.

1332 Nach einer Analyse des Bundeskartellamts wurde das Marktvolumen für Deutschland bereits 2005 auf mehrere hundert Millionen Euro geschätzt.[1794]

1333 *Zwei Report-Systeme* werden vorgestellt: *erstens* der Adresshandel bezüglich (potentieller) Kundenlisten, wie er im Rahmen des CRM und der personalisierten Bewerbung vorgenommen wird, und *zweitens* die Kreditauskunfteien resp. das Credit Reporting. Beide Rapportsysteme und -methoden zogen fortwährend die datenschutzrechtliche Aufmerksamkeit auf sich, wobei allem voran Kreditauskunfteien seit jeher kritischen Stimmen begegnen.[1795]

1334 Selbst in der Schweiz gaben beide Aktivitätsbereiche früh Anlass zu gerichtlichen Überprüfungen. So befasste sich der bereits diskutierte BGE 97 II 97 mit der Rechtmässigkeit des Geschäftsgebarens eines Adressverlages.[1796] Das Urteil dokumentiert, wie mit dem Verbot der Weitergabe (i. c. des Verkaufes) eines Schriftstückes, welches Mitglieder eines bestimmten Vereins listete, Angaben über ein Element des privaten Lebensbereiches (die Vereinszugehörigkeit) abgeschirmt wurden. Der Auskunftei war es nicht gestattet, ebendiese Angaben aus wirtschaftlichen Motiven weiterzureichen. Mit der Zulässigkeit des kommerziellen Transfers von Adressdaten im Lichte der datenschutzrechtlichen Vorgaben hatten sich später der EDÖB und das Bundesverwaltungsgericht in BVGer A-5225/2015 – Lucency, Urteil vom 12. April 2017 zu befassen.[1797]

1335 Hinter den ebenda zu beurteilenden Werbe-Aktivitäten in Gestalt von Werbeschreiben oder -anrufen steht regelmässig der Adresshandel als ein in das Direktmarketing resp. CRM eingebettetes Element.

1794 Bundeskartellamt, B9–32/05, Bonn 2005, <http://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Fusionskontrolle/2005/B9-32-05.pdf?__blob=publicationFile&v=3> (zuletzt besucht am 30. April 2021).

1795 Vgl. Buchner, 71 und 153 ff.; vgl. z. B. der Vorstoss Savary, abrufbar unter: <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20123578> (zuletzt besucht am 30. April 2021); zu den Kreditauskunfteien vertiefend insb. Helfrich, 21 ff.; Kamp/Weichert, *passim*; Koch, MMR 1998, 458 ff.; Rudin, digma 2007, 50 ff.; Strasser, SJZ 1997, 449 ff.; Wuermeling NJW 2002, 3508; NZZ vom 4. Januar 1995, 23 ff.; Ammann, *passim* und in NZZ vom 28. März 1990; Consumers Union, New Assault on Your Credit Rating, Consumer Reports 2001; zur Solvenzprüfung nach Schweizer Recht vgl. Schmid, in: Schmid/Girsberger (Hrsg.), 151 ff., 162 ff.

1796 *Pro memoria:* Der Betreiber M des Adressverlages bot verschiedene Adresslisten zum Kauf an. Bei einer der Listen handelte es sich um das Verzeichnis der Mitglieder des Vereins «Philanthropische Gesellschaft Union». Der Adressverlag bot das Verzeichnis in seiner Gesamtheit mit rund 400 Adressen zu etwas über CHF 300.00 an, ein Segment beschränkt auf Adressen in Zürich war bereits für rund CHF 15.00 zu haben. Auf Klage hin befand das Bundesgericht, dass der Verkauf der Liste mit Namen der Vereinsmitglieder den Schutz der Privatsphäre der Mitglieder und des Vereins selbst verletze, wobei auf Unterlassung des Adressverkaufs geurteilt wurde. Zur Begründung hiess es, dass die Mitgliedschaft in einem Verein eine unter dem Schutz von Art. 28 ZGB stehende geschützte persönliche Angelegenheit sei, wobei eine Information hierüber nicht weitergegeben und veröffentlicht werden dürfe.

1797 *Pro memoria:* Drei in Deutschland lebende Personen hatten sich an den EDÖB gewandt, um Unterstützung beim datenschutzrechtlichen Vorgehen gegenüber der Lucency AG zu erlangen. Sie hatten unerwünscht Werbeschreiben für eine Bank erhalten, wobei die Adressangaben über die Lucency AG bezogen worden waren.

In der aktuellen Praxis des Adresshandels sind – das Datensubjekt vorbehalten – meist *vier Akteure* involviert: erstens der Listeneigentümer, zweitens der Adressverlag, drittens der Adressvermittler und viertens der Listennutzer. Bezeichnenderweise wird das Datensubjekt nicht als Hauptakteur erwähnt, spielt es doch lediglich am Rande des Prozesses eine Rolle. In erster Linie tritt es im Rahmen seiner Beziehung zu einem Grossisten oder Warenhaus auf, dessen Treueprogrammteilnehmer es ist. 1336

Das Unternehmen, welches aus seinem Kerngeschäft, dem Waren- oder Dienstleistungshandel, Kundenverzeichnisse generiert, wird als *Listeneigentümer* bezeichnet. Es stellt seine Listen dem Adresshandel zur Verfügung. Die Rolle der Listeneigentümer lässt sich anhand des Warenhauses Jelmoli mit seinen früheren AGB illustrieren, an deren Stelle neuerdings indes eine Datenschutzerklärung ausgeschaltet ist: 1337

> «10.1 Der Teilnehmer willigt ein, dass seine persönlichen Angaben, Einkaufs- und Kontaktdaten sowie Daten aus dem Zugriff auf digitale Jelmoli-Kanäle gespeichert, analysiert und für die Erstellung eines Kundenprofils genutzt werden. Die Daten des Teilnehmers können von Jelmoli mit Daten von Dritten, namentlich sozialen Medien, Webanalyse-Tools und Zahlkartenanbietern, mit zusätzlichen Merkmalen zu Interessen, Hobbys, Lifestyle, Kauf- und Surfverhalten sowie Kaufkraft angereichert werden. Der Teilnehmer kann durch schriftliche Mitteilung an den Jelmoli Kundendienst jederzeit die Erstellung eines Kundenprofils untersagen. Damit verbunden ist der Verzicht auf personalisierte Angebote und Dienstleistungen.
>
> 10.2 Jelmoli und die teilnehmenden Shops können dem Teilnehmer allgemeine sowie personalisierte Produkt- und Dienstleistungsangebote per Post, E-Mail, Telefon oder SMS sowie über soziale Medien unterbreiten. Der Teilnehmer kann auf solche Angebote jederzeit mit schriftlicher Erklärung an den Jelmoli Kundendienst verzichten. Weiter kann Jelmoli die erhobenen Daten für Serviceleistungen, Angebotsoptimierungen und für Marktforschung nutzen, wobei die Daten anonymisiert bearbeitet werden. Um eine bessere Kundenberatung zu ermöglichen, sind Personendaten, die Kaufhistorie und Auszüge des Kundenprofils des Teilnehmers vom Verkaufspersonal der teilnehmenden Shops abrufbar. Mit schriftlicher Erklärung an den Jelmoli Kundendienst kann der Teilnehmer auf die Anzeige seiner Daten verzichten.
>
> 10.3 Inhaberin der Datensammlung ist Jelmoli. Jelmoli kann die gesammelten Daten zu den erwähnten Zwecken sowie zur technischen und organisatorischen Abwicklung des JELMOLI CARD Statusprogramms durch die teilnehmenden Shops, Marktforschungsinstitute, Direktmarketing- und Onlinemarketing-Dienstleister und Softwareanbieter (die „Vertragspartner") im In- und Ausland bearbeiten lassen. Dabei wird durch Vereinbarung mit der bearbeitenden Partnerfirma sowie durch geeignete technische und organisatorische Massnahmen sichergestellt, dass keine über die genannten Zwecke hinausgehende Verwendung der Daten stattfindet. Die gesammelten Daten werden vertraulich behandelt und ausser den Vertragspartnern keinen Dritten zugänglich gemacht; es sei

> denn, dass Jelmoli dazu rechtlich verpflichtet ist oder dass dies zur Wahrung berechtigter Interessen von Jelmoli notwendig ist.»[1798]

1338 Selbst wenn eine solche Textpassage gelesen wird, kann keine Kenntnis darüber erlangt werden, wer welche Personendaten in welcher Weise verarbeitet. Ein Gegenbeispiel insofern liefern z. B. die AGB der Globuscard, wo unter dem Titel «Datenschutz» zu lesen ist:

> «Indem Sie die Allgemeinen Geschäftsbedingungen (AGB) akzeptieren, nehmen Sie am Globus-Card-Programm teil. Sie erlauben der Magazine zum Globus AG, Informationen über Ihre Einkäufe zu sammeln und für Marketingzwecke auszuwerten. Gestützt auf Ihre Einkaufsdaten bei den Unternehmen Globus und Herren Globus können Warenkorbanalysen durchgeführt werden. Personendaten werden streng vertraulich behandelt und nicht ausserhalb der Magazine zum Globus AG weitergegeben oder Dritten zugänglich gemacht.»[1799]

1339 Diese sog. *Listeneigentümer* gewinnen ihre Personenangaben erfassenden Verzeichnisse («ihre Listen») anhand der Aktivitäten in ihrem primären Geschäftsfeld.[1800] Die Verarbeitung von Personendaten dient damit vorab der Effektuierung des hieran geknüpften Zweckes und Zieles.

1340 Anders bildet für die *Adressverlage* das Sammeln von Personendaten, die Aktualisierung, Auswertung, Analyse personenbezogener Angaben und ggf. die Prognosen-Bildung in Gestalt von Score-Werten sowie Verkauf resp. Handel mit entsprechenden personenbezogenen Angaben deren (Kern-)*Geschäft*. Die Adressverlage speisen ihre Datenbestände nicht bloss über Einpflegungen vonseiten der Listeneigentümer, sondern auch aus sog. «allgemein zugänglichen Quellen» wie Telefonbüchern, öffentlichen Registern, weiter durch eigene oder kooperative «Recherche-Aktivitäten» im Internet. Hierbei kommt den Geschäftsaktivitäten der Adressverlage zugute, dass sich bis heute Ansichten halten, wonach «das Internet» quasi ein «öffentlicher Bereich» darstelle.[1801] Die Adressverlage finden insb. über die sozialen Plattformen aussagekräftige und detaillierte Angaben zu Vorlieben, Interessen, Freizeitaktivitäten und Hobbies, besuchten Orten und Lokalen, aber auch zu wirtschaftlichen Lebensverhältnissen, sozialem Milieu usf.

1798 So die AGB 2018, dazumals noch abrufbar unter: <https://www.jelmoli.ch/media/pdf/DEF_JEL_AGBs_Statusprogramm_Bonusprogramm.pdf>; anders dagegen neuerdings die Datenschutzerklärung, abrufbar unter: <https://www.jelmoli.ch/datenschutz> (zuletzt besucht am 20. September 2021).

1799 So der Stand im April 2019; mit Stand am 25. Mai 2020 waren auch hier die AGB und Datenschutzerklärung geändert, wobei die Personendaten nicht mehr in dem bisher beschränkten Rahmen verarbeitet werden, vgl. <https://www.globus.ch/datenschutz/v1-1> (zuletzt besucht am 30. April 2021); festzustellen ist damit auch im Zuge dieser Schrift, dass sich Datenschutzerklärungen in hoher Frequenz ändern und entsprechend die Unübersichtlichkeit des Instruments verstärkt wird.

1800 Zum Ganzen m. w. H. Buchner, 154 ff.; Nissenbaum, 45 ff.

1801 Indikativ insofern auch Art. 12 Abs. 3 DSG; Nissenbaum, Dædalus, 32 ff., 41.

Dieses *Zusammenziehen von Personendaten aus diversen Pools und Quellen* 1341
geschieht in der Regel – abgesehen von einer vorgeschalteten Einwilligung im Rahmen der Geschäftsbeziehung mit dem Unternehmen, das zugleich Listeneigentümer ist, sowie von direkten Erhebungsaktivitäten mittels Umfragen durch die Adressverlage selbst – weitgehend «an den Datensubjekten vorbei».[1802] Die Adressverlage nehmen vor diesem Hintergrund – wird erneut die im Zuge dieser Arbeit herausgearbeitete neue Sichtweise eingenommen – die Funktion eines *Knotenpunktes* wahr. Bei ihnen fliessen unzählige Datenströme in einem Pool zusammen, wobei die gesammelten Angaben kombiniert und ausgewertet werden, um anschliessend in diverse Richtungen zu zahlreichen Akteuren in facettenreichen Handlungsfeldern distribuiert zu werden.

Eine Ausdifferenzierung findet das Geschäftsmodell, wenn zwischen die *Adress-* 1342
verlage und die *sog. Listennutzer als Endnutzer* ein sog. *Adressvermittler* oder *Listbroker* geschaltet wird.[1803] Der *Listennutzer*, der in aller Regel im Marketingbereich agiert und Werbeinteressen bedient sowie befriedigt, erhält die Listen von den Adressverlagen mit entsprechenden personenbezogenen Angaben meist nicht direkt resp. unmittelbar. Vielmehr übernimmt ein *sog. Adressvermittler resp. Listbroker*, der gegenüber Adressverlag und Listeneigentümern zu Vertraulichkeit verpflichtet ist, den Werbeversand an die jeweiligen Adressen, die der Listennutzer ansprechen will. Der Adressvermittler resp. Listbroker ist dem Listennutzer nicht nur zur Eruierung geeigneter Listen sowie zur diskreten (vertraulichen) Behandlung der Angaben verpflichtet, sondern auch zur Bewerbung. Der Adressvermittler resp. Listbroker nimmt eine Art Maklerfunktion wahr: Seine Aufgabe liegt im Zusammenführen von Listeneigentümer resp. Adressverlag und Listennutzer.

Der *Listennutzer* erhält in einem solchen Modell nur dann die vom Adressverlag 1343
zum Adressvermittler resp. Listbroker (der die Bewerbung durchgeführt hat) vermittelten Angaben, wenn die Werbeaktionen zu Rückläufen vonseiten der Beworbenen führen.[1804]

Die Ausbildung einer solchen Diskretion gewährleistenden Geschäftspraxis illus- 1344
triert für sich selbst betrachtet in eindrücklicher Weise, wie hoch der ökonomische Wert eingestuft wird, der Personenangaben zugemessen wird. Um diesen zu schützen, wird die Zurverfügungstellung resp. Verfügbarkeit der Personendaten kontrolliert und limitiert.

1802 Vgl. Buchner, 160 f.
1803 Vgl. Ders., 153 ff.: Weichert, wrp 1996, 522 ff., 523 ff., 530.
1804 Ders., 158 ff.

2.2.3.2.2. Reflexion und Evaluation

1345 Dieser Abriss zeigt, dass die Personendatenverarbeitungsprozesse über weite Strecken hinter dem Rücken der Datensubjekte ablaufen (in der Terminologie von Buchner «an den Datensubjekten vorbei»[1805]) und für diese kaum transparent, geschweige denn nachvollziehbar sind. Vollends undurchschaubar werden die Praktiken, wenn Personenangaben – wie es für den Bereich des Direktmarketings beschrieben wurde – im Internet mittels Cookies oder Web-Bugs erhoben werden.[1806]

1346 Erneut drängt sich angesichts dieser technologisch unterstützten Geschäftspraktiken die Frage auf, ob die datenschutzrechtliche Einwilligung mit ihren Gültigkeitsvoraussetzungen der Informiertheit und Freiwilligkeit überhaupt sinnhaft erfolgen kann oder ob sich diese nicht vielmehr als eine Utopie entpuppt, die vielleicht auf dem Papier, nicht aber im Lichte der datenschutzrechtlichen Realitäten zu überzeugen vermag.[1807]

1347 Zugleich bestätigt die Darlegung der Funktionsweise der beschriebenen Praktiken und Prozesse der Personendatenverarbeitung, dass eine Perzeption, die das technisch wie vertraglich hochgradig verästelte und verdichtete (Informations-)Netzwerk in die Aufmerksamkeit einschliesst, die datenschutzrechtliche Ausgangslage trefflicher zu beschreiben vermag als das datenschutzrechtlich etablierte Subjekt-Objekt-Paradigma. Die Geschäftsmodelle und Praktiken dokumentieren, wie Personendaten zwischen unzähligen Unternehmen (und wohl darüber hinaus) mit Geschäftsaktivitäten in verschiedensten Branchen unter Nutzbarkeit unterschiedlichster Medien sowie zwischen pluralen Kontexten zirkulieren. Eine solche Ausgangslage mit einer diese abbildenden Betrachtungsweise konterkariert erneut die dualistischen (sowie monistischen) und statischen Konzeptionierungen, die auf fragmentierenden und reduzierenden Vorstellungen von Datensubjekt versus Datenobjekt, öffentlichem Bereich versus privatem Bereich, Offline-Welt versus Online-Welt usf. beruhen. Der bestärkende Impuls, wonach sich ein Perspektivenwechsel im und für die Konzeptionierung des Datenschutzrechts aufdrängt, wird durch die Betrachtung der sog. Wirtschafts- und Kreditauskunfteien erhärtet.

1805 Buchner, 160 f.

1806 Vgl. zu den verschiedenen Methoden des Online-Marketings auch Kollmann/Tanasic, digma 2012, 98 ff.; Buchner, 156; Weber, digma 2012, 110 ff. mit einer Analyse der Gefahren für die Privatheit.

1807 Vertiefend hierzu dritter Teil, VIII. Kapitel, B.2.–4.; früh als Formalismus bezeichnet durch Körner, in: Simon/Weiss (Hrsg.), 131 ff., 145 ff.; Buchner/Kühling, Beck-Komm.-DSGVO, Art. 7 N 10; Radlanski, 18; kritisch zur Einwilligung auch Rosenthal, Jusletter vom 27. November 2017, N 35.

2.2.3.3. Wirtschafts- und Kreditauskunfteien

Einen eigentlichen Kulminationspunkt des in den vorangehenden Ausführungen (e)skalierend und sich sukzessive verdichtenden Bildes kommerzieller Datenverarbeitungsprozesse liefern die sog. Wirtschafts- und Kreditauskunfteien. 1348

Auch ihre Listen haben eine lange und bewegte Geschichte – bereits im Mittelalter warnten sog. *Lumpenlisten vor saumseligen Schuldnern*.[1808] Die heutigen Praktiken des sog. Credit-Scoring und -Reporting haben damit allerdings nur noch wenig gemein.[1809] 1349

Legitimiert werden die Praktiken mit wirtschaftlichen Interessen. *De lege lata* anerkennt der Schweizer Datenschutzgesetzgeber aufgrund einer abstrakten Interessenabwägung ein überwiegendes Interesse für solche Kreditauskünfte, vgl. Art. 13 Abs. 2 lit. c DSG.[1810] Mit der Totalrevision werden die Anforderungen angehoben, vgl. Art. 31 Abs. 2 lit. c nDSG. 1350

Nachfolgend werden vorab die Geschäftsprozesse beschrieben, was aufgrund der vorangehenden Erörterungen verkürzt geschieht. Es folgt die Reflexion und Evaluation: Die Praxis der Kreditauskunfteien ist, weil sie ein einschlägiges Beispiel für den Befund der expansiven Kraft ökonomischer Begehrlichkeiten und Rationalitäten darstellt, besonders geeignet, Erkenntnisse zwecks Restrukturierung des Datenschutzrechts der Zukunft zu gewinnen. 1351

2.2.3.3.1. Darstellung faktischer Prozesse

Namhafte Plattformen und Unternehmen für Wirtschafts- und Bonitätsangaben sind neben der Itonex AG und Moneyhouse in Deutschland insb. die «berühmtberüchtigte» SCHUFA AG.[1811] Sie schloss mit der früheren Orell Füssli Wirtschaftsinformationen AG (OFWI), übernommen durch die CRIF, Kooperationsverträge ab. Sodann zu nennen sind die Schober AG, Arvato Bertelsmann, in der 1352

1808 Gilomen, in: Holbach/Pauly (Hrsg.), 109 ff., 112 ff.; vgl. die Novelle aus dem Mittelalter vom Holzschnitzer und Schuldner Matteo, dem Dicken, Groebner, 7 ff., 49 ff.

1809 Zu diesen für die Schweiz Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16; Buchner, 71 und 153 ff.; Helfrich, 21 ff.; Kamp/Weichert, *passim*; Koch, MMR 1998, 458 ff.; Rudin, digma 2007, 50 ff.; Strasser, SJZ 1997, 449 ff.; Wuermeling, NJW 2002, 3508; NZZ vom 4. Januar 1995, 23 ff.; Ammann, *passim* und in NZZ vom 28. März 1990; Consumers Union, New Assault on Your Credit Rating, Consumer Reports 2001; Forschungsbericht Scoring-Systeme zur Beurteilung der Kreditwürdigkeit, Chancen und Risiken für Verbraucher, Schleswig Deutschland erg. 2005; vgl. z. B. der Vorstoss Savary, abrufbar unter: <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20123578> (zuletzt besucht am 30. April 2021); zum Scoring im Kreditwesen auch Sachs, 31 f.

1810 Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.22 f.; vgl. zu den allgemeinen Bearbeitungsgrundsätzen, die auch in diesem Zusammenhang anwendbar sind, Guntern, in: Weber/Thürer/Zäch (Hrsg.), 49 ff., 56 ff.

1811 Der SCHUFA wurde in Deutschland gar eine eigenständige rechtswissenschaftliche Dissertation gewidmet, vgl. Helfrich, *passim*, mit zahlreichen weiteren Hinweisen.

Schweiz weiter der Verein ZEK, der Verein zur Führung einer Zentralstelle für Kreditinformationen sowie IKO, der Verein zur Führung einer Informationsstelle für Konsumkredit.

1353 Alle spielen eine wichtige Rolle im Warenhandel, unter Umständen im E-Commerce. So finden sich auf der Homepage der CRIF die folgenden Worte vom Chief Financial Officer der Mövenpick Wein AG:

> «Ein wesentlicher Teil der Verkäufe von Mövenpick Wein erfolgt gegen Rechnung. Um Debitorenverlusten vorzubeugen, ist eine konsequente Bonitätsprüfung unerlässlich. Dabei verlassen wir uns auf die Wirtschaftsauskünfte des Gastropools von CRIF.»[1812]

1354 Das Credit-Scoring, so wird seit jeher legitimiert, diene *gewichtigen wirtschaftlichen Interessen*.[1813] Schätzungen für die Schweiz gehen davon aus, dass sich die Konkursverluste im Jahr 2014 auf rund CHF 1'900'000'000.00 beliefen, die Gesamtsumme der nicht einbringlichen Forderungen, also diejenigen inkludiert, die nicht betrieben wurden, auf rund CHF 8'300'000'000.00.[1814]

1355 Informationen, welche Ausfälle verhindern, minimieren oder kompensieren sollen, sind dementsprechend gefragt, wertvoll und folglich selbst kommerzialisierbar. Nutzbar gemacht werden auch Versprechungen im Zusammenhang mit dem Einsatz von Algorithmen, welche Kreditrisiken kalkulierbar machen (sollen).[1815] Was ist von diesem *prima vista* bestechenden Versprechen zu halten?

1356 Ähnlich der dargelegten Funktionsweise im Marketing-Bereich basiert das Credit-Reporting-System auf *vertraglichen Bindungen und einem eigentlichen Vertragsnetz*. Die Auskunftei fungiert quasi als zentrale Dateneinlieferungs- und verarbeitungsstelle.[1816] Sie tritt in vertragliche Beziehungen zu möglichst vielen Unternehmen, die Geld- oder Warenkredite gewähren – Banken- und Kreditinstitute, Leasinggesellschaften, Telekommunikationsanbieter, zudem Einzelhändler und Dienstleister, Warenhäuser, Versicherungen oder Vermieter usf. Die Einlieferung personenbezogener Angaben zu (potentiellen) Kundinnen und Kunden durch die kreditgebenden Unternehmen erfolgt in Erfüllung ihrer Vertragspflicht gegenüber der Auskunftei.

1357 Wie schon für die personalisierte Werbung beschrieben, bildet auch hier die *Marktmacht der Kreditauskunftei* ein zentrales Erfolgskriterium: Je grösser die Zahl an Unternehmen, die mit einer Auskunftei kontrahieren und ihrerseits

1812 So Bucher, abrufbar unter: <https://www.crif.ch/weitere-branchen/referenzen/moevenpick> (zuletzt besucht am 20. September 2021).
1813 Für eine beschränkende Auslegung allerdings Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.3; m. w. H. Buchner, 125.
1814 Vgl. Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.2 m. w. H.
1815 Vertiefend zu Funktionsweisen von Algorithmen Heuberger, N 10 ff., insb. N 17 ff. m. w. H.; Helfrich, 26 ff.; vgl. zum Scoring von Kreditrisiken insb. durch die SCHUFA Wuermeling, NJW 2002, 3508 ff.; Sachs, 31 f.
1816 Hierzu Buchner, 119 ff.

Daten resp. Informationen einpflegen, desto grösser der Datenpool und desto dichter die Grundlage, aufgrund derer Prognosen getroffen werden, wovon nicht nur die Auskunftei, sondern auch die kontrahierenden Unternehmen profitieren.

Je mehr Kreditauskunfteien untereinander in Austauschbeziehungen stehen, desto stärker «schwellen» Datenpools und Informationsflüsse an. Die CRIF beispielsweise, auf die, wie erwähnt, Mövenpick setzt, präsentiert auf ihrer Homepage unter der Rubrik «Partner» fast zwanzig weitere Auskunfteien.[1817] Mit einer solchen Zusammenarbeit zwischen der Schober AG und der Itonex AG hatte sich auch der EDÖB zu befassen.[1818] 1358

Dieses (Massen-)Phänomen – Stichwort «big is beautiful» – wird durch diverse Fusionierungen zwischen Unternehmen der Informationsindustrie «abgerundet»: Die heute aktive CRIF ist aus nahezu unüberschaubar vielen Zusammenschlüssen hervorgegangen, was ebenso für die Bestände an «informationellen Gütern» signifikante Bedeutung hat. 1359

Auskunfteien bündeln und sammeln die von den Vertragspartnern eingelieferten Angaben und reichern diese mit Angaben aus weiteren Quellen – namentlich Handelsregisterangaben[1819] – an, woraufhin eine Auswertung und Ermittlung eines prädiktiven «Bonitätswertes» zu einer Person vorgenommen wird. Hierzu werden vorab anhand bestehender Datensätze diverse Merkmalsgruppen gebildet – beispielsweise Wohngegend, Ausbildung, Beruf, Hobbies, Anzahl der Kinder usf. – und mit differenzierenden Risikowahrscheinlichkeiten versehen. (Vermeintlich) einschlägige Daten werden aus unterschiedlichsten Quellen gewonnen – Telefonbücher, Handelsregistereinträge usf. –, wobei die eingelieferten Informationen der Vertragspartner von besonderer Relevanz sind. 1360

Die Auskunfteien erteilen in Erfüllung ihrer Vertragspflicht den anfragenden Unternehmen Bonitätsangaben über einen Kreditinteressenten oder einen antragstellenden Kunden. Auf Anfrage eines Vertragsunternehmens wird eine Bonitätsauskunft erteilt, in aller Regel in Gestalt eines *Scores*. Beim Score-Wert handelt es sich um eine *Prognose* der Auskunftei *über das zu erwartende Zahlungs- und Vertragsverhalten* des potentiellen Kunden. 1361

Die Berechnung des sog. Score-Wertes erfolgt aufgrund standardisierter, statistisch-mathematischer Methoden.[1820] Sowohl die «statistisch-mathematische» Me- 1362

1817 Vgl. <https://www.crif.ch/partner/inkassopartner/> (zuletzt besucht am 20. September 2021).

1818 Vgl. Empfehlung des EDÖB vom 15. November 2012 betreffend die von Itonex AG angebotenen Dienstleistungen unter <www.moneyhouse.ch>, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April); in Deutschland befasste sich der BGH mit der SCHUFA, vgl. BGHZ 95, 362 ff. – SCHUFA Klausel; hierzu auch Buchner, 104 ff.

1819 Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.19.

1820 Prägnant insofern Weichert, ver.di 2008, 12 ff. mit dem Titel «Scoring – die gesetzliche Erlaubnis zur wissenschaftlichen Diskriminierung».

thode als auch der «Schatz eines riesigen Datenpools» werden als Garanten für akkurate und rationale Einschätzungen verkauft.[1821] Auf konkrete Anfrage des Kredit-, Handels-, Dienstleistungs- oder Telekommunikationsunternehmens hin ermittelt die Auskunftei den Score-Wert, eine Grösse, eine Note, eine Ampelfarbe, welche die (mutmassliche) Kreditwürdigkeit oder Bonität (Zahlungsfähigkeit und -willigkeit) der interessierenden Person (die an einem Vertrag interessierte Person) abbilden soll.[1822]

1363 Der Score-Wert einer konkreten Person ist nichts anderes als eine Prognose aufgrund von Erfahrungswerten anhand der Vergleichsgruppen. Das heisst: Je besser das Vertragsgebaren der Vergleichsgruppen in der Vergangenheit, desto günstiger die Prognose für die in ihrer Kreditwürdigkeit auf dem Prüfstand stehende potentielle Kundin, die von dieser Kategorisierung profitiert (oder im umgekehrten Fall davon beeinträchtigt wird).[1823] Bonitätsauskünfte – genauer Bonitätsprognosen – werden heute nicht nur von Kreditinstitutionen eingeholt. Viele in Vorleistung erbringende Unternehmen resp. Personen holen solche Bonitätsprognosen ein, z. B. Unternehmen der Telekommunikationsbranche oder Warenhäuser, die den Kauf auf Rechnung anbieten, aber auch Vermieterinnen und Vermieter.

2.2.3.3.2. Reflexion und Evaluation

1364 In Bezug auf den Datenschutz stossen die Vorgehensweisen der Kreditauskunfteien auf Widerstand.[1824] Dieser wird eindrücklich anhand der *Medienberichterstattung* und einer Sendung des Kassensturzes vom 13. August 2008 unter dem Titel «Datenschnüffler: So werden Mieter ausspioniert» dokumentiert.[1825] Berichtet wurde über Deltavista/CRIF, die sich als führende Wirtschaftsauskunftei bezeichnet und Bonitätsprognosen mittels sog. Score-Werten in der für (fast) jedermann

1821 Vergleichbar die (Fehl-)annahme, wonach Algorithmen rational und objektiv, frei von Biases sowie Vorurteilen im Kontext seien, Glatthaar, SZW 2020, 43 ff., 44 f.

1822 Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.1.

1823 Zu dieser Methode Buchner, 119 ff., insbes. 121.

1824 Zur jüngsten Diskussion im Versicherungskontext Stark, NZZ vom 28. August 2018, 9 mit Hinweis auf die politischen Vorstösse, Listen säumiger Prämienzahler abzuschaffen; allgemeiner zu Lumpenlisten und schwarzen Listen Baeriswil, digma 2003, 160 ff.; die EU-Art. 29-Datenschutzgruppe charakterisiert schwarze Listen wie folgt: «Erhebung und Verbreitung von bestimmten Daten über eine bestimmte Gruppe von Personen nach bestimmten, von der Art der jeweiligen schwarzen Listen abhängigen Kriterien […], die im Allgemeinen für die in der Liste erfassten Personen mit negativen und nachteiligen Folgen verbunden sind, welche darin bestehen können, dass eine Personengruppe dadurch diskriminiert wird, dass ihr die Möglichkeit des Zugangs zu einer bestimmten Dienstleistung verweigert wird oder dass ihr Ruf geschädigt wird.» In Europa hat sich namentlich die deutsche SCHUFA einen (nicht nur guten) Namen sowohl in den Medien, im wissenschaftlichen Schrifttum als auch in den Akten der Datenschutzbeauftragten sowie den Gesetzgebungsmaterialien gemacht; vgl. hierzu Buchner, 104 ff.; vgl. hierzu die Frage von Bull, Computer, 166 ff., ob Detekteien und Kreditauskunfteien einen fairen Schutz vor Betrügern und Schuldnern darstellen.

1825 Vgl. Müller, SRF vom 13. Mai 2008, Datenschnüffler: So werden Mieter ausspioniert, <http://www.srf.ch/sendungen/kassensturz-espresso/themen/wohnen/datenschnueffler-so-werden-mieter-ausspioniert> (zuletzt besucht am 30. April 2021).

verständlichen Gestalt einer Ampel mit rotem, gelbem und grünem Licht anbietet. Dieser sog. Mietercheck etabliere eine Art der Sippenhaft, indem potentielle Mietinteressenten infolge des Fehlverhaltens einer entfernt verwandten Person als «nicht zu empfehlen» abgestempelt wurden.

Zudem wird über den Umgang mit einem geltend gemachten Löschungsanspruch durch ein Datensubjekt berichtet: Die Auskunftei reagierte auf das Löschungsbegehren der Frau mit dem Hinweis, wonach sie sich das Löschungsbegehren nochmals überlegen möge, da eine Lücke bei einer Anfrage durch ein Unternehmen negative Konsequenzen zeitigen könnte. Deltavista hielt lapidar und sinngemäss fest, dass eine Löschung einer schlechten Bonität gleichkomme.[1826] Dass aus der fehlenden Registrierung eine Negativinterpretation i. S. eines Schlusses auf die Kreditunwürdigkeit gefolgert und in der Folge ein Vertrag verweigert würde, bestritten auf Nachfrage der Reporter die konfrontierten Banken, die Swisscom und Warenhäuser.[1827] 1365

Dass den Praktiken des Credit-Scoring Unbehagen entgegenschlägt, zeigt sich nicht nur medial, sondern auch *politisch*. Beispielhaft zu nennen ist die Motion Savary unter dem Titel «Bonitätsdatenbanken – ein Problem, das gelöst werden muss», die abgelehnt wurde.[1828] Zudem zu nennen ist das (angenommene) Postulat Schwab 16.3682 «Die Tätigkeiten von Wirtschaftsauskunfteien einschränken» vom Dezember 2016.[1829] Das Thema beschäftigte auch im Zuge der Totalrevision des DSG. Im Ergebnis wurde lediglich eine geringfügig strengere Normierung im Rahmen der Rechtfertigungsgründe verabschiedet, vgl. Art. 31 Abs. 2 lit. c nDSG. 1366

In der *Lehre und Rechtsprechung* werden Kreditauskunfteien seit jeher kritisch betrachtet: Ein Fachbeitrag aus dem Jahr 2015 taxiert das (undurchsichtige) Vorgehen der Kreditauskunfteien als nicht mit dem geltenden eidgenössischen Datenschutzgesetz kompatibel.[1830] Zwei frühe Bundesgerichtsentscheide geben Zeugnis für das seit Langem anerkannte wirtschaftliche Interesse an solchen Praktiken mit dem ihnen entgegengebrachten Widerstand. 1899 befasste sich das Bundesgericht im Entscheid Vogelsanger mit dem Versand von Listen, die 1367

1826 So Thür im Beitrag von Müller, Datenschnüffler: So werden Mieter ausspioniert: http://www.srf.ch/konsum/themen/wohnen/datenschnueffler-so-werden-mieter-ausspioniert (zuletzt besucht am 30. April 2021).

1827 Baumgartner, SRF vom 12. Juli 2013, Deltavista will heikle Daten nicht löschen, <https://www.srf.ch/sendungen/kassensturz-espresso/rechtsfragen/sonstiges-recht/deltavista-will-heikle-daten-nicht-loeschen> (zuletzt besucht am 30. April 2021).

1828 Das Schweizer Parlament, Bonitätsdatenbanken. Ein Problem, das gelöst werden muss, Bern 2012, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20123578> (zuletzt besucht am 30. April 2021).

1829 Das Schweizer Parlament, Die Tätigkeiten von Wirtschaftsauskunfteien einschränken, Bern 2016, <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163682> (zuletzt besucht am 30. April 2021).

1830 Cellina/Geissbühler, Jusletter vom 13. Juli 2015.

(vermeintlich) schlechte Schuldner auswiesen.[1831] Rechtlich nicht zu beanstanden sei die Praxis, sofern die Informationen *wahr* seien. Allerdings müsse präzisierend zwischen «saumselig» und «zahlungsunfähig» differenziert werden, und für die gelisteten Personen haben die Gründe ersichtlich zu sein, die zur jeweiligen Kategorisierung geführt hatten. Das höchste schweizerische Gericht formulierte damit bereits im 19. Jahrhundert basierend auf persönlichkeitsrechtlichen Erwägungen Vorgaben in Bezug auf die Transparenz und Richtigkeit im Rahmen der Verarbeitung von Personendaten. Besagte Grundsätze wurden ab Mitte der zweiten Hälfte des 20. Jahrhunderts Bestandteil der Datenschutzgesetzgebung, und im 21. Jahrhundert lassen sie sich als fest etablierter und konsolidierter Kern materieller datenschutzrechtlicher Vorgaben qualifizieren. Von den allgemeinen Prinzipien der Transparenz und Richtigkeit gingen weitere konkretisierende Impulse für die Gestaltung des Datenschutzrechts aus, womit der Entscheid noch richtungsweisender und zukunftsträchtiger erscheint: Die spezifischen Vorgaben zum Profiling sowie zur automatisierten Einzelfallentscheidung, wie sie mit der DSGVO und der Totalrevision einhergehen, erinnern stark an die Erwägungen in diesem alten Entscheid.[1832]

1368 Ebenso in Erinnerung gerufen wird BGE 97 II 97, der sich zur Zulässigkeit der Weitergabe eines Vereinsmitgliedschaftsverzeichnisses äusserte. Das Bundesgericht urteilte auf ein Verbot des Verkaufes der Vereinsmitgliederliste, weil es sich dabei um Angaben aus dem *privaten Lebensbereich* der Mitglieder handle. Ein (überwiegendes) Interesse an der Verbreitung der Informationen hingegen sei nicht anzuerkennen, wobei namentlich der argumentative Rückgriff der Beklagten auf die Praxis von Auskunfteien, welche vertrauliche Bankauskünfte erteilen würden, das Bundesgericht nicht überzeugte.[1833] Eine analoge Betrachtungsweise könne schon deshalb nicht verfangen, weil dem Wunsch nach den genannten Informationen in der Regel wirtschaftliche Motive zugrunde lägen. Letzteren könne eine gewisse Berechtigung zwar nicht abgesprochen werden, allerdings nur in engen Grenzen.

1369 Die Praktiken der Kreditauskunfteien gerieten wiederholt ins Visier der Behörden, wobei sich der EDÖB und in der Folge das Bundesverwaltungsgericht jüngst

1831 BGE 25 II 621.

1832 Vgl. Art. 5 lit. f und lit. g nDSG, Art. 6 Abs. 7 lit. b und lit. c nDSG sowie Art. 31 Abs. 2 lit. c Ziff. 1 nDSG sowie Art. 34 Abs. 2 lit. b nDSG; Botschaft DSG 2017–1084, 17.059, 6941 ff., 7022: «[…] jede Auswertung mit Hilfe von computergestützten Analysetechniken […]. Dazu können auch Algorithmen verwendet werden, aber deren Verwendung ist nicht konstitutiv für das Vorliegen eines Profilings. Vielmehr ist lediglich verlangt, dass ein automatisierter Auswertungsvorgang stattfindet; liegt hingegen lediglich eine Ansammlung von Daten vor, ohne dass diese ausgewertet werden, erfolgt noch kein Profiling»; beachte auch Art. 4 Nr. 4 und Art. 22 DSGVO sowie WP 29, Profiling.

1833 BGE 97 II 97, E 4.

mit den Dienstleistungen von Moneyhouse beschäftigten.[1834] Bereits 2012 erliess der EDÖB eine Empfehlung gegenüber Moneyhouse, 2015 folgte eine weitere. Mehrere Privatpersonen hatten sich beim EDÖB über Moneyhouse beschwert. Moniert wurde gemäss Beitrag in der NZZ, dass Moneyhouse über Wohnort, Geburtsdatum, Beruf und partiell über Familienverhältnisse und Immobilien ohne Einwilligung der Datensubjekte Auskunft erteile.[1835]

Der EDÖB stellte mehrere datenschutzrechtliche Verstösse fest und verlangte An- 1370
passungen der Verarbeitungsprozesse. Eine Rechtfertigung im Sektor der Bonitätsauskünfte gemäss Art. 13 Abs. 2 lit. c DSG schloss er aus, weil die Itonex AG (die Vorläufergesellschaft der Moneyhouse) zusätzlich Persönlichkeitsprofile bearbeitete. Sodann monierte er den geforderten Interessennachweis von Betroffenen, um eine Selbstauskunft erhalten zu können.[1836] Während ein Teil der Empfehlungen des EDÖB umgesetzt wurde, konnte hinsichtlich anderer Punkte keine Einigung erzielt werden. In der Folge gelangte der EDÖB im April 2015 mit einer Beschwerde an das Bundesverwaltungsgericht.

Das Gericht hielt in einem Urteil gegen das Unternehmen im Jahr 2017 fest, 1371
dass Persönlichkeitsprofile nur noch bei Vorliegen einer Einwilligung der Betroffenen bekanntgegeben werden dürften. Das Kerngeschäft – die Beschaffung von Bonitätsdaten – dagegen wurde prinzipiell nicht in Frage gestellt. Der amtierende EDÖB Lobsiger beurteilte den Bundesverwaltungsgerichtsentscheid als wegweisend.[1837]

An dieser Stelle geht es *nicht* um eine detaillierte Analyse der Praktiken im Lichte 1372
der datenschutzrechtlichen Normen.[1838] Umrissen wird, was der Praxis unter dem Titel des Datenschutzes vorgehalten wird. Dies geschieht anhand *dreier Cluster*, die mit den Stichworten *Exklusion, Intransparenz* und *Unrichtigkeit* erfasst werden.

1834 Vgl. Empfehlung des EDÖB zu Moneyhouse vom 6. November 2014, sodann bereits die Empfehlung des EDÖB an die Itonex AG vom 14. November 2011, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/empfehlungen.html> (zuletzt besucht am 30. April 2021).

1835 NZZ vom 30. April 2015.

1836 EDÖB, Empfehlung vom 6. November 2014, 1 ff., 25.

1837 Vgl. BVGer A-4232/2015 – Moneyhouse, Urteil vom 18. April 2017; in der Fallkonstellation lässt sich namentlich auch der Beginn eines Trends verzeichnen, wonach der EDÖB dem Datenschutzrecht nicht nur durch seine Empfehlung Nachachtung zu verschaffen sucht. Sofern seine Empfehlungen ignoriert werden, wird weiter auch der Weg an das Bundesverwaltungsgericht beschritten; jüngst auch geschehen im BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018.

1838 Insofern sei auf die einschlägige Lehre und Praxis verwiesen, vgl. auch Rosenthal, HK-DSG, Art. 13 N 49 ff. m. w. H.; Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16; im Mai 2020 haben sich sodann die Schweizer Wirtschaftsauskunfteien auf einen gemeinsamen Verhaltenskodex im Umgang mit Personendaten geeinigt, vgl. <https://www.crif.ch/news-und-events/news/2020/mai/kodex/> (zuletzt besucht am 30. April 2021).

1373 Vorausgeschickt sei der sog. «Take it or leave it»-Negativeffekt, der auch im Rapport des Kassensturzes sowie im Antwortschreiben der Deltavista auf ein Lösungsbegehren zum Tragen kam: Den Datensubjekten bleibe kaum eine andere Wahl, als sich besagtem Informationsregime zu beugen. Ein neuer Vertrag scheint unter Umständen nur realisierbar, wenn der Einholung einer Bonitätsauskunft resp. der Weitergabe personenbezogener Angaben zugestimmt resp. auf ein Löschungsbegehren verzichtet wird.[1839] Zentral für die datenschutzrechtlich angelegte Kritik am Credit Reporting ist, dass es gewisse Personen weitestgehend aus dem Geschäftsleben ausschliesse.[1840] Zu Recht wird attestiert, dass im Bedürfnis an Informationen zur Vertrags- und Erfüllungstreue der Individuen nicht die eigentliche datenschutzrechtliche Problematik liege. Das Einholen von Bonitätsangaben, um Risiken einer Nicht- oder Schlechterfüllung eines Vertrages zu vermeiden, sei ein legitimes Interesse. Nicht die Verweigerung eines Vertrages oder gewisser Konditionen infolge mangelhafter Bonität, die rechtskonform, korrekt und konkret diagnostiziert sowie kommuniziert wurde, sei datenschutzrechtlich problematisch.[1841] Vielmehr seien aus der Perspektive des Datenschutzrechts die *Intransparenz der Datenverarbeitungsprozesse*, die *Exklusion des Datensubjektes* aus dem Datenverarbeitungsprozess sowie die *(Un-)Richtigkeit* der Angaben resp. der Prognosen kritisch.[1842]

1374 Das Stichwort der *Intransparenz als erstes Problemfeld* umfasst mehrere kritische Elemente: Der ganz überwiegende Teil der «Konsumentinnen» weiss nicht, dass Kreditauskunfteien ihre Vertragswürdigkeit und Bonität registrieren und analysieren.[1843] Ein Versuch des Kassensturzes, von Deltavista in Erfahrung zu bringen, welche Daten über eine Person gespeichert seien und was daraus abgeleitet würde, wurde ausweichend abgeblockt. Zutreffend, wenn auch kurz, hält Hofer fest:

> «Erfährt oder vermutet eine Person, dass eine Auskunftei Daten über sie bearbeitet, wird sie zunächst das Auskunftsrecht gemäss Art. 8 DSG geltend machen.»[1844]

1375 Immerhin bietet beispielsweise die ZEK auf ihrer Homepage ein Formular zur Ausübung des Auskunftsrechts an, was – anders als die Auskunft der SCHUFA in Deutschland – kostenlos ist. Allerdings ist es faktisch unmöglich, den Verbund der Vertragsparteien und deren Vernetzungen sowie die Datenquellen, -pools und

1839 Kritisch Buchner, 119.
1840 M. w. H. Ders., 119; Cellina/Geissbühler, Jusletter vom 13. Juli 2015, N 26; vgl. auch Botschaft DSG 1998 II 404 ff., 421, 460.
1841 So Buchner, 119 ff.
1842 Zum Ganzen vertiefend Ders., a. a. O.
1843 Cellina/Geissbühler, Jusletter vom 13. Juli 2015, N 2 und N 72; so auch die Autorin dieser Schrift, die im Jahr 2019 online einen Artikel bestellen wollte auf Vorkasse, woraufhin die Lieferung infolge eines schlechten Score-Wertes nicht vorgenommen wurde. Wie es zu einem solchen Wert trotz einwandfreier Zahlungsmoral kommen konnte, vermochte indes niemand zu erklären.
1844 Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.8.

-flüsse zu durchschauen. Selbst wenn ein Auskunftsbegehren mit Erfolg geltend gemacht wird und aus dessen Geltendmachung keine negativen Aussagen gefolgert werden, bleibt der Erkenntnisgewinn für das Datensubjekt gering. In aller Regel ebenso wenig nachvollziehbar ist, wie der «bonitäre Wahrscheinlichkeitswert», der Score, gebildet wird.

Damit haben sich die Kreditauskunfteien den Namen der «Black Box» eingehandelt.[1845] Ebendies steht in einem scharfen Kontrast zu dem Narrativ, wonach die entsprechenden Prozesse glasklare, nachvollziehbare «Berechenbarkeit» liefern. Damit zusammenhängend – gleichzeitig indes ebenso unter dem Titel der «Richtigkeit» resp. «Fehlerhaftigkeit» zu erwähnen – ist weiter die Problematik der «statistic bias» und der Tatsache, wonach auch Algorithmen zumindest punktuell von Menschen programmiert werden. Damit fliessen ebenso allzu menschliche Bewertungen und (Vor-)Urteile in die Berechnungsmethoden ein, weshalb diese oftmals weit weniger rational, nachvollziehbar und berechenbar sind, als es vorgegeben wird. 1376

Daran ändert auch kein von den Kreditauskunfteien wiederkehrendes, abstrakt rezitiertes Gelöbnis auf Transparenz, Nachvollziehbarkeit und Einhaltung des Datenschutzrechts, auf die Wissenschaftlichkeit der Rechenmethoden und die «Stichhaltigkeit» der Prozesse und Ergebnisse etwas.[1846] Exemplarisch insofern nur die deutsche SCHUFA mit ihrem Slogan «Wir schaffen Vertrauen».[1847] Vollmundig werden ein «Höchstmass an Transparenz» und die «Bereitschaft, über die gesetzlichen Anforderungen hinaus alles zu tun, um den Gedanken der Transparenz zu fördern» versprochen.[1848] 1377

Unter dem Titel der Transparenz und mit Treu und Glauben kollidierend zu beurteilen ist ein Vorgehen, wonach das Einholen einer Selbstauskunft oder ein Löschungsbegehren durch das Datensubjekt – also die Wahrnehmung eines datenschutzrechtlich verbürgten Anspruches – als Bekundung eines schlechten Gewissens der ersuchenden Person interpretiert wird («sie hat etwas zu verbergen»).[1849] Es ist unrechtmässig, wenn ein rechtlich geschützter Anspruch geltend gemacht wird und dies negativ in eine Krediteinschätzung integriert wird. 1378

Im Zusammenhang mit «unredlichen» Strategien findet ein wie folgt dokumentiertes Einschüchterungs- und Druckinstrument Einsatz: In Deutschland drohte Vodafone einer Mobilfunkvertragspartnerin, eine SCHUFA-Meldung zu machen, sofern sie ihre Rechnung nicht begleichen würde. Die Abonnentin selbst war der 1379

1845 Buchner, m. w. H., 121.
1846 Hierzu mit Blick auf die SCHUFA Buchner, 120.
1847 SCHUFA, Wiesbaden 2021, <https://www.schufa.de/de/> (zuletzt besucht am 30. April 2021).
1848 Vertiefend zum Kreditscoring, der Scorewertbildung und deren Weitergabe durch die SCHUFA im Lichte des Datenschutzrechts Helfrich, 43 ff.; vgl. Kamlah, MMR 1999, 395 ff.
1849 Buchner, 123.

Auffassung, dass nicht korrekt fakturiert worden sei. Der BGH hiess eine geltend gemachte Verbraucherschutzklage gut.[1850]

1380 Solch retorsionsartiges Verhalten unter Integration unzulässiger Kriterien, fehlende, lückenhafte, aber auch abstrakte, leere oder kaum aussagekräftige Transparenzgelöbnisse, plakative Slogans und Illustrationen, wie sie die SCHUFA einsetzt, sind eher dazu geeignet, Misstrauen zu schüren denn Vertrauen zu schaffen. Folglich scheinen sie bereits für sich betrachtet im Lichte des für das Datenschutzrecht verbürgten Verarbeitungsgrundsatzes von Treu und Glauben kritisch.

1381 Hinsichtlich Transparenzvorgaben ist ebenso relevant, dass die für durchschnittliche Verbraucher und Datensubjekte *wohl relevantesten Fragen unbeantwortet bleiben*: Welche persönlichen Angaben wurden woher zusammengetragen und ausgewertet? Aufgrund welcher Personenangaben und welcher individuellen Geschäftsverhaltensweisen erfolgte eine Zuweisung in eine bestimmte Risikogruppe? Wie kommt es dazu, dass niemals betriebene Personen gleichwohl als solche mit schlechter Bonität «disqualifiziert und diskreditiert» werden? Doch selbst wenn sämtliche Kriterien sowie Prozesse und die maximale Gewährleistung von «Transparenz» gewährleistet würden – im Ergebnis vermögen diese nicht zu garantieren, dass die getätigten Datenverarbeitungsprozesse mit ihren Schlussfolgerungen für einen Menschen über- und durchschaubar, verständlich und nachvollziehbar sind.

1382 In engem Zusammenhang mit der ungenügenden Transparenz gegenüber dem Datensubjekt steht das *zweite Kritikfeld*, das Buchner *als Exklusion des Datensubjektes* aus dem Prozess beschreibt:

> «Die bisherige Datenschutzgesetzgebung mit ihren pauschalen Interessenabwägungen führt in der Praxis dazu, dass der gesamte Prozess des Credit-Reporting *am Betroffenen vorbei stattfindet*.»[1851]

1383 Der Einzelne als Konsument und Datensubjekt spielt höchstens eine Randrolle, ja erscheint zum Informationsobjekt degradiert. «Emanzipiert» das Datensubjekt sich – eine Vorstellung, die, wie gezeigt, nicht unwesentlich für die Datenschutzgesetzgebung ist –, indem es seine subjektiven Rechte wahrnimmt, wird es als «Störenfried» und «verdächtig» taxiert und mit Konsequenzen belegt. Das Datensubjekt wird regelmässig vor vollendete Werturteile (selten Tatsachen) gestellt, deren Zustandekommen es meist weder kennt noch nachvollziehen kann

1850 Deck, Heise online vom 20. März 2015, Schufa-Drohung: Verbraucherschützer klagen erfolgreich vor BGH gegen Vodafone, <http://www.heise.de/newsticker/meldung/Schufa-Drohung-Verbraucherschuetzer-klagen-erfolgreich-vor-BGH-gegen-Vodafone-2581584.html> (zuletzt besucht am 30. April 2021); während das Vorgehen der SCHUFA aus datenschutzrechtlicher Perspektive oft skeptisch beurteilt wird, beurteilte dieses Wuermeling, NJW 2002, 3508 ff., 3510 als unbedenklich.

1851 Buchner, 119.

und gegen die es mit seinen retrospektiv wirkenden und schwach ausgestalteten Betroffenenrechten nicht ankommen kann. Das Auskunftsrecht läuft auf eine Art Holschuld hinaus, auf eine Suche aufs Geratewohl.

Aus der Perspektive der Akteure des Credit Reportings – Unternehmen und Auskunfteien – bedeutet die Ausübung von Betroffenenrechten wie des Auskunfts-, Löschungs- oder Berichtigungsrechts administrativen und kostenverursachenden Aufwand. Denn in einem (gesetzgeberisch getragenen) System, das zwischen den kreditgebenden Unternehmen und den Auskunfteien aufgespannt ist, wird dem Individuum die Funktion eines Dritten, eines allfälligen Intervenienten, eines Störfaktors zugewiesen.[1852] 1384

Die jüngsten datenschutzrechtlichen Neuerungen sowohl auf europäischer Ebene als auch in der Schweiz wollen einige der hier beschriebenen Defizite beheben. Sie sehen Vorgaben für das Profiling und die automatisierte Einzelfallentscheidung vor.[1853] Allerdings bleibt fraglich, ob dieses für das Vorgehen von Kreditauskunfteien spezifische Instrumentarium eine Verbesserung mit Blick auf die Inklusion des Datensubjektes und damit für den Datenschutz bringt. 1385

Gleichwohl gilt auch an dieser Stelle, was im Zuge der bisherigen Analyse sichtbar wurde: Die auf den Subjektschutz ausgerichteten Transparenz- und Einwilligungslösungen, die auf die Integration der Person und die Gewährleistung der Autonomie abzielen, sind eher formeller Natur. Faktisch bringen sie aus mehreren Gründen kaum Effektuierungswirkungen für den Datenschutz.[1854] 1386

Damit ist auf ein *drittes Cluster* von datenschutzrechtlichen Schwierigkeiten einzugehen, das mit dem Stichwort *«Fehleranfälligkeit und Fehlerhaftigkeit»* bezeichnet werden kann. Die Kategorie der Richtigkeit versus Unrichtigkeit ist in Gestalt eines Verarbeitungsgrundsatzes seit Anbeginn der Datenschutzgesetzgebungen anerkannt. So widmet das DSG dem Grundsatz der Richtigkeit *de lege lata* eine eigenständige Bestimmung, vgl. Art. 5 DSG. Nach Totalrevision wird der Richtigkeitsgrundsatz in Art. 6 Abs. 6 nDSG verbürgt. In der DSGVO ist der Grundsatz der Richtigkeit in Art. 5 Ziff. 1 lit. d DSGVO niedergelegt. In der Datenschutzkonvention des Europarates, die ebenso erneuert wurde, findet sich das Richtigkeitsgebot in Art. 7 Ziff. 4 lit. d.[1855] An dieser Stelle, wo eine Auseinander- 1387

1852 Ders., hierzu grundlegend, 119 ff.

1853 Vgl. Art. 4 Nr. 4, Art. 22 Abs. 1 DSGVO sowie mehrere Bestimmungen in nDSG; vgl. zum Profiling und zu automatisierten Einzelfallentscheidungen gemäss DSGVO und E-DSG Heuberger, N 54 ff.; Glatthaar, SZW 2020, 43 ff., 46 ff.

1854 Kritisch und vertiefend zum Rezept der informierten Einwilligung und dem annektierenden Ansatz des Subjektschutzes dritter Teil, VIII. Kapitel, B.; vgl. kritisch auch Nissenbaum zu einem Konzept der absoluten Vorherrschaft eines Kontrollrechts durch das Datensubjekt, 2, 69 ff., 147 f.

1855 Zur Datenschutzkonvention des Europarates von 1981 vertiefend Henke, 42 ff. und 57 ff. mit dem Hinweis, wonach sich die Staaten mit dieser zur Umsetzung eines Minimalstandards im innerstaatlichen Recht verpflichten.

setzung mit den Praktiken der Kreditauskunfteien stattfindet, ist ergänzend auf den US-amerikanischen *Fair Credit Reporting Act* hinzuweisen, der für die Personendatenverarbeitungen in diesem Zusammenhang die Begriffe «accuracy» resp. «inaccurate» verwendet, § 602 lit. a Ziff. 1.[1856] Das Spektrum der Formulierungen – von der «Richtigkeit» über die «Akkuratesse» resp. die Gegenbegriffe «Fehleranfälligkeit» resp. «Fehlerhaftigkeit» – dokumentiert, dass diverse Phänomene und Ebenen datenschutzrechtlich einschlägig sind. Relevant sind namentlich die folgenden Aspekte:

1388 Die Fehlerhaftigkeit der Primärdaten – also veraltete, falsche oder unvollständige Angaben – führt zwangsläufig zu einem fehlerhaften Score. Fehlerhaftigkeit kann weiter aus einer Verwechslung verschiedener Personen resultieren. Zudem ist von der Fehlerhaftigkeit des gebildeten Score-Wertes auszugehen, also der Prognose und damit der eine Person betreffenden Schlussfolgerung zu ihrer Bonität, wenn der als Prognose gebildete Wert von der realen Bonität einer Person (mehr oder minder deutlich) abweicht, weil zwar richtige, aber ggf. irrelevante oder unsachgemässe Angaben zur Bewertung beigezogen wurden oder weil eine bestimmte Schlussfolgerung für eine bestimmte Person falsch ist. Als *Fehlerquellen* für inakkurate Kreditauskünfte werden diverse Faktoren aufgeführt: falsche Auskünfte Dritter, Übertragungsfehler, Identifikationsverwechslungen, widersprüchliche, veraltete oder unvollständige Angaben oder eben statistische Diskriminierungen.[1857]

1389 Die *Problematik der statistischen Diskriminierung* wird mit dem Einsatz von künstlicher Intelligenz und Algorithmen sowie automatisierten Entscheidungen akzentuiert.[1858] Hierzu nur einige punktuelle Gedanken: Das Narrativ, wonach Algorithmen rein objektiv, fair und frei von Vorurteilen seien und damit stets präzise Resultate lieferten, geht fehl. Es gibt hinreichend Beweis, dass künstliche Intelligenzen, ungeachtet ihres Einsatzfeldes, insb. von rassischen oder geschlechtsbezogenen Biases beeinflusst und damit mitursächlich für anschliessende Diskriminierungen sind. Es gibt mehrere Korrelationen zwischen Antidiskriminierungsrecht, Datenschutzrecht, künstlicher Intelligenz usf.

1856 Vgl. <https://www.ftc.gov/enforcement/statutes/fair-credit-reporting-act> (zuletzt besucht am 10. September 2021).

1857 Hierzu auch Cellina/Geissbühler, Jusletter vom 13. Juli 2015, N 38 ff.; Buchner, 124 f.

1858 Vgl. Weber, SZW 2020, 20 ff.; allgemein zur statistischen Diskriminierung Dickenson/Osaca, Digital Commons@USU; zum Zusammenspiel von Diskriminierung, Massnahmen zur Beseitigung von Diskriminierung sowie Algorithmen und künstlicher Intelligenz auch der Konferenzbeitrag von Parris/Dougoud/Diallo/Pfaffinger, Diversity and Inclusion: An AI-Formula for HR-success, European Data Protection Intensive Online, IAPP, 23. April 2021; Wildhaber/Lohmann/Kasper, ZSR 2019, 459 ff.; zur Diskriminierungsproblematik aufgrund des Scorings Weichert, ver.di 2008, 12 ff.; eine verständliche Umschreibung der «statistischen Diskriminierung» lässt sich abrufen unter <https://www.thoughtco.com/the-economics-of-discrimination-1147202> (zuletzt besucht am 10. September 2021).

Unbestritten dürfte vorab sein, dass das Datenschutzrecht nicht bezugslos zum Antidiskriminierungsrecht ist. Dies ist nicht der Ort, um die Korrelationen und das Zusammenspiel zwischen Datenschutzrecht, Diskriminierungsrecht und ggf. weiterer Rechtsgebiete wie dem Arbeitsrecht darzustellen. Eine vertiefende Untersuchung dürfte im Licht neuer Technologien und Verarbeitungsmethoden wie Profiling, künstliche Intelligenz und automatisierten Einzelfallentscheidungen von Interesse sein. An dieser Stelle mögen wenige Hinweise genügen: Die Relevanz des Diskriminierungsverbotes wird über Art. 1 DSGVO, aber auch Art. 1 DSG eingeführt. Geschützt werden sollen namentlich die Grundrechte und Freiheiten resp. Persönlichkeitsrechte von natürlichen Personen. Das Diskriminierungsverbot ist ein Element des Grundrechtsschutzes und des Schutzes der Persönlichkeit der Person. Entsprechend spielt das Datenschutzrecht eine Rolle im Kontext von Antidiskriminierung und *vice versa*. Diskriminierungsherausforderungen liessen sich namentlich auch über das neu geschaffene Instrument der Datenschutz-Folgenabschätzung adressieren, die sowohl die DSGVO als auch das totalrevidierte DSG vorsehen. Zudem widmen die neuen Erlasse den automatisierten Entscheidungen sowie dem Profiling spezifische Bestimmungen. Ein eigentliches Recht für Algorithmen gibt es (noch) nicht. Für ein solches dürfte zunächst die Erkenntnis relevant sein, dass die Programmierer von Algorithmen Menschen und damit nicht frei von Vorurteilen sind. Wenn der grosse Teil von Programmierern weisse Männer sind, dann muss davon ausgegangen werden, dass das die Algorithmen beeinflusst. Zudem basieren Algorithmen auf historischen Daten. Wenn z. B. ein Rekrutierungsalgorithmus auf historischen Anstellungsdaten basiert, dann darf angenommen werden, dass Top-Management-Positionen darin weitestgehend von weissen Männern besetzt sind. Entsprechend relevant wird sein, die Trainingsdaten zu monitoren sowie Strategien und Prozesse zu entwickeln, welche diskriminierende Entscheidungen identifizieren und zu Verbesserungen führen. Algorithmen müssen trainiert werden, um selbst nicht zu diskriminieren und stattdessen einen Beitrag zu leisten, um Diskriminierungen zu beseitigen. 1390

Zurück zum Credit Reporting: Für die USA ist eine Praxis nachgewiesen worden, wonach Kreditgeber *wissentlich* sog. Positivdaten – also die vertragsgemässe Erfüllung durch die Vertragspartei – *nicht* einspeisen, um so zu verhindern, dass potentielle künftige Vertragspartner aufgrund eines daraus resultierenden besseren Score-Wertes von besseren Kreditkonditionen profitieren könnten.[1859] Solche Vorgehensweisen, wonach wissentlich und willentlich relevante Angaben nicht oder falsch registriert werden, neigen zumindest dem Graubereich betrügerischer und unrechtmässiger Machenschaften zu (ähnlich wie die retorsionsartige 1391

1859 Buchner, 128.

Einspeisung einer Information, wonach ein Auskunftsbegehren indikativ für eine schlechte Bonität sei).

1392 Datenschutzrechtlich als Kernherausforderung anzusehen ist, dass die «Richtigkeit und Vollständigkeit» der *ausgewerteten* Daten *kein* Garant für einen «richtigen» resp. «akkuraten» Score ist. Letzterer stellt eine personenbezogene Angabe dar. Der Score-Wert kann trotz korrekter Rohdaten «unzutreffend» sein. Nicht nur, dass es sich beim Score um eine Momentaufnahme handelt, welche nicht zwingend aktuell sein muss.[1860] Verfälschungen resultieren aus Rechenfehlern, falsch programmierten Priorisierungen oder der Integration *irrelevanter* Kriterien wie Zahlungsschwächen weit entfernter Verwandter oder aus einem «kausalen Schluss» aufgrund eines bestimmten Wohnortes auf die Zahlungsfähigkeit. Beispielsweise kann aufgrund der den Prognosen zugrunde liegenden «Stereotypisierungen» eine dunkelhäutige Frau mit fremdländischem Namen und Wohnadresse in einem wenig vornehmen Wohnquartier sowie vier Kindern obschon aus vermögenden Verhältnissen stammend und selbst eine erfolgreiche und gutverdienende Managerin mit einer mangelnden Bonität belegt werden. Dies einzig und allein, weil mehrere Kriterien in stereotypisierender (ggf. diskriminierender) Weise bewertet und auf diese konkrete Frau angewendet werden. Der frühere EDÖB hielt in diesem Zusammenhang fest:

> «Es müssen Kriterien herbeigezogen werden, die wirklich eine Aussage zur Kreditwürdigkeit dieser Person erlauben. Wenn Kriterien wie Sippenzugehörigkeit eine Rolle spielen, dann muss ich ganz klar sagen, das erfüllt die Anforderung nicht.»[1861]

1393 Die Herausforderung, die unter dem Titel der Fehlerhaftigkeit abgehandelt wird, ist damit facettenreich. Von Fehlerhaftigkeit im engeren Sinne lässt sich sprechen, wenn Verwechslungen stattfinden, falsche oder nur unvollständige Angaben verarbeitet werden. Fehlerhaftigkeit im weiteren Sinne und datenschutzrechtlich von besonderem Interesse ist die Verarbeitung von Personendaten, die im Ergebnis zu einer falschen Bewertung der Bonität einer Person führt. Dies, weil *unsachgemässe, irrelevante* resp. *pauschalisierende* Kriterien in die Bewertung eingeflossen sind. Folglich bildet das Ergebnis – der Score – nicht die reale Zahlungsbereitschaft und -fähigkeit einer Person ab. Es geht damit im weitesten Sinne auch um das (verwirklichte) Risiko der Diskriminierung und damit um eine Problematik, die weit über das Datenschutzrecht hinausgeht.[1862]

1860 Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.31.

1861 So Thür im Beitrag von Müller, SRF vom 13. Mai 2008, Datenschnüffler: So werden Mieter ausspioniert: <http://www.srf.ch/konsum/themen/wohnen/datenschnueffler-so-werden-mieter-ausspioniert> (zuletzt besucht am 30. April 2021).

1862 Vgl. WP 29, Profiling, 5; weiterführend Goodman/Flaxman, 3; vgl. zu den verschiedenen Risiken des Profilings Guthirt/Hildebrandt, 34; Kaeser, NZZ vom 6. Juli 2019, 10; vgl. zur Problematik der Diskriminierung durch Algorithmen Wildhaber/Lohmann/Kasper, ZSR 2019, 459 ff.; zur Diskriminierungsproblematik aufgrund des Scorings Weichert, ver.di 2008, 12 ff.

Die beschriebenen Facetten der Fehlerhaftigkeit von Personenangaben kollidieren mit datenschutzrechtlichen Vorgaben: Das DSG verpflichtet Datenbearbeitende, sich über die Richtigkeit der Daten zu vergewissern, Art. 5 Abs. 1 DSG.[1863] Das gilt sowohl für die verarbeiteten (Roh-)Daten, aus denen später ein Score ermittelt wird, als auch für den errechneten Score selbst. Weil die Richtigkeit und Vollständigkeit der Personendaten zentrale Elemente einer rechtskonformen Datenbearbeitung bilden, sind die datenschutzrechtlichen Bedenken am Credit Reporting gewichtig.[1864] 1394

Auch die noch so mathematisch-statistische Rationalisierung qua modernster Technologien und Algorithmen vermag als Narrativ nicht darüber hinwegzutäuschen, dass das Ergebnis der Prognose für eine bestimmte Person falsch sein kann und damit die reale Bonität *nicht* akkurat wiedergibt. Allzu oft wird aufgrund stereotypisierter Kategorisierungen eine Hypothese über die Bonität einer Person abgebildet, welche diese in Anbetracht ihrer real zu erwartenden Zahlungsfähigkeit nicht präzis wiedergibt.[1865] 1395

Zwar ist ebenso im Kontext der Kreditauskünfte anerkannt, dass eine *Nullfehlertoleranz* nicht verlangt werden kann. Plädiert wird für einen Fehlerquotienten von einem Prozent, was aus einer analogen Anwendung der bundesgerichtlichen Vorgabe an das «Verpixeln» von Gesichtern usf. im Google-Entscheid abgeleitet wird.[1866] Gleichwohl ist davon auszugehen, dass die Praxis der Kreditauskünfte hiervon weit entfernt ist. Für Deutschland hat eine Untersuchung ergeben, dass *jede zweite Auskunft der SCHUFA fehlerbehaftet* ist.[1867] 1396

Die Fehlerhaftigkeit der Score-Werte lässt sich folglich ebenso unter dem Grundsatz der Verhältnismässigkeit problematisieren, vgl. Art. 4 Abs. 2 DSG und Art. 6 Abs. 2 nDSG. Die Weitergabe und Verwendung eines falschen Score-Wertes, also eines Wertes, der die Bonität einer bestimmten Person nicht akkurat wiedergibt, ist nicht geeignet, das mit der Datenverarbeitung deklarierte Ziel zu erreichen. Fehlerbehaftete Kreditauskünfte verletzen den Verarbeitungsgrundsatz der Verhältnismässigkeit. 1397

1863 Zum Grundsatz vertiefend vgl. zweiter Teil, V. Kapitel, B.5.; nach Totalrevision vgl. Art. 6 Abs. 5 nDSG.

1864 Buchner, 123.

1865 Bei Lichte betrachtet nähern sich die entsprechenden Praktiken dann eher einer Versicherungskonstruktion an, wobei Risiken des Kreditausfalles auf ein Kollektiv entsprechend hypothetisch gebildeter Risikokriterien umgelagert werden.

1866 Hofer, in: Passadelis/Rosenthal/Thür (Hrsg.), § 16 N 16.29 ff. mit Hinweis auf BGE 138 II 346, E 10.7.

1867 Koark, Focus online vom 15. Juli 2019, Test Falsche Daten, teure Gebühren, Test enthüllt Fehler in jeder zweiten Schufa-Auskunft, <http://www.focus.de/finanzen/banken/ratenkredit/falsche-daten-teure-gebuehren-test-enthuellt-fehler-in-jeder-zweiten-schufa-auskunft_id_4046967.html> (zuletzt besucht am 30. April 2021).

1398 Mit diesen Ausführungen ist die datenschutzrechtliche Problematik noch nicht erschöpfend erschlossen. Das Bild vervollständigt sich, wenn eine Schätzung aus den USA vor Augen geführt wird. Für den Hypothekenmarkt in den USA haben die Consumer Federation of America (CFA) und die National Credit Reporting Association (NCRA) eine ungerechtfertigte Mehrbelastung durch höhere Zinsen von bis zu 124.000 US-Dollar errechnet. Demnach verursacht ein ungünstiger(er) Darlehensvertrag als Folge eines (fälschlichen) Scores mit höherer Einstufung in eine Risikogruppe beträchtliche Mehrbelastungen und -kosten für die potentiellen Konsumentinnen und Konsumenten. Die «Gegenparteien» dagegen profitieren in erklecklicher Weise von nicht akkuraten Score-Werten. Mit anderen Worten zahlt sich eine das Datenschutzrecht missachtende Praxis wirtschaftlich aus. Das Ausmass der Fehlerquoten und ihrer Folgen ist damit keineswegs vernachlässigbar. Die Nachteile sind nicht nur datenschutzrechtlicher Natur. Darüber hinaus sind die ungerechtfertigten finanziellen (Mehr-)Belastungen für die Einzelnen immens. Die Fehlerhaftigkeit mit ihren Nachteilen für die Individuen müssen als *systemimmanent* beurteilt werden. Entsprechende Schätzungen dürften auch für andere Länder ihre Gültigkeit haben.[1868]

1399 Im Ergebnis *alimentieren* sich die kreditgebenden Unternehmen und Auskunfteien *durch und über fehlerhafte Krediteinschätzungen und -stufungen* unter Missachtung des Datenschutzrechts; zumindest teilweise pseudowissenschaftliche und pseudokausale Erklärungen dienen dazu, *wirtschaftliche Begehrlichkeiten zu befriedigen*. Die Nichteinhaltung datenschutzrechtlicher Vorgaben zahlt sich aus, und zwar zulasten jedes einzelnen betroffenen Subjektes, das unter Umständen nicht nur mit finanziellen Mehrkosten zu rechnen hat. Es ist zugleich stereotypisierenden Vorurteilen ausgesetzt.

1400 Die Praxis des Kreditauskunftswesens – die auf objektiven, relevanten und einschlägigen, aktuellen, vollständigen Kriterien basierende und nachvollziehbar eingeschätzte sowie akkurate Bonität zwecks Vermeidung verlustbringender Geschäfte – stellt sich damit *über weite Strecken selbst in Frage*. Handelt es sich um ein lukratives Geschäft für Auskunftei wie kreditgebendes Unternehmen zulasten der Datensubjekte, zeigt sich die *korrumpierende Wirkung wirtschaftlicher Begehrlichkeiten in extremis*. Das Datenschutzrecht und seine Einhaltung entfalten ihre Relevanz indes keineswegs isoliert mit der Stossrichtung eines ideell gedachten Subjektschutzes.

1401 Wenn kreditgebende Institute auf die soeben umrissenen Praktiken zurückgreifen und damit in unfairer sowie unsachlicher Weise Individuen durch höhere Zinsen und anderes mehr belasten, erodieren sie gleichzeitig das Vertrauen der Kund-

1868 Buchner, 124; ein Kreditinformationsgesetz verlangte früh Mallmann, 115 ff., weil für Menschen existentielle Entscheidungen durch die Kreditauskunfteien getroffen würden, letztere sich indes nahezu ausschliesslich auf die Interessen der Kreditgeber und andere Kunden fokussieren würden.

schaft in das eigene Geschäftsgebaren. Damit ist es die *Integrität und Effizienz des Kredit- oder Finanzsektors selbst, die durch diese Verarbeitungsprozesse kontaminiert* wird.

Ebendies statuiert der US-amerikanische *Fair Credit Report Act* unmissverständlich wie folgt: 1402

> «§ 602. Congressional findings and statement of purpose [15 U.S.C. § 1681] (a) Accuracy and fairness of credit reporting. The Congress makes the following findings: (1) The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.»

Folglich ist es der Schutz der *kontextuellen Integrität*, hier des *Finanzsektors*, den dieser datenschutzrechtlich basierte Erlass als sein Schutzziel definiert und anerkennt. Der hier freigelegte *informationelle Systemschutz* inkludiert den informationellen Subjektschutz. 1403

Ein datenschutzrechtliches Kernproblem der Kreditauskünfte liegt somit in der stereotypisierenden, oft auch unsachlichen Kategorisierung namentlich aufgrund von Angaben, die in keinem kausalen Zusammenhang zur Beurteilung der Bonität einer Person stehen. Das Resultat ist eine «Bereicherung» der agierenden Unternehmen, die mittel- und langfristig das *Vertrauen in den Finanzsektor untergräbt*. Ein solcher Effekt wird mitverursacht, wenn aus Angaben zu Wohnort oder Freundes- und Familienbeziehungen Prognosen zur Bonität einer Person abgeleitet werden. Damit fliessen zumindest teilweise kontextfremde Informationen in die Beurteilung der Zahlungsfähigkeit ein. Folglich geht von der Praxis der Kreditauskunfteien ein Erosionsrisiko für weitere gesellschaftliche Bereiche aus, namentlich den Bereich der privaten resp. persönlichen und familiären Lebensführung. 1404

Eindrücklich sichtbar wird besagtes Risiko, wenn die FAZ in der Sparte Wirtschaft berichtet: «Schufa will Facebook-Profile auswerten» und «Verbraucherschützer und Politiker sind entsetzt […]».[1869] Die SCHUFA prüfe in einem Forschungsprojekt, wie sie ihre Kreditprüfung mithilfe von Facebook und Twitter effektuieren könne. Der Datenschützer des Landes Schleswig-Holstein bezweifelte die Rechtmässigkeit der Umsetzung der Pläne und wies darauf hin, dass es sich um eine gänzlich neue Dimension der Datenbearbeitung handle. Laut der Verbraucherschutzministerin dürfe die SCHUFA nicht zum Big Brother des Wirtschaftslebens werden, und die Justizministerin hält es für inakzeptabel, 1405

1869 Vgl. FAZ vom 7. Juni 2014, Prüfung der Kreditwürdigkeit, Schufa will Facebook-Profile auswerten, <http://www.faz.net/aktuell/wirtschaft/pruefung-der-kreditwuerdigkeit-schufa-will-facebook-profile-auswerten-11776537.html> (zuletzt besucht am 30. April 2021).

dass «Facebook-Freunde und Vorlieben dazu führen, dass man zum Beispiel keinen Handyvertrag abschließen kann.»

1406 Wenn infolge von Freundschaften und dazu gehörigen Kommunikationsbeziehungen Rückschlüsse auf die Kreditwürdigkeit gezogen werden, wird ein Konnex zwischen Bereichen hergestellt, die prinzipiell der Abgrenzung voneinander bedürfen. Wenn man infolge jedweder persönlichen (Kommunikations-)Beziehung zu fürchten hat, dass daraus Rückschlüsse auf die Kreditwürdigkeit gezogen werden, wird man sich letztlich in der Gestaltung persönlicher Beziehungen mit ihren Kommunikationsbeziehungen nicht mehr frei fühlen. Einzig und allein aus kurzfristig gedachten monetären Erwägungen werden durch besagte Datenverarbeitungspraktiken der private Lebensbereich sowie die Integrität des Kreditwesens untergraben.

1407 Mit ähnlichen Herausforderungen sieht sich der *Versicherungsbereich* konfrontiert. Auskunfteien verkaufen ihre Dienste und Personendaten über sämtliche Sektoren hinweg.[1870] Doch was ist ein höherer Zinsfuss auf einem Kredit infolge eines «unfairen» Scores im Vergleich dazu, aufgrund von Negativmerkmalen auf einer «Lumpenliste» im Versicherungssektor zu kursieren, die beispielsweise anhand von Freundschaften auf Facebook zustande gekommen ist, worauf eine personalisierte Versicherungsprämie basiert wird?[1871]

1408 Abrundend lässt sich festhalten: Das Ausmass der Fehlerhaftigkeit und die Effekte der Praktiken stellen eine Kognition in Frage, wonach mathematisch-statistische, technikbasiert ermittelte Grössen und Werte per se einen unschätzbar wertvollen (Objektivitäts-)Gewinn erbringen.[1872] Das Credit Reporting mit seinen (pseudo-)statistisch-rechnerischen Verfahren wird zur Technik stilisiert, zur erleichternden Ordnung für eine Gesellschaft, in der Wirtschaftlichkeit und Objektivität hoch gesetzte Ziele sind. Allzu oft kommt es als Druckinstrument gegenüber Konsumentinnen und Konsumenten zum Einsatz, die aufgrund der Unberechenbarkeit des Systems und der hohen Fehleranfälligkeit alles tun werden, um keine Negativdaten zu generieren. Allerdings hängt dies, wie gezeigt, bei Weitem nicht nur von ihrem eigenen Verhalten ab, worin eines der vielen Probleme des Credit Reporting zu verorten ist. Es handelt sich um ein System, das zulasten potentieller und vertragstreuer Verbraucherinnen und Verbraucher die Datenindustrie, aber auch entsprechende Dienste in Anspruch nehmende

1870 Vgl. Nissenbaum, 45 ff.

1871 Vgl. zur Erhebung von Personendaten im Rahmen des Abschlusses von Versicherungsverträgen Brunner, in: Schaffhauser/Horschik (Hrsg.), 142 ff.; bezüglich der Privatversicherungen Zittel, in Passadelis/Rosenthal/Thür (Hrsg.), § 12 N 12.6 ff.; zum Datenschutz im Kontext der Sozialversicherungen Prieur, in: Passadelis/Rosenthal/Thür (Hrsg.), § 13 N 13.1 ff.; Buchner, 137.

1872 Eine historische Aufarbeitung des Ziels von Objektivität durch quantifizierende Methoden findet sich bei Porter, *passim*.

Handels-, Kommunikations- und Kreditunternehmen alimentiert: Riesige und zahlreiche florierende Unternehmen fungieren mit gigantischen Umsätzen als Auskunfteien. Die kreditgewährenden Unternehmen als deren Klientinnen und Klienten häufen aufgrund nicht akkurater negativer Scores mittels scheinbar gerechtfertigter erhöhter Zinsbelastungen beträchtliche Gewinne an. Wenn sich die Datenindustrie wie auch die Finanzindustrie durch pseudosachliche Analyseergebnisse zulasten der Betroffenen bereichern, erodieren sie ihre Vertrauens- sowie Glaubwürdigkeit. Damit wird ihre Funktionstüchtigkeit, zu welcher auch die Wirtschaftlichkeit gehört, untergraben. Das (kurzfristig gedachte) kapitalistische Interesse infiltriert weitere Gesellschaftsbereiche, wobei ebenda generierte Personenangaben nicht immer die hinreichende Konnexität zur Frage der Kreditwürdigkeit aufweisen. Welche Freunde eine Person hat, wo sie wohnt, wie ihr Name lautet, wie viele Kinder sie hat usf. kann, muss aber nichts über ihre Zahlungswilligkeit oder -fähigkeit aussagen.[1873] Werden indes entsprechende Angaben aus Bereichen mit ungenügend garantierter Konnexität zur Beurteilung einer Eigenschaft im Konsum- und Kreditbereich transferiert und hierbei zulasten der Personen ungerechtfertigte monetäre Vorteile generiert, werden nicht nur einzelne Individuen unfair behandelt. Beschädigt werden sowohl der Bereich des Kredit- und Konsumwesens als auch der Bereich persönlicher resp. familiärer Beziehungen und Lebensführung.

1409 In der einbettenden Beschreibung der Praxis der Kreditauskunfteien spiegelt sich einmal mehr wider, dass das Bild des informationellen und technischen Netzwerkes mit Datenreservoirs sowie Datenflüssen die Ausgangslage und Realitäten, auf welche das Datenschutzrecht zu reagieren hat, weitaus besser trifft als eine Fokussierung auf das Datensubjekt mit quasi-objekthaften Personendaten. Wenn auch die problematisierten Verarbeitungstechniken offensichtlich einschlägige, auch rechtlich relevante negative Konsequenzen für die Einzelnen bringen, sollten diese nicht die Wahrnehmung der systemischen Dimension annektieren, wonach die Gesellschaftsbereiche, in welche die fraglichen Verarbeitungstechniken eingebettet sind, systemisch auf den Prüfstand gestellt werden.

2.3. Kontextualisierende Schlussfolgerungen

1410 Unter dem Schlagwort der *Ökonomisierung resp. Transformation von Personendaten in Wirtschaftsgüter resp. der Generierung pekuniärer Werte durch Personendaten* lassen sich diverse Prozesse, Praktiken, Methoden resp. Modelle beschreiben. Es handelt sich um ein heterogenes Phänomen. Nicht nur, dass sich ein Markt für Personendaten etabliert hat und Personendaten wie Güter abgegriffen,

1873 Kritisch zu diesen beiden Kategorien unter dem Titel des Grundsatzes der Datenrichtigkeit vgl. Cellina/Geissbühler, Jusletter vom 13. Juli 2015, N 20 ff.

gehandelt und verwertet werden. Auch in unzähligen weiteren Zusammenhängen – im Gesundheits- und Versicherungsbereich, im Forschungsbereich usf. – werden über Personendaten wirtschaftlich relevante Vorteile generiert.

1411 Die ökonomische Relevanz persönlicher Angaben hat aus rechtlicher Perspektive zunächst unter dem Titel der sog. Kommerzialisierung von Prominenten in den Medien beschäftigt.[1874] Damit baute sich ein Spannungsfeld auf zwischen der Kommerzialisierung von Persönlichkeitsmerkmalen auf der einen und Angaben mit einer Dogmatik der ideellen Natur des Persönlichkeitsrechts auf der anderen Seite. Diskutiert wurden Konstellationen der sog. Eigenkommerzialisierung sowie der Fremdkommerzialisierung. Seit rund zehn Jahren werden Personendaten selbst von Nichtprominenten zusehends eigen- und fremdkommerzialisiert.[1875] Die vorangehenden Ausführungen zielten darauf ab, ein Phänomen präziser zu umreissen, das in der juristischen Debatte unter dem Titel der Kommerzialisierung von Personendaten resp. der Persönlichkeit oder von Persönlichkeitsgütern diskutiert wird. Das ist im Lichte der Anknüpfung des Datenschutzrechts für den privaten Bereich im zivilrechtlichen Persönlichkeitsschutz konsequent.[1876] An dieser Stelle war es gleichwohl kein Ziel, einen weiteren dogmatischen Beitrag zur Ausdifferenzierung oder Konsolidierung der intensiv und zuweilen unruhig geführten zivilrechtlichen Auseinandersetzungen – so die Worte von Büchler – vorzulegen. Die einschlägigen Praktiken wurden folglich nicht einzig im Lichte der Art. 27 f. ZGB resp. der konkretisierenden Bestimmungen des DSG reflektiert.

1412 Vielmehr wurden die *(Geschäfts-)Praktiken als zweite faktische Hauptherausforderung* des Datenschutzes (durchaus in ihrem Zusammenwirken mit der ersten faktischen Hauptherausforderung, den Informationsverarbeitungstechnologien) im Zusammenhang mit Personendatenverarbeitungsprozessen mit einem erweiterten Fokus beschrieben. Dies führte zu dem Befund, wonach die Expansion von Geschäftsaktivitäten ins Internet zu absorbierenden Wirkungen der ökonomischen Rationalitäten führt. Ein Trend der *expansiven Kraft ökonomischer*

1874 Vgl. Büchler, AcP 2006, 300 ff., 303 ff.; Emmenegger, in: Gauch/Pichonnaz (Hrsg.), 209 ff.; Ladeur, 9 ff.; Biene, 3 ff.; Höning, 1 ff.; Meyer, *passim*; Freitag, *passim*.

1875 Vgl. Unseld, 11 ff.; Specht, 11 ff.; Buchner, DuD 2010, 39 ff.; spezifisch mit Blick auf den Namen Bunneberg, *passim*; Burkert, Fakten. Die Zeitschrift für Datenschutz des Kantons Zürich, Sondernummer 4/1996, 23 ff.; zur ideologischen Sonderzone, in der das Persönlichkeitsrecht operiert, wohingegen der übrige Bereich des Privatrechts dem *homo oeconomicus* gewidmet ist, Emmenegger, in: Gauch/Pichonnaz (Hrsg.), 209 ff., 210 ff. mit dem Hinweis auf BGE 110 II 411, E 3, der vor einer Zweckentfremdung des Persönlichkeitsrechts und einer Degradierung über die Anerkennung vermögensrechtlicher Ansprüche warnt; Langhanke, 11 ff.; zur Vermarktung von Persönlichkeitsmerkmalen auch Peukert, in: Leible/Lehmann/Zech (Hrsg.), 95 ff., 110 ff.; Ullmann, AfP 1999, 209 ff.; weiter zum Ganzen Pfeifer, GRUR 2002, 495 ff., 498 mit dem Hinweis, wonach das Persönlichkeitsrecht als Abwehr- und Verfügungsrecht Ähnlichkeiten zum Sacheigentum aufweise.

1876 Hierzu Rhinow, AB 88.032, 13. März 1990, 130.

Logiken im Zusammenhang mit Personendatenverarbeitungsprozessen wurde anhand einer *Stufenordnung* freigelegt.

Ausgehend von einer Betrachtung des CRM unter Einsatz von elektronischen Kundenkarten über den Transfer der Praktiken in das Internet wurde eine eigentliche Datenindustrie beschrieben. Um den Boden für eine Re-Evaluierung datenschutzrechtlicher Vorgaben weiter aufzubereiten, wurde anhand der sukzessiven Verdichtung ökonomischer Begehrlichkeiten und Rationalitäten namentlich über Geschäfts- und Verarbeitungstechniken im Internet die zweite den Realitäten entspringende Hauptherausforderung des Datenschutzes besser verständlich gemacht.[1877] 1413

Hierbei wurde gezeigt, inwiefern die Verdichtung monetärer Begehrlichkeiten zur Verdrängung weiterer, an die einbettenden Kontexte gebundenen Schutzanliegen führt. Die Praxis der Kreditauskunfteien dokumentiert dies besonders eindringlich. Erläutert wurde, wie diese sich – zulasten der Datensubjekte und Kreditnehmenden – durch unrichtige Scores selbst alimentieren. Ihr Vorgehen kollidiert regelmässig mit mehreren der in Kontinentaleuropa datenschutzgesetzlich verbürgten Verarbeitungsgrundsätzen. Nach DSG resultieren hieraus regelmässig Persönlichkeitsverletzungen, deren Widerrechtlichkeit nur selten durch Rechtfertigungsgründe entfallen kann. Eine weitere Perspektive, die sich von der subjektivrechtlichen Betrachtung löst, führte vor Augen, dass die Integrität und das Vertrauen in den Finanz- und Bankensektor sowie das Kreditwesen erodiert werden. Eine derartige systemische Dimension bringt allem voran der US-amerikanische *Fair Credit Reporting Act* unmissverständlich zum Ausdruck. 1414

Daraus folgt, dass die Einräumung einer differenzlosen und universalen Befugnis des Datensubjektes, über seine Personendaten zu disponieren, zu kurz greift. Die Anerkennung einer Rechtsposition, die mit der ökonomischen Ingredienz eines Rechts auf informationelle Selbstbestimmung assoziiert werden kann,[1878] vermag die datenschutzrechtlichen Schutzzwecke und -aufgaben nicht adäquat einzufangen. Im Lichte der dargestellten expansiven Kraft ökonomischer Rationalitäten, in die auch Personendatenverarbeitungen und damit der Datenschutz eingebettet sind, können der Wille des Datensubjektes und seine Entscheidungszuständigkeit, Personendaten auch wirtschaftlich zu nutzen, nicht pauschal als Lösungsansatz anerkannt werden. 1415

Dargestellt wurde, inwiefern wirtschaftliche Rationalitäten im Umgang mit Personendaten unter Umständen die Integrität anderer Gesellschaftsbereiche untergraben. Mit anderen Worten wird wegen des ökonomischen Wertes von Perso- 1416

1877 Vgl. auch die Darstellung verschiedener Bereiche, in denen Personendaten kommerzialisiert werden, bei Weichert, in: Bäumler (Hrsg.), 158 ff., 161 ff., inkl. des Internets, 166 ff.

1878 Vgl. insofern die Forderungen von Buchner, 125 ff.; sodann auch Helfrich, 251 ff.

nendaten und Verarbeitungsprozessen riskiert, die Pluralität gesellschaftlicher Bereiche mit ihren eigenen etablierten Zielen, Zwecken und Rationalitäten zu unterminieren. Der kontinentaleuropäische, in den Entitäten des Subjektes und des Objektes verankerte datenschutzrechtliche Ansatz trägt der Systemrelevanz ungenügend Rechnung.

1417 Die Mehrschichtigkeit der datenschutzrechtlichen Aufgabenstellungen offenbarte sich am Befund, wonach Datensubjekte durchaus regelmässig entscheiden, ob und wie sie allfällige Dienstleistungen, Praktiken und Angebote unter Hingabe ihrer Personendaten nutzen wollen. Sie werden zugleich im Rahmen von AGB oder Privacy-Erklärungen über die geplanten Personendatenverarbeitungen informiert[1879] und erhalten im Rahmen zahlreicher Praktiken eine Gegenleistung für ihre Personendaten, sei es in monetärer Gestalt oder in Gestalt von Dienstleistungen. Gleichwohl bleiben aus Datenschutzperspektive Vorbehalte.

1418 Zwei bereits bekannte datenschutzrechtliche Beiträge vonseiten Rechtsprechung und Lehre bestätigen die im Zusammenhang mit den Kommerzialisierungspraktiken herausgearbeiteten Feststellungen.

1419 Deren erster ist der jüngste datenschutzrechtliche Entscheid des Bundesverwaltungsgerichts aus dem Jahr 2019, der zweite der Rechtsgeschichte schreibende wissenschaftliche Aufsatz von Warren/Brandeis aus dem Jahr 1890. Zwei Beiträge, die eine Zeitspanne von knapp 150 Jahren umklammern und ungeachtet des rasanten technischen Fortschrittes gleichermassen Zeugnis davon geben, wonach die expansive Kraft ökonomischer Rationalitäten zulasten der Integrität anderer Gesellschaftsbereiche seit jeher und bis heute eine Kernherausforderung des Datenschutzes darstellt.

1420 Im *Entscheid des Bundesverwaltungsgerichts i. S. Helsana+* gaben die Nutzenden des App-Programmes ihre Einwilligung in die Verarbeitung von Personendaten, wobei ihnen aufgrund der Erfassung von Personendaten über einen gesundheitsfördernden Lebensstil ein Bonus zukommen sollte.[1880] Das Bundesverwaltungsgericht befand, dass es den Einwilligungen an der Informiertheit sowie der Einhaltung der Formerfordernisse mangelte. Umgekehrt heisst dies: Wäre die Einwilligung gültig gewesen, hätten die (Daten-)Subjekte sowohl willentlich als auch monetär partizipiert.

1421 Bei der Konstellation handelt es sich um einen Prozess der Kommerzialisierung von Personendaten resp. der datenschutzrechtlichen Einwilligung. Das darunterliegende Datenschutzproblem wird subkutan in den Empfehlungen des EDÖB wie auch den Erwägungen des Bundesverwaltungsgerichts reflektiert: Der Verar-

1879 Zu Online-AGB und Transparenzvorgaben im Zusammenhang mit Big Data Weber/Staiger, in: Weber/Thouvenin (Hrsg.), 151 ff., 154 ff.

1880 BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018.

beitungsprozess und die dazu gehörige Praxis stellen bei Lichte betrachtet ein sozialversicherungsrechtliches Grundprinzip auf den Prüfstand, die *Einheitlichkeit der Prämie in der Grundversicherung*.

Ein tragendes Prinzip aus dem Kontext der Grundversicherung soll nicht zwecks Generierung finanzieller Vorteile der individualrechtlichen Dispositionsbefugnis anheimgestellt werden. In besagter Konstellation ist vielmehr die Zulässigkeit eines Prozesses und einer Praxis, welche die individualrechtliche Disposition über Personenangaben eröffnet, in Frage zu stellen. Wenn der Datenschutz, so die These dieser Schrift, nicht nur Subjektschutz, sondern ebenso Systemschutz zu gewährleisten hat und die datenschutzrechtlichen Vorgaben nicht isoliert, sondern integriert resp. akzessorisch zu dem einbettenden Gesellschaftsbereich zu sehen sind, so muss die zu beurteilende Praxis als nicht kompatibel mit Grundprinzipien des Sozialversicherungskontextes gelten. Das Prinzip der Einheitlichkeit der Prämie in der Grundversicherung stabilisiert und gewährleistet eine für jede Person gleichermassen geltende Basisversicherung für den Krankheitsfall, ungeachtet ihrer Lebensführung, familiären Prädisposition usf. Wenn durch den Nachweis besonders gesunder Lebensgestaltung (indirekte) Kostenmodifizierungen in der Grundversicherung erfolgen, wird über den Datenumgang nicht nur ein Kerngedanke des Sozialversicherungsrechts, sondern auch der Bereich der privaten Lebensführung unter Druck gesetzt. 1422

Dem Entscheid lag somit eine Situation individualrechtlich gedachter Kommerzialisierung von Personendaten zugrunde, wobei die akzessorische und systemische Dimension der Herausforderung auch datenschutzrechtlich nicht hinlänglich erfasst wurde. Zwar wurde die Praxis mangels gültiger Einwilligung *de lege lata* als datenschutzrechtswidrig taxiert; dass über diese individualrechtliche Perspektive hinausgehend das sozialversicherungsrechtliche Prinzip der Einheitlichkeit der Prämie – das zumindest in gewissem Umfang auch Garant für eine persönliche Lebensführung, einen abgeschotteten persönlichen Lebensbereich ist – von der expansiven Kraft ökonomischer Antriebe unter Druck gesetzt wird, wurde nicht in letzter Konsequenz anerkannt. 1423

Gegen ein profitgetriebenes Vorgehen zulasten des privaten Lebensbereiches verwehrten sich sodann bereits Warren/Brandeis. In ihrem bahnbrechenden Aufsatz kritisierten sie die nicht autorisierte Publikation von Informationen aus dem persönlichen und familiären Lebensbereich durch die Presse, die ebendies einzig und allein zur Befriedigung eigener wirtschaftlicher Begehrlichkeiten sowie der Neugierde des Pöbels vornahm. Eine solche Publikationspraxis, die unter der Headline der Yellow Press steht, präsentierte sich in einem scharfen Kontrast gegenüber einer Presse, welche die Allgemeinheit mit sachlich berichtenswerten 1424

Informationen versorgt, die gemeinhin auch als Garant für die demokratische Meinungsbildung gesehen werden.[1881]

1425 Gerade ökonomische Rationalitäten, so die Erkenntnis dieses Titels, können schutzwürdige Ziele und damit die Integrität anderer Gesellschaftsbereiche erodieren – ein Befund, der für die Rekonzeptionalisierung des Datenschutzrechts der Zukunft von besonderer Relevanz ist.

C. Resümee

1426 Dieses *VII. Kapitel im dritten Teil befasste sich mit der Effektivität und Effektuierung* resp. der Wirksamkeit des Datenschutzes und des Datenschutzrechts. Nachdem im zweiten Teil dieser Studie die Frage nach der Wirkungs- resp. Funktionsweise des Datenschutzgesetzes der Schweiz durch die Herausarbeitung von drei Strukturmerkmalen beschrieben wurde, ging dieses VII. Kapitel im dritten Teil folgenden Fragen nach: Wie wirksam ist das Datenschutzrecht? Welche Bedeutung wird ihm zugemessen? Welche Ursachen werden für eine ungenügende Wirksamkeit angeführt? Und: Welchen Herausforderungen begegnet ein wirksames Datenschutzrecht?

1427 Analysiert wurde, welche *Bedeutung dem Datenschutz und namentlich dem Datenschutzrecht mit seinem Querschnittserlass, dem DSG,* beigemessen wird. Erforscht wurden gerade auch die *Wirksamkeit, Effektivität und Effektuierung in der Praxis und Realität*. Es ist von einer ungenügenden Einhaltung der Vorgaben des DSG gerade für den privaten Bereich auszugehen. Zudem ist eine nur beschränkte Effektuierung des DSG durch die Rechtsprechung, aber auch Lehre zu attestieren. Kompensierend kommt dem Datenschutz *hohe mediale sowie politische Relevanz* zu. Mit der DSGVO und dem totalrevidierten DSG dürfte sich das Vollzugsdefizit immerhin abschwächen. Weiter wurde *Ursachenforschung* betrieben und gezeigt, dass es keineswegs nur die «Nachlässigkeit des Datensubjektes» ist, die für das Vollzugsdefizit verantwortlich ist. Ebenso wenig sind einzig faktische Entwicklungen hierfür ursächlich. Vielmehr stehen die Regelungsstrukturen mit den datenschutzrechtlichen Ansätzen zumindest teilweise einem wirksamen Datenschutzrecht entgegen. Auch hier dürften neue Ansätze, wie sie die DSGVO und das DSG mit seiner Totalrevision bringen, teilweise Milderung bringen. Vertiefend wurde auf die *beiden wichtigsten faktischen Herausforderungen* eingegangen, die nicht nur in der Allgemeinsprache mit den

1881 Vgl. jüngst der spektakuläre Fall in der Beschattungsaffäre um Konzernleitungsmitglieder der CS Baches/Gallarotti/Beglinger, NZZ vom 17. Dezember 2019, 1 und 23; für den öffentlichen Bereich und den Geheimdienst nur ein Tag zuvor ebenso auf der Titelseite Rhyn, NZZ vom 16. Dezember 2019, 1.

Schlagworten *«rasanter technischer Fortschritt und grenzenlose Personendatenverarbeitungstechnologien»* sowie *«Personendaten sind das Gold des 21. Jahrhunderts»* eingefangen werden. Die *neuen Informationsverarbeitungstechnologien* wurden anhand *dreier Kernkompetenzen* erläutert. Die *Kommerzialisierung von Personendaten* wurde anhand *einer Stufenordnung mit sukzessiver Verdichtung und Ausbreitung ökonomischer Rationalitäten* beschrieben.

Die wichtigsten Erkenntnisse zum ersten Themenfeld, das unter den Titel «Da- 1428
tenschutzrecht auf dem Prüfstand» gestellt wurde, lassen sich im Einzelnen wie folgt zusammenfassen:

Hinsichtlich der *Wirksamkeit des DSG* in seiner noch geltenden Fassung muss 1429
ein *Vollzugsdefizit* attestiert werden, namentlich für den privaten Bereich. Zwar darf davon ausgegangen werden, dass seit dem Jahr 2017 und im Zuge der von der DSGVO angestossenen Entwicklungen zumindest gewisse Verbesserungen mit Blick auf die Datenschutz-Compliance erzielt wurden.[1882] Dies ändert indes noch nichts Prinzipielles an dem Befund, wonach datenschutzgesetzliche Vorgaben gerade auch in der Unternehmenspraxis nur teilweise eingehalten werden. Dokumentiert wurde dies anhand von empirisch angelegten Untersuchungen. Zudem erhellt eine Sichtung der Behördenpraxis, dass Verstösse gegen das DSG nur ausnahmsweise (behördliche) Konsequenzen nach sich ziehen. Dass sich die Verarbeitenden, die vom Anwendungsbereich des DSG erfasst sind, bis dato nur beschränkt in der Pflicht sehen, seine Vorgaben einzuhalten und ihm im Unternehmensalltag faktisch Nachachtung zu verschaffen, wird allem voran mit dem geringen Risiko von Konsequenzen bei Datenschutzverstössen erklärt. Problematisiert wird von den Bearbeitenden die Gesetzgebungstechnik der generalklauselartigen Bearbeitungsgrundsätze, wobei vom generalklauselartigen Regime eine ungenügende Strukturierungswirkung ausgeht. Die eingeräumte «Nonchalance» bei der Einhaltung der datenschutzgesetzlichen Vorgaben wird zudem mit ökonomischen Argumenten sowie der unternehmerischen Notwendigkeit, entsprechende Chancen des technischen Fortschrittes zu nutzen, sowie dem unzumutbaren bürokratischen Aufwand legitimiert resp. entschuldigt. Bereits unter diesem Titel zeichnet sich ab, dass es in erster Linie das ökonomische Interesse ist, welches die Motivation, die Datenschutzvorgaben einzuhalten, konterkariert. Solange mit einschneidenden Konsequenzen nicht ernsthaft zu rechnen ist, kann sich eine solche Strategie durchaus auszahlen. Allerdings zeichnet sich in Anbetracht des von der EU angestossenen datenschutzrechtlichen Bedeutungswandels eine Entwicklung ab: Ungeachtet allfälliger schärferer Sanktionen findet der Da-

1882 Die jüngsten Entwicklungsanstösse werden in diesem dritten Teil im VII. und VIII. Kapitel genauer dargestellt.

tenschutz eine Aufwertung, womit ein erhöhtes Reputationsrisiko aufgrund einer negativen Presse infolge von Datenschutzverstössen einhergeht.[1883]

1430 Ein Gesetzgebungsregime, das in pointierter Weise auf *generalklauselartigen Vorgaben* beruht, ist auf die *konkretisierende und strukturierende Lehre sowie Praxis angewiesen*. In Anbetracht der quantitativen und qualitativen Bedeutung von Personendatenverarbeitungen und der Nichteinhaltung der datenschutzrechtlichen Vorgaben in der Praxis handelt es sich bei den behördlichen und gerichtlich beurteilten Fällen im Anwendungsbereich des eidgenössischen Datenschutzgesetzes gerade für seinen privaten Bereich und den darauf basierenden Empfehlungen sowie Entscheidungen allerdings um Einzelfälle.

1431 Die persönlichkeitsrechtliche und individualrechtliche Anknüpfung des DSG ist konsequenterweise gleichermassen für die Rechtsdurchsetzung vorgesehen, wobei Datensubjekte kaum je den Rechtsweg beschreiten. Die wenigen Urteile, die infolge von *individualrechtlichen Klagen* errungen wurden, laufen im Ergebnis regelmässig auf eine Interessenabwägung für den konkreten Einzelfall hinaus. Folglich konnte die Behördenpraxis nur punktuell strukturierende Wirkungen für das DSG generieren. Der persönlichkeitsrechtliche Ansatz des DSG, der die Rechtsdurchsetzung in erster Linie dem Individuum auferlegt, sowie das generalklauselartige Regime, das einer konkretisierenden Praxis bedarf, verfehlen über weite Strecken ihre Ziele und Aufgaben. Der Einhaltung sowie Durchsetzung des DSG kann damit über das im Vordergrund stehende persönlichkeitsrechtliche Paradigma vonseiten der Gerichtspraxis kaum Nachachtung verliehen werden. Sie hat nur am Rande dazu beigetragen, das Datenschutzgesetz mit seinen Generalklauseln zu effektuieren.

1432 Von grösserer Relevanz sind dagegen Urteile des Bundesverwaltungsgerichts und des Bundesgerichts, die für den *privaten Bereich im Anschluss an Interventionen vonseiten des EDÖB bei sog. Systemfehlern* ergehen. Der Ausdruck «Systemfehler» wird primär «quantitativ» definiert, weil massgeblich auf die Anzahl der Personen abgestellt wird, die von datenschutzgesetzlich problematischen Verarbeitungsprozessen betroffen sind. Der überwiegende Teil der hier anzusiedelnden behördlichen Interventionen befasste sich mit Personendatenbearbeitungen im *Internet*. Gerade in den letzten Jahren ist eine Intensivierung der behördlichen Interventionen festzustellen, wobei der EDÖB seinen Empfehlungen konsequenter Nachachtung verschafft, indem er bei Nichtbeachtung den Gerichtsweg beschrei-

1883 Ein jüngeres Beispiel hierfür ist die CS-Affäre, wobei der Reputationsschaden als gross beurteilt wird, Baches/Gallarotti/Beglinger, NZZ vom 17. Dezember 2019, 1 und 23; insofern unlängst Pfaffinger/Balkanyi-Nordmann, Schweizer Bank Mai 2018, 22 f.; zur Korrelation zwischen Datenschutzvorfällen, Vertrauen und wirtschaftlichem Impact Ponemon Institute LLC/Centrify, Impact on Reputation, insb. 2 ff.; zur Bedeutung des Vertrauens in der digitalen Gesellschaft auch Cavoukian, digma 2009, 20 ff., 20; zu den Mitteilungspflichten infolge von Datenschutzvorfällen gemäss DSGVO Räther, ZHR 2019, 94 ff., 100.

tet. Die alsdann ergangenen Urteile hatten eine gewisse Signalwirkung dergestalt, dass auch in der Schweiz das Datenschutzgesetz nicht ignoriert werden kann. Die Urteile befassen sich vorab mit den allgemeinen Verarbeitungsgrundsätzen sowie der Zulässigkeit von Rechtfertigungsgründen. Zentrale Bedeutung für die Griffigkeit der allgemeinen Verarbeitungsgrundsätze hat eine konsolidierte Auslegung gefunden, wonach eine Verletzung des in Art. 12 Abs. 2 lit. a DSG verbürgten «Minimalstandards» nur mit Zurückhaltung gerechtfertigt werden kann.

1433 Die *Behördenpraxis resp. Rechtsprechung* für den öffentlichen wie privaten Bereich ist gekennzeichnet von einer bemerkenswerten Inkongruenz in Bezug auf die Umschreibung des datenschutzrechtlichen Schutzobjektes sowie der Regelungsmechanik des DSG. Insofern artikuliert sich nichts anderes als die für die allgemeinen Verarbeitungsgrundsätze in Gestalt von Generalklauseln attestierte ausbleibende Konkretisierungsleistung durch die Gerichte. Zugleich lassen die Urteile teilweise eine gewisse argumentative Sorgfalt vermissen, wobei die jüngsten Urteile ein markant erhöhtes argumentatives Niveau aufweisen. Mit Blick auf das Schutzobjekt resp. den Schutzzweck, der gemäss Art. 1 DSG im Schutz der Persönlichkeit und der Grundrechte verortet wird, referieren die Urteile auf unterschiedliche Figuren. Nahezu sämtliche denkbaren Konzepte, die inhaltlich sich präzis zu unterscheiden lohnen, werden angerufen: vom «Missbrauchskonzept» über die Sphärentheorie und vom Schutz der Privatsphäre über das Recht auf informationelle Selbstbestimmung bis hin zu einem Herrschaftsrecht an Personendaten. Damit vermisst man in der rudimentären schweizerischen Praxis zum Datenschutzgesetz über weite Strecken die für ein generalklauselartiges Regime so bedeutsame strukturierende und konkretisierende Effektuierung durch und über die Behördenpraxis.

1434 Aktuell zeichnet sich ab, dass mit der DSGVO, die auch für Schweizer Unternehmen anwendbar sein kann, und der Totalrevision des DSG zu einem Bedeutungswandel im und für den Datenschutz und dessen Recht angesetzt wird. Die rechtlichen Neuerungswellen zielen nicht zuletzt auch auf die Eliminierung der festgestellten *Wirksamkeitsdefizite* bisheriger Normierungen ab. Zugleich sollen angemessene Antworten auf die faktischen, insb. technischen Entwicklungen gefunden werden.

1435 Der nicht erschöpfende Abriss über die schweizerische Datenschutzpraxis hat gezeigt, dass die Durchsetzung von Datenschutzverletzungen im privaten Bereich in der behördlichen Praxis eher marginale Bedeutung erlangt hat, womit umgekehrt die Praxis nur beschränkt einen Beitrag zur Effektuierung des DSG geleistet hat. Immerhin konnte der kursorische Blick sichtbar machen, dass der Datenschutz nicht isoliert anhand des DSG als Querschnittsgesetz realisiert werden kann. Der bereichsspezifische Ansatz wird gerade auch anhand der Rechtsprechung dokumentiert, jüngst anhand des Bundesverwaltungsgerichtsentscheides Helsana+.

1436 Für die *Lehre* ist festzustellen, dass es in erster Linie Kommentar- und Aufsatzliteratur ist, mittels derer das Datenschutzrecht aufbereitet wird. Dagegen sind akademisch-wissenschaftliche Monografien zum Datenschutzrecht bis heute rar. Immerhin findet das Datenschutzgesetz mit seiner Totalrevision akademisch intensiveres Interesse.

1437 Lange bleiben es die *Publikumsmedien, die als die wichtigste Kontrollinstanz* für den Datenschutz figurieren. Dem Datenschutz(-recht) wurde und wird *medial ein zentraler Platz* zugewiesen. Umgekehrt spielen damit die Medien eine bedeutsame Rolle für den Datenschutz. Vor den grossen datenschutzrechtlichen Neuerungen, die eine gewisse Veränderung der Landschaft mit sich bringen, auch was die Effektuierung der Rechtsdurchsetzung anbelangt, bezeichnete Vesting im Jahr 2003 in pointierter wie zutreffender Weise das mediale Rauschen als Hauptwirkung des Datenschutzrechts.[1884] Das Risiko, aufgrund einer Medienberichterstattung über Datenschutzverstösse einen Reputations- und Vertrauensverlust zu erleiden, scheint bis heute für private Unternehmen in der Schweiz gravierender als behördliche Konsequenzen. Erst mit dem Inkrafttreten und dem Ablauf der Umsetzungsfrist der DSGVO zeichnet sich eine Veränderung ab, indem seit 2018 in der EU die behördlich angeordneten Massnahmen und Entscheidungen markant an Relevanz gewonnen haben. Auch die Totalrevision zielt darauf ab, dem DSG faktisch Nachachtung zu verschaffen, wobei der behördliche Massnahmenkatalog ausgebaut wird und die strafrechtlichen Sanktionen verschärft werden.

1438 Die Beiträge in den *Publikumsmedien (re-)präsentieren die Weite und Breite relevanter Datenschutzthemen*. Neben technologie-, innovations- und unternehmensbezogenen Inhalten wird aus juristischer Perspektive die Bedeutung des Datenschutzes für diverse Gesellschaftsbereiche sichtbar. Mit anderen Worten dokumentiert die Medienberichterstattung, dass sich Datenschutzrecht nicht isoliert im Datenschutzgesetz als Querschnittsgesetz erschöpft. Vielmehr wird der verzahnte Rechtsrahmen mit seinen diversen Gesetzen abgebildet, die sich auf verschiedene Sektoren resp. Bereiche beziehen. Zudem äussern sich Autorinnen und Autoren verschiedenster Berufsgattungen zum Datenschutz, wobei die Anwaltschaft regelmässig in den Publikumsmedien zum Thema Datenschutz(-recht) Stellung bezieht. Datenschutzrechtliche Herausforderungen lassen sich unbestritten nur durch eine interdisziplinäre Herangehensweise bewältigen.

1439 Die Intensität und Häufigkeit, mit welcher der Datenschutz medial behandelt wird, ist nicht nur *Indikator für das Vollzugs- und Durchsetzungsdefizit des Rechts und des Rechtsdurchsetzungsapparates, sondern auch für die gesellschaftliche Relevanz des Themas*. In den Medien spiegelt sich die Bedeutsamkeit der Thematik für eine Gesellschaft wider, die sich selbst als Informations- und Kom-

1884 Vesting, in: Ladeur (Hrsg.), 155 ff., 182.

munikationsgesellschaft bezeichnet. Die Eindringlichkeit der Thematisierung des Datenschutzes in den Publikumsmedien erfolgt regelmässig mittels eines beunruhigenden Duktus. Diesen als Angstmacherei abzutun, würde der Sache nicht gerecht. Die Risiken erodierender Auswirkungen von gewissen Personendatenverarbeitungsprozessen auf gesellschaftliche Strukturen und die Robustheit von Institutionen sowie Organisationen wird gerade medial in eindrücklicher Weise vor Augen geführt.

Wie intensiv die Anliegen des Datenschutzes «die Gesellschaft» beschäftigen und 1440
diese sich mit diesen auseinandersetzt, belegen zahlreiche *politische Vorstösse im Bereich des Datenschutzes*. In der Schweiz wurden in den letzten Jahren – unabhängig von der Totalrevision des DSG – mehrere Vorstösse zur Stärkung des Datenschutzrechts eingereicht. Im Einklang mit dem tradierten datenschutzrechtlichen Persönlichkeitsparadigma zielen diese regelmässig auf die Stärkung resp. Klärung des Schutzobjektes resp. der individualrechtlichen Position des Datensubjektes ab.

Nach der Betrachtung der Effektivität und Effektuierung des Datenschutzrechts 1441
– mit ernüchterndem Ergebnis – wurde *«Ursachenforschung»* für die schwache Wirksamkeit datenschutzgesetzlicher Vorgaben betrieben. An erster Stelle werden zwei faktische Disruptoren in die Verantwortung genommen: der rasante technische Fortschritt sowie der Kommerzialisierungstrend.[1885] Bevor eine Auseinandersetzung mit diesen datenschutzrechtlichen Herausforderungen stattfand, wurden weitere Erklärungsmuster freigelegt, die in erster Linie in der Gesetzgebungsstrategie und den ihr zugrunde liegenden paradigmatischen Annahmen wurzeln. Die Ursachen für die ungenügende Wirksamkeit und die faktischen Herausforderungen des Datenschutzrechts präzis zu erfassen, ist eine *conditio sine qua non*, um ein wirksames Datenschutzrecht *de lege ferenda* entwickeln zu können.

Das *Attest der ungenügenden Wirksamkeit des DSG* in seiner noch in Kraft 1442
stehenden Fassung in Realität und Praxis wurde und wird nicht selten der *«Achtlosigkeit» oder dem Desinteresse der Datensubjekte zugeschrieben*. Eine solche Verantwortungszuweisung an das einzelne Subjekt vermag in verschiedener Hinsicht nicht zu überzeugen. Bereits der Stellenwert, welcher dem Datenschutzrecht

1885 Illustrativ hierfür Birnhack, CLSR 2008, 508 ff., 512 ff., dessen Aufsatz einen Titel «Technology and Commerce» setzt; dass es zu kurz greife, einzig die technischen Fortschritte als Wurzel des Übels zu taxieren, zeigt Simitis, in: Schlemmer (Hrsg.), 67 ff., 68 f.; in dieser Arbeit wird denn auch gezeigt werden, dass die Technik untrennbar mit gesellschaftlichen Realitäten und Gegebenheiten sowie Erwartungen verbunden ist und eine Konzeption, welche dies ausblendet und einzig die Technik als Gegenspieler des Menschen resp. der Natur in den Blick nimmt, die datenschutzrechtlichen Herausforderungen nicht zu adressieren vermag; vgl. auch Bull, Computer, 37, wonach es zu kurz greife, datenschutzrechtliche Regeln aus Eigenschaften technischer Systeme abzuleiten, um soziale Beziehungen rechtlich zu gestalten und steuern.

in Medien und Politik wie auch in der Schweiz sowie der europäischen Rechtsentwicklung eingeräumt wird, dokumentiert, wie ernst der Datenschutz im Zeitalter der Digitalisierung genommen wird. Auch empirische Studien stellen fest, dass dem grössten Teil der Menschen der Schutz ihrer Personendaten wichtig ist. Zudem wurde gezeigt, dass die schwache Einhaltung der Datenschutzgesetzgebung resp. das sog. Vollzugsdefizit des DSG – der Befund, wonach dieses in der Praxis kaum eingehalten wird, Datensubjekte kaum je ihre Ansprüche geltend machen, weder die Betroffenenrechte noch die Klagebehelfe, und behördliche Anordnungen, Empfehlungen oder Urteile Raritäten sind – Konsequenz der Gesetzgebungstechnik sowie der datenschutzrechtlichen Realitäten sind.[1886] Die Anknüpfung des DSG an einem defensiv- und individualrechtlich gedachten Persönlichkeitsschutz für die Normierung im privaten Bereich mit seiner prinzipiellen Verarbeitungsfreiheit ist, so muss es aus den bisherigen Ausführungen gefolgert werden, mitursächlich für die ungenügende Wirksamkeit und Griffigkeit datenschutzgesetzlicher (generalklauselartiger) Vorgaben in der (Unternehmens-)Praxis. Die regulatorische Aufmerksamkeit des noch geltenden DSG richtet ihren Fokus weitgehend auf die Verletzungshandlung gegenüber dem einzelnen Individuum, das in der Konsequenz von Gesetzes wegen quasi an erster Stelle für die Durchsetzung der Rechtseinhaltung in die Pflicht genommen resp. für Defizite der Einhaltung verantwortlich gemacht wird. Die Betroffenenrechte sowie die vom DSG für eine individualrechtliche Durchsetzung verbürgten zivilrechtlichen Klagebehelfe werden äusserst selten ergriffen. Darüber hinaus wurde eine limitierte Durchsetzungskompetenz des EDÖB verankert. Obschon in jüngster Zeit eine Intensivierung der Behördenaktivität für den privaten Bereich zu verzeichnen ist, kann diese nicht darüber hinwegtäuschen, dass die *ratio* des DSG im Individual- und Persönlichkeitsschutz liegt. Dieser Ansatz bildet sich datenschutzgesetzlich konsequent in den Instrumenten der Rechtsgewährleistung und -durchsetzung ab. Eine Konzeptionierung, die vom deliktsrechtlichen Persönlichkeitsschutz getragen wird, installiert ein abwehrrechtliches Regelungsregime. Eine primäre und antizipierende Zuständigkeit sowie Verantwortung der Datenverarbeitenden ist damit keine Selbstverständlichkeit.[1887]

1443 Vor diesem Hintergrund mag man sich zu dem Schluss verführt sehen, wonach Datenschutz im Zeitalter der Digitalisierung seine Daseinsberechtigung verloren habe und nicht mehr als einschlägiges und schutzwürdiges Anliegen gelten könne. Umgekehrt fordere diesen nur ein, wer etwas zu verheimlichen resp. zu

1886 Vgl. hierzu grundlegend zweiter Teil, der die Wirkungsweise des DSG anhand dreier Leitprinzipien herausgearbeitet hat.

1887 Ein Perspektivenwechsel vollzieht sich, wie nachfolgend im VIII. Kapitel gezeigt wird, mit den Neuerungen der DSGVO, die punktuell auch in der Totalrevision des DSG übernommen werden sollen; vgl. EJPD, Bericht Begleitgruppe, 1 ff., 3.

verstecken habe; ausverkauft werde er sodann für ein paar Bonuspunkte.[1888] Entsprechende Folgerungen mögen sich im Rahmen eines Datenschutzrechts aufdrängen, dessen individualrechtliches Paradigma nicht verfängt. Allerdings wurde im Zuge dieser Arbeit gezeigt, dass eine solche Einschätzung zu kurz greift. Vorab ist darauf hinzuweisen, dass selbst heute für das Gros der Menschen der Datenschutz ein zentrales Anliegen ist. Das Erklärungsmuster des «unvorsichtigen» oder «vorteilsbedachten» Datensubjektes als Verantwortungsträger für die schwache Datenschutzwirkung bildet die Komplexität seiner Ausgangssituation nicht richtig ab. Diese ist regelmässig eine dilemmatische sowie nicht selten eine aussichtslose, nämlich dann, wenn es um die Sinnhaftigkeit und Verständlichmachung von Datenschutzerklärungen geht: Wer online eine Zeitung lesen will, will eine Zeitung lesen und keine mehrseitige privacy policy studieren; wer online ein Buch erwerben will, will ein Buch erwerben und keine Datenschutzerklärung studieren. Der dem Individuum angelasteten Verantwortlichkeit für den Datenschutz resp. dessen ungenügende Wirksamkeit ist sodann auf einer anderen Ebene entgegenzutreten: Im Zuge dieser Arbeit wurde gezeigt, inwiefern sich der Schutzzweck des Datenschutzrechts nicht im Individualrechtsschutz erschöpft. Entsprechend greift es zu kurz, die (ungenügende) Funktionstüchtigkeit des Datenschutzrechts dem Datensubjekt zuzuschreiben. Wenn der Datenschutz ebenso die Robustheit und Integrität diverser gesellschaftlicher Kontexte und Institutionen mit ihren jeweiligen Zwecken zu garantieren hat, vermag eine alleinige Verantwortungszuweisung an das Datensubjekt nicht zu überzeugen.

1444 Nachdem die Bedeutung und der Stellenwert, die dem Datenschutzrecht und spezifisch dem DSG beigemessen werden, umrissen und erste Erklärungsmuster für den Befund des sog. Vollzugsdefizites beleuchtet wurden, schwenkte der Fokus auf *zwei faktische Hauptherausforderungen,* mit denen das Datenschutzrecht konfrontiert ist. Dies sind erstens der «rasante technische Fortschritt» und zweitens die «Ökonomisierung und Kommerzialisierung von Personendaten». Beides sind Chiffrierungen, die keine hinreichend präzisen Anleitungen für die Gestaltung eines Datenschutzrechts zu generieren vermögen. Entsprechend wurde den beiden Topoi «rasanter technischer Fortschritt» und «Personendaten sind das Gold des 21. Jahrhunderts» nachgegangen, um konkretisierende Erkenntnisse für die Gestaltung eines wirksamen Datenschutzrechts zu generieren.

1445 Zu den *technischen Entwicklungen und Realitäten als erster Hauptherausforderung des Datenschutzrechts:* Die Personendatenverarbeitungstechnologien wurden anhand *dreier Kernkapazitäten* beschrieben. Erstens anhand des *Tracking und Monitoring*, zweitens anhand des *Aggregierens und Analysierens* sowie drittens anhand der *Verteilung (Dissemination) und Abrufbarkeit*. Sämtliche

1888 Vgl. Schaar, 22 ff.; die jüngsten datenschutzrechtlichen Entwicklungen setzen einer solchen Ansicht einen Kontrapunkt entgegen, vgl. vertiefend dritter Teil, VIII. Kapitel, A.

dieser technischen Potenzen entfalten sich sowohl im Online- als auch im Offline-Bereich. Es wurde aufgezeigt, dass eine Verarbeitungsmethode, isoliert vorgenommen, oft weniger problematisch ist als die häufig erfolgenden Kombinationen aller drei Kernkapazitäten. Zudem wurde beschrieben, wie sich der Charakter einer Verarbeitungsmethode durch den Transfer in das Netz regelmässig grundlegend verändert. Die Beschreibung neuer Datenverarbeitungstechnologien anhand dreier Potenzen veranlasste wiederum zu einem Perspektivenwechsel bezüglich der datenschutzrechtlichen Ausgangslage: Anstelle einer Anknüpfung am Datensubjekt sowie an Personendaten als Quasi-Objekten scheint die Ausgangssituation von *Datenflüssen in netzwerkartigen Strukturen mit Knotenpunkten die Ausgangslage, derer sich der Datenschutzgesetzgeber anzunehmen hat,* adäquat abzubilden. Nachgezeichnet wurde hieran anknüpfend, inwiefern namentlich der Übertritt von Datenflüssen von einem gesellschaftlichen Kontext in einen anderen Kontext, aber auch von der Offline-Welt in die Online-Welt der besonderen Aufmerksamkeit aus Datenschutzperspektive bedarf. Die neuen Technologien (sowie hierauf basierende und fortentwickelte Geschäfts- und Verwaltungspraktiken) ermöglichen die Generierung tiefer, breiter und hoch mobiler, massiver Datenbestände, die Personenangaben aus verschiedensten Quellen und Kontexten «poolen». Hieran schliessen diverse Analysen an, aus denen Folgerungen gezogen und auf Basis derer entsprechende Massnahmen ergriffen werden, wobei gewonnene Informationen – wiederum divers verteilt – abgerufen und genutzt werden. Diese Zusammenführung, Auswertung und Überleitung von Personendaten aus und zwischen diversen und facettenreichen Quellen und Kontexten – vom Facebook-Profil bis zum LinkedIn-Profil, von öffentlichen Registern bis zu Telefonbüchern, vom Bereich der persönlichen Beziehungspflege in den wirtschaftlichen Kontext und alsdann in den politischen Bereich, vom Offline-Bereich in den Online-Bereich – zeigt sich aus Datenschutzperspektive als kritisch und herausfordernd.[1889] Eine Herausforderung, welche über das individual- und persönlichkeitsrechtliche Paradigma nicht angemessen bewältigt werden kann. Stattdessen bedarf es der Integration systemischer Schutzerwägungen.

1446 Anknüpfend an die Beschreibung der Kernkapazitäten der neuen Datenverarbeitungstechnologien und die Formulierung der hieraus für das Datenschutzrecht resultierenden Herausforderungen folgte eine Auseinandersetzung mit dem Trend der *wirtschaftlichen Bedeutung von Personendaten*. Die Analyse folgte einer *Stu-*

1889 Illustrativ mit Blick auf den Kontext der Freundschaft und die Veränderung, wenn die Beziehungspflege von der analogen Welt in die Online-Welt verlagert wird, aus der Perspektive des Privatheitsschutzes Rössler, Eurozine vom 27. Februar 2015; der Beitrag von Fried, Yale L.J. 1968, 475 ff. lässt sich dergestalt lesen, dass er spezifisch auf den Kontext der Freundschaft sowie Liebesbeziehungen eingeht und die besondere resp. spezifische Bedeutung von privacy resp. Informationsaustausch resp. Geheimhaltung herausarbeitet; zu den ausdifferenzierten Graden von Intimität und Distanz in Relationen auch verschiedener Kontexte Mallmann, 45 f.

fenordnung, aufgrund derer die expansive Kraft kommerzieller Logiken und ihre Verdichtung namentlich im Internet herausgearbeitet wurde. Hierbei zeigte sich, inwiefern die kombinierende Nutzung der Kernpotenzen neuer Technologien in Verbindung mit spezifischen Geschäfts- und Vertragspraktiken nicht nur individualrechtliche Fragen der Kommerzialisierung aufwirft. Vielmehr ist die expansive und verdrängende Tendenz ökonomischer Rationalitäten zulasten von Zielen und Logiken anderer Gesellschaftsbereiche zu verzeichnen. In der juristischen Auseinandersetzung wird der sich in den Alltagsrealitäten vollziehende Trend zur Transformation von Personendaten in Güter in Einklang mit der Anknüpfung des aktuellen DSG im Persönlichkeitsrecht mit seinen Wurzeln in Art. 28 ZGB unter dem Titel der Kommerzialisierung der Persönlichkeit resp. der Selbstbestimmung von Personendaten abgehandelt. Die vorliegende Schrift verzichtet bewusst auf eine Auseinandersetzung mit dem Dogma der ideellen Natur des Persönlichkeitsrechts und den rechtswissenschaftlichen Analysen und verfolgte stattdessen das Ziel, die Diskussion im Kontext des Datenschutzes auf dahinterliegende, weiter angelegte Dimensionen hinzuführen. Das Phänomen, das unter Topoi wie «Personendaten sind Gold wert» oder «Kommerzialisierung von Personendaten» beschrieben wird, ist facettenreich, wobei mehrere Aspekte benannt wurden, die für eine Rekonzeptionalisierung des Datenschutzrechts relevant sind: Bezogen auf eine individualrechtliche Konzeption ist vorab zu befinden, dass selbst dann, wenn Datensubjekte entscheiden können, ihre Personendaten zur Verfügung zu stellen und eine eigentliche Gegenleistung dafür erhalten – folglich eine Inklusion in «wirtschaftlicher» und «demokratischer» Hinsicht erfolgt –, damit die datenschutzrechtlichen Herausforderungen, Chancen und Probleme nicht erschöpfend gelöst werden. Gezeigt wurde darüber hinaus, inwiefern Personendatenverarbeitungen gerade auch im Rahmen des CRM wirtschaftliche Vorteile sowohl aufseiten der Datensubjekte als auch aufseiten der Datenverarbeitenden generieren können. Zudem lässt sich für mehrere Einsatzbereiche von Personendatenverarbeitungsprozessen beschreiben, dass diese auch, aber keineswegs isoliert nur pekuniäre Bedeutung haben, sondern dass durch Personendatenverarbeitungsprozesse mit den diesen zugrunde liegenden Geschäftspraktiken unter Einsatz neuer Technologien zugleich übergeordnete oder weitere Ziele und Zwecke von einbettenden gesellschaftlichen Bereichen effektuiert werden können: Verringerung von Lebensmittelverschwendung und Staus, effizientere Aufdeckung von Straftaten usf. Der Fokus schwenkte alsdann auf die Kommerzialisierungspraktiken von Personendaten im Online-Bereich. Dargestellt wurde, dass die Praxis der sog. Customization eine im Vergleich zum CRM im Offline-Bereich neue Dimension eröffnet. Technische Limiten des Cookies-Einsatzes werden durch dichte Netze von Vertrags- und Geschäftsbeziehungen überwunden, womit in der Folge das Surf-Verhalten der Individuen im Internet namentlich zur Bewerbung umfassend getrackt wird. Solche Prozesse sind für die einzelne Person kaum verständ-

lich oder nachvollziehbar. Zudem werden nicht nur Personendaten zu Interessen im Konsumkontext ermittelt, sondern auch Daten über den Besuch von Homepages mit Informationen zu Gesundheit, Politik sowie von sozialen Plattformen werden erhoben. Generiert wird folglich keineswegs bloss ein «umfassendes Kundenprofil», sondern ein umfassendes «Interessenprofil». Dieses detaillierte Monitoring und Tracking erfolgt dabei nicht zur Terrorbekämpfung, sondern in erster Linie zur individualisierten, interessenbasierten Bewerbung. Daher wurde hinsichtlich der entsprechenden Praktiken von der *expansiven Kraft wirtschaftlicher Rationalitäten im Internet* gesprochen. Es erscheint fast so, als ob der Online-Bereich als ein einziger, grosser Marktplatz wahrgenommen würde, wobei das Internet primär von einem Geschäftsmodell der Werbung geprägt ist. Allerdings: Auch das Internet ist ein hochdifferenzierter «Raum», in dem sich (ähnlich wie in der Offline-Welt) diverse gesellschaftliche Bereiche abbilden:[1890] der Bereich der familiären und freundschaftlichen Beziehungspflege, der Gesundheitsbereich, der politische Bereich usf.[1891] Obschon Personendatenverarbeitungen durch ihren Transfer vom Offline-Bereich in den Online-Bereich in ihrer Topografie wesentliche Veränderungen erfahren, ist auch der Online-Bereich kein eigenständiger und von der Offline-Welt losgelöster Bereich; vielmehr replizieren sich ebenda etablierte gesellschaftliche Strukturen. Gleichwohl akzentuiert sich die *expansive Tendenz des ökonomischen Kontextes im Zusammenhang mit Personendatenverarbeitungen im Internet*. Den eigentlichen Kulminationspunkt bildet die Datenindustrie mit ihren Geschäftsmodellen. Auch hier zeigten sich – vergleichbar mit den Werbenetzwerken – dicht verwobene Geschäfts- und Vertragsnetzwerke, innerhalb derer Personendaten nahezu unbeschränkt verarbeitet und genutzt werden. Die sog. Auskunfteien stehen seit jeher gerade aus datenschutzrechtlicher Perspektive in der Kritik. Mit Blick auf das Kreditauskunftswesen, das nicht zuletzt aufgrund seiner Intransparenz problematisiert wird, wurde insb. bemängelt, dass beliebige Informationen mit ungenügender «Konnexität» zur Beurteilung der «Kreditwürdigkeit» herangezogen werden. Ein spezifisches Problemfeld der Kreditauskünfte ist somit unter der datenschutzrechtlichen Anforderung der Richtigkeit abzuhandeln, wozu auch gehört, dass der Score-Wert akkurat ist. Allerdings gilt die Fehlerquote statistisch erwiesen als hoch. Eine Konsequenz dessen ist, dass Konsumierenden erhebliche finanzielle Mehrbelastungen aufgebürdet werden, beispielsweise hinsichtlich des Zinsfusses bei der Kreditvergabe. Damit alimentieren sich sowohl die auskunftserteilenden als auch die kre-

1890 Vgl. ebenso m. w. H. Schachtner/Duller, 61 ff., 68 ff.; vgl. auch Weichert, in: Bäumler (Hrsg.), 158 ff., 167, wonach bei Nutzung des Internets nicht nur kommerzielle Zwecke verfolgt werden; vgl. zum Internet insb. im Zusammenhang mit der Telekommunikation und der Netzneutralität Eberle, in: Mehde/Ramsauer/Seckelmann (Hrsg.), 979 ff.

1891 Aufschlussreich bezüglich des hier entwickelten Konzepts zum Kontext der Freundschaft, wobei Differenzen bestehen zwischen den in der analogen Welt gepflegten und den online via sozialen Plattformen wie Facebook, Rössler, Eurozine vom 27. Februar 2015.

diterteilenden Institutionen zulasten der Datensubjekte resp. Kreditnehmenden unter Vorschützung «statistisch-mathematischer» und (pseudo-)wissenschaftlicher Verfahren. Dass solchen Praktiken nicht nur eine *individualrechtliche* Problematik, sondern ebenso eine *systemische Dimension* inhärent ist, bringt das US-amerikanische Recht unmissverständlich mit seinem *Fair Credit Reporting Act* zum Ausdruck: Es seien das Banksystem und der Finanzsektor selbst, die vom fairen und akkuraten Credit Reporting abhängen, da unfaire Credit Reports die Effizienz des Bankensektors konterkarieren und das Vertrauen der Allgemeinheit in diesen erodieren. Folglich schützen bereichsspezifische Datenschutzvorgaben auch, aber nicht nur das Individuum. Im Zentrum steht die *Gewährleistung des Schutzes der Integrität spezifischer Gesellschaftsbereiche*, woran das Datenschutzrecht angekoppelt ist. Damit wurde die *akzessorische Natur datenschutzrechtlicher Vorgaben und ihre Konnexität zu den Logiken, Zielen, Zwecken und Normen der jeweils einbettenden Kontexte* weiter bestätigt.

Abrundend lässt sich befinden, dass annektierende Tendenzen des ökonomischen 1447
Sektors gegenüber weiteren gesellschaftlichen Kontexten mit ihren jeweiligen Zielen, Zwecken und Logiken namentlich datenschutzrechtlich zu adressieren sind. Ein solcher Befund hat Relevanz für die Beurteilung der Angemessenheit und Funktionstüchtigkeit der neuerdings implementierten sowie diskutierten jüngsten Ansätze, die zur Bewältigung datenschutzrechtlicher Vorgaben vorgestellt werden.

VIII. Kapitel: Aktuelle Lösungsstrategien

> «Policymakers will continue down the rabbit hole of defining personally identifiable information and informed consent. Social scientists and designers will continue to worry about refining notice and choice. In the meantime, miners of big data are making end runs around informed consent and anonymity. A lesson may be drawn from biomedicine where informed consent and anonymity function against a rich ethical backdrop. They are important but not the only protective mechanisms in play. Patients and research subjects poised to sign consent forms know there are limits to what may be asked of them. Treatment or research protocols that lie outside the norm or involve a higher than normal risk must have passed the tests of justice and beneficence. In other words, clinicians and researchers must already have proven to their expert peers and institutional review boards that the protocols being administered or studied are of such great potential value to the individual subject or to society that the reasonable risks are worthwhile. Consent forms have undergone ethical scrutiny and come at the end of a process in which the values at stake have been thoroughly debated. The individual's signature is not the sole gatekeeper of welfare.»[1892]

1448 Die folgende Analyse umreisst die bedeutsamsten der unlängst entwickelten Lösungsansätze, mit denen auf die Datenschutzherausforderungen reagiert wird. Sie werden zugleich auf ihre Stärken und Schwächen hin reflektiert werden. Die Darstellung bereitet den Boden weiter, um im IX. Kapitel einen Perspektivenwechsel und abgeleitet einen eigenen Lösungsansatz zur Rekonfiguration des Datenschutzrechts vorzustellen.

1449 Dass es bislang nicht gelungen ist, dem Schutzobjekt, das unter dem Dachbegriff des Privaten abgehandelt wird, eine konzise Kontur und einen fixierten Inhalt zu verleihen, gilt als Kernproblem des Datenschutzrechts und seiner Wirksamkeit.[1893] Umgekehrt klingt das Echo aus dem ersten Teil dieser Schrift unter dem Titel «Vergangene Zukunft», der sich mit historischen und literarischen Texten befasste, nach: «Und die Welt hebt an zu singen / triffst Du nur das Zauberwort»[1894] – eine Metapher, die trefflich eine bis heute verfolgte Hauptstrategie zur Überwindung datenschutzrechtlicher Defizite und namentlich des Vollzugsdefizites einfängt: Es geht darum, den «Code des Privaten» zu knacken. An eine Auseinandersetzung mit datenschutzrechtlichen Lösungsansätzen mag nun an erster Stelle die Erwartung gerichtet sein, dass diese eine griffige und zeitgemässe Definition des Schutzobjektes – des «Privaten» – vorlegt. Damit würde zugleich

1892 Barocas/Nissenbaum, Communications of the ACM 2014, 31 ff., 33.
1893 Nissenbaum, 1 ff.; HRC, Special Rapporteur Right to Privacy 2016, N 9; vgl. EJPD, Erläuternder Bericht, 1 ff., 16; Schiedermair, 23; Amelung, 9 ff.
1894 Von Eichendorff, Wünschelrute, 1835: «Schläft ein Lied in allen Dingen / Die da träumen fort und fort / Und die Welt hebt an zu singen / Triffst du nur das Zauberwort».

eine vertiefte Beschäftigung mit Schriften berühmter Persönlichkeiten, die sich mit dem «Privaten» befassen, naheliegen.[1895]

Die anschliessenden Ausführungen konzentrieren sich auf die *aktuell formulierten Lösungsansätze*. Sie wurden nicht zuletzt mit dem Ziel entwickelt, das faktische Vollzugsdefizit zu beseitigen, aber auch, den neuen technologischen Möglichkeiten sowie dem Trend zur Kommerzialisierung Rechnung zu tragen. 1450

Unter A. werden die *jüngsten datenschutzrechtlichen Neuerungswellen* dargestellt. Hier werden die Neuerungen, wie sie mit der DSGVO, aber auch der Totalrevision des DSG installiert werden, beschrieben. Es geht darum, die grossen Entwicklungslinien freizulegen, womit eine parallele Vorgehensweise zum zweiten Teil dieser Arbeit gewählt wird. Herausgeschält werden die dem Datenschutzrecht in Europa ein komplexeres Gesicht verleihenden Akzente, die neue Strukturmerkmale in das Datenschutzrecht einführen. Damit wird sich zeigen, inwiefern *die im zweiten Teil dieser Arbeit benannten drei Strukturmerkmale ergänzt oder neu ausgerichtet werden*. Für eine erschöpfende Exegese und Analyse *en détail* der jeweiligen einzelnen Bestimmungen der DSGVO sei auf die mittlerweile solide Kommentarliteratur hingewiesen. Auch in Bezug auf die Totalrevision des DSG existiert bereits ein erster Bestand an Analysen. 1451

Unter B. folgt eine *Betrachtung der Reaktionen und Vorschläge*, die vonseiten der *Lehre (und Rechtsprechung)* zwecks Bewältigung der datenschutzrechtlichen Herausforderungen vorgeschlagen werden. An dieser Stelle wird erst eine Rückblende vorgenommen, zumal die Herausforderungen der Technologisierung sowie Kommerzialisierung im Zusammenhang mit Personendaten für das Recht keineswegs neu sind. Eine rechtshistorische Betrachtung zeigt, dass Antworten in erster Linie in einer Auseinandersetzung mit den *subjektiven Rechten* gesucht wurden.[1896] Der Ansatz ist noch heute wirkungsmächtig. Die besagte subjektivrechtliche Tradition und eine Prämisse, wonach das Recht die Emanzipation des Menschen gegenüber seiner technischen Annektierung zu gewährleisten hat, lassen sich nicht nur anhand der datenschutzrechtlichen, sondern auch der biomedizinrechtlichen Debatte nachweisen.[1897] 1452

Deshalb wird ebenso ein Blick auf die Entwicklungen im Bereich des *Biomedizinrechts* und insb. die dort gewählten datenschutzrechtlichen Lösungsstrategien geworfen. Alsdann wird dem *Recht am eigenen Bild* spezifische Aufmerksam- 1453

1895 Vgl. m. w. H. zu den Theorien und Thematisierungen des Privaten Rössler, 11 ff., mit Hinweisen insb. auf Habermas, Arendt, Elias, Dworkin und dann insb. den liberal-demokratischen Rahmen mit Locke, Mill und Rawls.

1896 Vgl. Gareis, Zeitschrift für Gesetzgebung und Praxis auf dem Gebiete des deutschen öffentlichen Rechtes 1877, 137 ff.; Warren/Brandeis, Harv. L. Rev. 1890, 193 ff.

1897 «Der Mensch steht höher als Technik und Maschine», illustrativ der Titel des Beitrages von Pfeil, InTeR 2020, 82 ff.

keit gewidmet, das als stabilisiertes Datenschutzsonderrecht bezeichnet werden kann. In ihm lassen sich Parallelen zu den im ersten Teil dieser Arbeit aus (rechts-)historischer Perspektive eingeführten Geheimhaltungspflichten nachweisen, wobei beide Rechtskonstruktionen – das Recht am eigenen Bild sowie der Geheimnisschutz – nur ungenügend als Teil des Datenschutzrechts betrachtet werden. Nachdem anhand des Rechts am eigenen Bild faktische wie rechtliche Entwicklungslinien freigelegt werden und der vergleichende Blick zu «gewöhnlichen» personenbezogenen Angaben und deren rechtlichen Erfassung eine Verifizierung des im zweiten Teil beschriebenen Systems ermöglicht, wendet sich die Arbeit den wissenschaftlichen Theorieansätzen zu, die in jüngster Vergangenheit für die Zukunft des Datenschutzrechts präsentiert werden. Im Lichte der oft bloss schematisch umrissenen Herausforderungen des Datenschutzes werden namentlich die Gewährleistung eines Rechts auf informationelle Selbstbestimmung sowie die Anerkennung eines (geistigen) Eigentumsrechts an Daten vorgeschlagen sowie der Versuch einer «erfolgreichen» Definierung des Privaten unternommen.

A. Die legislativen Neuerungswellen in Europa

«Mit der DSGVO wird das europäische Datenschutzrecht in eine neue Ära eintreten.»[1898]

1. Tour d'Horizon

1454 Europa setzt legislativ in den ersten beiden Dezennien des 21. Jahrhunderts einen Akzent auf das Datenschutzrecht. Die Materie gewinnt die für eine Informations- und Kommunikationsgesellschaft, die sich der Chancen wie der Risiken der Digitalisierung bewusst geworden ist, angemessene Aufmerksamkeit und Bedeutsamkeit.[1899]

1455 Einschlägig sind namentlich die folgenden Erlasse und Rechtsetzungsprojekte: Zunächst ist auf die Änderung der Datenschutzkonvention des Europarates hinzuweisen. Der Bundesrat hatte basierend auf seinem Entscheid vom 30. Oktober 2019 in der Sitzung am 6. Dezember 2019 die Botschaft über die Genehmigung des Protokolls zur Änderung der Datenschutzkonvention verabschiedet. Richtungsweisend ist sodann die europäische Datenschutz-Grundverordnung (DSGVO), die im Mai 2016 in Kraft trat und deren Umsetzungsfrist im Mai 2018 ablief. Sie bringt, wie zu zeigen ist, signifikante Entwicklungsanstösse und

1898 So zutreffend Passadelis/Roth, Jusletter 4. April 2016, N 3.

1899 Vgl. in diesem Zusammenhang die Beiträge in: Gschwend/Hettich/Müller-Chen/Schindler/Wildhaber (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Dike Verlag Zürich/St. Gallen 2015.

Veränderungen für und im Datenschutzrecht mit sich. Kein Erfolg beschieden war dagegen der E-Privacy-Verordnung der EU für den Datenschutz in der elektronischen Kommunikation: Nach mehr als drei Jahren wurden die Verhandlungen, wie im Dezember 2019 berichtet wurde, abgebrochen.[1900] Die DSGVO gab, im Verbund mit den evaluierten Schwächen des DSG und dem rasanten technischen Fortschritt, einen Impuls für die Totalrevision des eidgenössischen DSG.[1901] In Anbetracht der Globalisierung und «Grenzenlosigkeit» von Personendatenverarbeitungsprozessen sind resultierende Harmonisierungsbemühungen ebenso sachlogisch motiviert.[1902] Die mit der Totalrevision des DSG angestrebte Kompatibilisierung mit den Entwicklungen in der EU ist namentlich auch mit Blick auf den sog. Angemessenheitsbeschluss von hoher Relevanz: Vonseiten der EU wird basierend auf Art. 45 Abs. 2 DSGVO eine Prüfung des eidgenössischen Datenschutzniveaus vorgenommen. Mit der Totalrevision des DSG soll die Schweiz das Attest der Angemessenheit resp. Gleichwertigkeit gegenüber dem Recht der EU erlangen können.[1903] Damit geht es nicht nur um das Datenschutzrecht, vielmehr geht es zugleich um die Wirtschafts- und Handelsbeziehungen zwischen der Schweiz und der EU. Ein harmonisiertes Datenschutzrecht schützt diese Beziehungen. Die Auseinandersetzung mit der DSGVO führt vor Augen, wie stark die Verordnung über den persönlichkeitsrechtlichen Subjektschutz hinaus zugleich auf den Schutz von Handelsbeziehungen sowie z. B. wissenschaftlichen Fortschritt ausgerichtet ist. Die DSGVO ist zudem aufgrund ihrer «extraterritorialen Wirkung» ggf. ebenso für Unternehmen in der Schweiz einschlägig.[1904]

In Bezug auf die Totalrevision des DSG wurde im Januar 2018 entschieden, den parlamentarischen Verabschiedungsprozess zu etappieren: Die Schengen-relevanten Aspekte sollten vorgezogen behandelt werden.[1905] Dagegen wurden die Beratungen zur Totalrevision des DSG wiederholt vertagt.[1906] Am 16. August 2019 1456

1900 Krempl, Heise online vom 3. Dezember 2019, E-Privacy: EU-Staaten lassen Verordnung scheitern, Kommission will Neustart, <https://www.heise.de/newsticker/meldung/E-Privacy-EU-Staaten-lassen-Verordnung-scheitern-Kommission-will-Neustart-4603164.html> (zuletzt besucht am 30. April 2021).

1901 Botschaft DSG 2017–1084, 17.059, 6941 ff.; zu den gesetzgeberischen Etappen und Entwicklungen vgl. die Dokumente abrufbar unter: <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html> (zuletzt besucht am 20. September 2021) sowie die verschiedenen Beiträge vonseiten der Datenschutzexpertinnen und -experten.

1902 Zur Forderung eines globalen Datenschutzes Schaar, 232 ff.

1903 Hierzu auch EuGH, C-362/14, Urteil vom 6. Oktober 2015 – Schrems, E 105: «[…] verlangt wird, dass das Drittland […] tatsächlich ein Schutzniveau gewährleistet, das dem in der Union aufgrund der Richtlinie 95/46 im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist».

1904 Vgl. Art. 3 DSGVO und zur extraterritorialen Wirkung nachfolgend 2.1.

1905 EDÖB, Etappierung der DSG-Revision: Grundrechtsschutz muss gewahrt bleiben, Bern 2018, <https://www.edoeb.admin.ch/edoeb/de/home/aktuell/aktuell_news/kommission-des-nationalrats-beschliesst-etappierung-der-dsg-revi.html> (zuletzt besucht am 30. April 2021).

1906 Am 16. August 2019 schloss die Staatspolitische Kommission des Nationalrates die Vorberatungen ab, womit das Geschäft in der Herbstsession 2019 in das Parlament gelangen soll; <https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-08-16-a.aspx> (zuletzt besucht am 30. April 2021).

verhandelte die staatspolitische Kommission des Nationalrates die Totalrevision; der Nationalrat beriet die Vorlage für das neue Datenschutzgesetz in der Herbstsession, womit diese im Dezember 2019 in der staatspolitischen Kommission des Ständerates und am 18. Dezember 2019 im Ständerat beraten wurde.[1907]

1457 Bundesrätin Keller-Sutter führte im Rahmen der Beratungen in der zweiten Kammer aus, dass einige Beschlüsse des Nationalrates den Standards der EU nicht genügen und teilweise einen Rückschritt gegenüber dem aktuell geltenden Datenschutzgesetz bringen würden (namentlich für das Profiling). Daher empfahl die staatspolitische Kommission des Ständerats dem Ständerat Anpassungen. Im Kern der Totalrevision stünden gerade mit dem Ziel des Angemessenheitsbeschlusses durch die EU die erhöhte Transparenz, der Ausbau der Betroffenenrechte, die verstärkte Eigenverantwortung der Verarbeitenden sowie des Ansatzes der Selbstregulierung, die Stärkung der Stellung des EDÖB sowie die Verschärfung der Strafbestimmungen.[1908] Die Totalrevision will gerade auch über den Ausbau der Instrumente des Subjektschutzes auf die neuen technologischen Fortschritte reagieren. Umgekehrt soll die Freiheit des Personendatenverkehrs optimal verwirklicht werden.[1909] Verabschiedet wurde die Totalrevision nach der Differenzbereinigung am 25. September 2020. Das Inkrafttreten ist für 2023 angesetzt. Vergleichbar zur DSGVO ist mit einer *Umsetzungsfrist* zu rechnen.

1458 Nachfolgend werden die neuen Akzente, wie sie von der DSGVO, aber auch der Totalrevision des DSG gesetzt werden, in das Zentrum der Aufmerksamkeit gerückt. Umrissen werden die grossen Entwicklungslinien. Auf eine detaillierte dogmatische Exegese wird an dieser Stelle verzichtet. Der Beschrieb der grossen Entwicklungslinien für die beiden Erlasse wird sichtbar machen, dass beträchtliche Unterschiede verbleiben, die im Ergebnis zu einer entsprechenden Differenz im Schutzniveau führen. Zugleich wird sich zeigen, inwiefern neue Lösungsstrategien und Ansätze vorgesehen werden, ohne dass datenschutzrechtlich für Kontinentaleuropa Etabliertes – beispielsweise die allgemeinen Verarbeitungsgrundsätze oder das Instrument der Betroffenenrechte – aufgegeben wird. Die datenschutzrechtlichen Neuerungswellen bringen *beachtliche Änderungen unter Bewahrung etablierter und bewährter Konzepte und Ansätze*.

1907 Das Schweizer Parlament, Medienmitteilung, Lobbyistinnen und Lobbyisten im Parlamentsgebäude: Keine neuen Regelungen, Bern 2019, <https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-05-24.aspx> (zuletzt besucht am 30. April 2021).

1908 Vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff.; zur Verstärkung der Transparenz im neuen DSG vgl. Baeriswyl, digma 2020, 6 ff.; Ders., auch kritisch zum Ausbau der Betroffenenrechte, digma 2019, 156 ff., einleitend als Übersicht zu den verschiedenen spezifischen Beiträgen; zur Stärkung der Betroffenenrechte qua DSGVO Giesinger, Jusletter vom 20. Januar 2020, N 1; zu den neuen Strafbestimmungen Rosenthal/Gubler, SZW 2021, 52 ff.

1909 Zur Freiheit des Datenverkehrs, der ebenso durch die DSGVO gewährleistet werden soll, Weber, Jusletter IT vom 24. September 2015, N 1.

Zwecks Anhebung und Verschärfung des Datenschutzes und seines Rechts kommen mehrere und verschiedene Mechanismen, Instrumente, Ansätze und Stossrichtungen zum Einsatz. Parallel zum Vorgehen im zweiten Teil werden *Strukturmerkmale*, die teilweise etablierte Instrumente stärken, teilweise datenschutzrechtliche «Noven» einfügen, herausgearbeitet. Anhand dieser *Beschreibung von Strukturmerkmalen* soll nachvollziehbar gemacht werden, weshalb mit den datenschutzrechtlichen Neuerungen, die mit der DSGVO und der Totalrevision des DSG einhergehen, von einem «Paradigmenwechsel» gesprochen wird.[1910] 1459

Wenige Vorbemerkungen zu den *Zielen*, die innerhalb der Entwicklungstrends angesprochen werden: Nach Art. 1 Abs. 2 DSGVO soll die Verordnung den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insb. deren Recht auf Schutz personenbezogener Daten sowie den freien Verkehr personenbezogener Daten, vgl. Art. 1 Abs. 3 DSGVO, gewährleisten. Neben den Schutz des Individuums tritt damit in der DSGVO offensichtlich ebenso das Ziel, einen freien, aber gleichwohl von vereinheitlichten Regeln sowie gemeinsamen Regeln unterworfenen Datenverkehr zu bewerkstelligen.[1911] Die Prämisse ist, dass ein gemeinsamer Markt gemeinsame Spielregeln bedingt. Im Lichte der «Grenzenlosigkeit» von Personendatenflüssen behindert eine primär nationalstaatlich erlassene Datenschutzgesetzgebung nicht nur die Datenflüsse, sondern zugleich die Marktbeziehungen. Weniger deutlich wird dieser Aspekt im totalrevidierten DSG, vgl. Art. 1 nDSG. Über das Instrument des erwähnten Angemessenheitsbeschlusses bewerkstelligt die EU über die DSGVO gleichwohl, dass Länder, die Handel mit EU-Staaten betreiben, sich an angemessene Datenschutzvorgaben halten. 1460

2. Entwicklungstrends der legislativen Neuerungen

2.1. Zum Ansatz des langen Arms

Die Erkenntnis, dass Datenströme an Landesgrenzen keinen Halt machen, ist gemeinhin bekannt.[1912] Auch das Recht greift diese Entwicklungen auf. 1461

Lediglich erwähnt, obschon in der Praxis von hoher Relevanz, ist der Ausbau der Vorgaben im 3. Abschnitt des totalrevidierten DSG zur Bekanntgabe von Personendaten ins Ausland. Die Verletzung der in Art. 16 Abs. 1 und Abs. 2 nDSG formulierten Pflichten werden strafrechtlich mit Busse bewehrt, vgl. Art. 61 lit. a nDSG. 1462

1910 Pfaffinger, A paradigm shift in data protection, Deloitte Academy, GDPR and the way forward, Vortrag vom 31. Januar 2019, Deloitte Zürich.
1911 Hierzu z. B. Weber, Jusletter IT vom 24. September 2015, N 1.
1912 Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.1.

1463 Die Ausführungen zu den im Zusammenhang mit grenzüberschreitenden Personendatenverarbeitungen einschlägigen Bestimmungen müssen fragmentarisch bleiben. Der Fokus liegt auf einem langen Arm insb. der DSGVO, aber auch des DSG. Es geht damit um eine *extraterritoriale Anwendbarkeit*.

1464 Aus einer Praxisperspektive sehen sich Unternehmen, die global agieren, bei der Implementierung von weltumspannenden Initiativen vor beträchtliche Koordinationsaufgaben gestellt. Eine Umsetzung im Einklang mit den einzelnen jeweils anwendbaren Rechtsordnungen ist oft nicht praktikabel. Die Identifizierung des anwendbaren Rechts resp. der anwendbaren Rechte stellt eine Vorprüfungsaufgabe dar. Insofern lässt sich mit Rechtskreisen arbeiten. In der Folge empfiehlt sich eine Orientierung an den Rechtsordnungen mit strengem Niveau und hohem Sanktionsniveau. Regelmässig wird eine an Risikoerwägungen ausgerichtete datenschutzrechtliche Lösung entwickelt, die verschiedenen Regelungsvorgaben bestmöglich Achtung verschafft.

1465 Im Zusammenhang mit internationalen Datenverarbeitungen sind in der Schweiz nach Totalrevision insb. Art. 16 nDSG ff. relevant. Die Verletzung gewisser Vorgaben kann nach Art. 61 lit. a nDSG strafrechtlich sanktioniert werden. Im Zusammenhang mit Personendatenverarbeitungen durch private Verantwortliche mit Sitz resp. Wohnsitz im Ausland ist sodann Art. 14 f. nDSG zu erwähnen. Eine Pflicht, einen Vertreter zu bestellen, lehnt sich an eine ähnliche Vorgabe in der DSGVO an, vgl. Art. 27 DSGVO. Von besonderem Interesse ist der räumliche Anwendungsbereich des DSG. Neu wird dieser in Art. 3 nDSG geregelt. Nach Art. 3 Abs. 2 nDSG gelten weiterhin die Bestimmungen gemäss IPRG. Aktuell sind insb. Art. 129 Abs. 1 IPRG und Art. 139 IPRG einschlägig.

1466 In der Schweiz löste der lange Arm aus dem europäischen (Rechts-)Raum, wie ihn die DSGVO brachte, Widerstand aus. Allerdings zeigt der Blick auf das Schweizer Recht, dass die Schweiz in Bezug auf die Anwendbarkeit «ihres» Datenschutzrechts ebenso wenig Halt an der Schweizer Grenze macht. Vielmehr sieht die Eidgenossenschaft mit ihren Normen im IPRG keineswegs eine zurückhaltende Anwendbarkeit des schweizerischen Datenschutzrechts im internationalen Kontext vor.[1913]

1467 Jüngst zeichnet sich sodann ab, dass Kalifornien dem europäischen Exempel folgen will, wobei der *California Consumer Privacy Act* als das schärfste Datenschutzgesetz gilt. Vom Gesetz erfasst werden – in Anlehnung an das Konzept der DSGVO – nicht nur Unternehmen mit Sitz resp. physischer Präsenz in Kalifornien; vielmehr genügt es, wenn sich die Klientel resp. Kundschaft in Kalifornien

1913 Grundlegend hierzu Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6.

(im Zeitungsbericht gilt als Anknüpfungskriterium, wonach Kalifornier zu den Kunden gehören) befindet.[1914]

Für schweizerische Unternehmen stellt die extraterritoriale Wirkung der DSGVO bis heute eine Herausforderung dar.[1915] Ihnen werden entsprechend ebenso einige Ausführungen gewidmet.[1916] Unternehmen in der Schweiz, die im EU-Raum geschäftliche Aktivitäten entfalten, hatten eine *Basisanalyse* zur Anwendbarkeit der DSGVO durchzuführen.[1917] 1468

Das *räumliche Element* ist eines von insgesamt vier Tatbestandselementen, die den Anwendungsbereich der DSGVO festlegen.[1918] Neben dem *zeitlichen Anwendungsbereich* – die Umsetzungsfrist der DSGVO lief am 25. Mai 2018 ab – sind der *sachliche sowie persönliche Anwendungsbereich* in Art. 1, Art. 2 und Art. 4 DSGVO geregelt:[1919] Die DSGVO erfasst die Verarbeitung von Personendaten *natürlicher* Personen, wobei als personenbezogen alle Angaben gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[1920] Geschützt sind gemäss DSGVO lediglich natürliche Personen; es findet keine Anwendung auf die Verarbeitung von Personendaten juristischer Personen statt.[1921] Der Verarbeitungsbegriff wird weit definiert und meint nahezu jeden, namentlich automatisierten Umgang mit personenbezogenen Angaben: erheben, organisieren, speichern, auswerten, weiterleiten usf.[1922] In persönlicher Hinsicht kann es sich aufseiten der Verarbeitenden um natürliche wie juristische Personen handeln, die alleine oder gemeinsam oder im Auftrag Personendaten verarbeiten. Die Rollen der 1469

1914 Vgl. Langer, NZZ vom 30. Dezember 2019, 4.

1915 Dokumentiert ist dieser Befund auch bei Ebert/Widmer, 11 f. und 19.

1916 Die nachfolgenden Ausführungen zur *extraterritorialen Wirkung der DSGVO* beruhen auf einem Vortrag gehalten an der Bankrechtstagung 2019 und dem im Anschluss daran publizierten Aufsatz im Tagungsband, vgl. Pfaffinger, in: Emmenegger (Hrsg.), 17 ff.

1917 Mit einer dokumentierten Analyse trägt man zugleich dem Accountability-Ansatz der DSGVO Rechnung; hierzu auch Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22; zur Accountability Cichocki, Jusletter IT vom 21. Mai 2015, N 49 ff.

1918 Insofern bereits Passadelis/Roth, Jusletter 4. April 2016, N 6 ff.; anhand jener Kriterien wird sich in vergleichbarer Weise der Anwendungsbereich des DSG nach seiner Totalrevision bestimmen lassen. Es wird vergleichbar zur DSGVO ebenso mit einer Übergangsfrist nach dem Inkrafttreten des totalrevidierten DSG gerechnet.

1919 Für Begrifflichkeiten nach Art. 4 DSGVO sei auf die einschlägige Kommentarliteratur verwiesen; zum Anwendungsbereich der DSGVO sodann Vasella, digma 2017, 220 ff.; zum persönlichen und sachlichen Anwendungsbereich sodann Art. 2 nDSG, zum räumlichen Anwendungsbereich Art. 3 nDSG.

1920 Art. 4 Nr. 1 DSGVO; vgl. Art. 5 lit. a nDSG.

1921 Diesem Konzept folgt ebenso die Totalrevision DSG. Nach Art. 1 nDSG schützt das Gesetz nur noch natürliche Personen.

1922 Art. 4 Nr. 2 DSGVO; hierzu Herbst, BeckKomm-DSGVO, Art. 4 N 1 ff.; vgl. auch Art. 5 lit. d und lit. e nDSG, wo die Verarbeitungshandlung ebenso breit definiert wird.

Verarbeitenden spielen eine Hauptrolle gemäss DSGVO.[1923] Der *räumliche Anwendungsbereich* wird in Art. 3 DSGVO fixiert.[1924]

1470 Das DSG wird mit seiner Totalrevision dieselben vier Kriterien vorsehen, vgl. Art. 2 nDSG zum persönlichen und sachlichen Anwendungsbereich sowie Art. 3 nDSG zum räumlichen Anwendungsbereich. Mit einer Umsetzungsfrist nach dem Inkrafttreten des DSG wird ebenso gerechnet.

1471 Die extraterritoriale Wirkung der DSGVO und damit ihr «langer Arm» wird anhand zweier *Hauptkonstellationen* umgesetzt: *Erstens* gilt das *Niederlassungskriterium* nach Art. 3 Abs. 1 DSGVO und *zweitens* das *Targetingkriterium* nach Art. 3 Abs. 2 DSGVO, das seinerseits zwei Unterfälle umfasst: in lit. a den Angebotstatbestand, in lit. b den Monitoringtatbestand.[1925]

1472 Zum räumlichen Anwendungsbereich publizierte der Europäische Datenschutzausschuss (European Data Protection Board, EDPB) Ende 2018 ein Konsultationspapier.[1926] Ebenda wird vom «Triggern» des Scopes der DSGVO gesprochen.[1927] Eine konstante Praxis und Lehre wird sich im Laufe der kommenden Jahre auch in Bezug auf den räumlichen Anwendungsbereich erst konsolidieren müssen. Gleichwohl gibt das Konsultationspapier Hinweise, womit sich mit diesem hinsichtlich der Auslegung der DSGVO Tendenzen und Linien abzeichnen. Der Europäische Datenschutzausschuss intendiert, mit dem Dokument Impulse für die Entwicklung einer vereinheitlichenden Interpretation hinsichtlich des räumlichen Anwendungsbereiches der DSGVO zu liefern. Das Ziel ist eine Harmonisierung.[1928]

1473 Im Zusammenhang mit der Anwendbarkeit der DSGVO und den insofern verfolgten Harmonisierungsbestrebungen ist auf die sog. Öffnungsklauseln hinzuweisen, vgl. z. B. für den Arbeitskontext Art. 88 DSGVO.[1929] Während die DSGVO einen (hohen) «Minimalstandard» bezüglich datenschutzrechtlicher Vorgaben verankert, ermöglichen es die sog. Öffnungsklauseln («opening clauses») den EU-Mitgliedstaaten, jeweils innerstaatliche Gesetze zu erlassen, die ein höheres Niveau vorsehen. Die Öffnungsklauseln der DSGVO sind in der Praxis eine

1923 EDPB, Consultation Paper Scope, 3 ff.; vertiefend sodann CNIL, Guide sous-traitant, *passim*; WP 29, Concept of controller and processor, *passim*; BLD, FAQ Auftragsverarbeitung, 1 ff.; vgl. Hartung, BeckKomm-DSGVO, Art. 4 Nr. 7 und Nr. 8 sowie Art. 28; beachte auch Art. 5 lit. j und lit. k nDSG, wobei mit der Totalrevision an die Differenzierung dieser Rollen verschiedene Pflichten geknüpft werden.

1924 Zum räumlichen Anwendungsbereich des totalrevidierten DSG vgl. Art. 3 nDSG, dessen Abs. 2 auf das IPRG verweist.

1925 Auf die Erörterung von Art. 3 Abs. 3 DSGVO wird verzichtet.

1926 Auf der Homepage des EDPB finden sich umfassende Dokumente sowie Informationen <https://edpb.europa.eu/edpb_en> (zuletzt besucht am 3. Juli 2021).

1927 Vgl. EDPB, Consultation Paper Scope, 6, 8 f., 13 ff., 17 f., 21.

1928 EDPB, a. a. O., 3.

1929 Auch zu diesem Bereich finden sich auf der Homepage des EDPB verschiedene Dokumente aufbereitet.

Herausforderung. Sie durchbrechen die mit der DSGVO beabsichtigte Harmonisierung markant. Über die DSGVO können damit ebenso nationale Gesetze der EU-Mitgliedstaaten zu beachten sein. Für Schweizer Unternehmen, die in den Anwendungsbereich der DSGVO fallen, bedeutet dies, dass ein jeweils angesprochenes nationales Datenschutzrecht einschlägig sein kann.

1474 Zur (extra-)territorialen Anwendbarkeit der DSGVO: Nach EDPB kommt dem *Wortlaut der Verordnung* hohe Bedeutung zu. Es ist mit einer engen Anlehnung an den Verordnungstext zu rechnen.[1930] Sodann lässt sich aufgrund der Erwägungen des Papiers vermuten, dass der *räumliche Anwendungsbereich weit, nicht aber exzessiv interpretiert* werden wird.[1931] Betreffend den systematischen Aspekt auch der Rechtsinterpretation ist zudem zu erwarten, dass die Auslegung der Vorgaben der DSGVO autonom, nicht aber beziehungslos resp. bezugsblind im Verhältnis zu angrenzenden Rechtsgebieten erfolgen wird.[1932] Wie ein roter Faden zieht sich die Forderung durch das Dokument, im Rahmen der zu tätigenden Assessments *sämtliche konkreten Umstände des Einzelfalls in die Erwägungen zu integrieren*.[1933] Einzig eine Gesamtsicht, die alle und gerade die *faktischen Gegebenheiten in die Analyse* einbezieht, ist geeignet, um Tatbestandselemente – i. c. diejenigen zum Anwendungsbereich (aber auch zu Rollen der Agierenden und daraus resultierenden Pflichten) – adäquat zu evaluieren.

1475 Diese Interpretation lässt sich als Entwicklungstrend der zeitgenössischen Datenschutzrechtsneuerungen beschreiben. Sie ist richtungsweisend: Eine bislang in erster Linie *formelle Herangehensweise* soll überwunden werden. Insofern wird an einem neuralgischen Punkt des bisherigen Datenschutzrechts angesetzt. Lange wies das Datenschutzrecht in der Realität beträchtliche Wirkungsschwächen auf.[1934] Der im Rahmen des räumlichen Anwendungsbereiches präsentierte Auslegungshinweis, *wonach sämtliche Umstände des konkreten Einzelfalles mit seinen faktischen Gegebenheiten* einschlägig sind, leistet einen Beitrag auf dem Weg zur *faktischen Verwirklichung des Datenschutzrechts*.

1476 Für die räumliche und damit auch extraterritoriale Anwendbarkeit der DSGVO sind sodann *zwei zusammenhängende Aspekte von strukturierender Relevanz*.[1935] *Erstens* wird zwischen *direkter und indirekter* Anwendbarkeit der DSGVO unterschieden. *Zweitens* hat eine Analyse zum Anwendungsbereich die *Rollen* der Ak-

1930 Beachte allerdings zum Angebotstatbestand den Hinweis auf die «manifested intention» EDPB, Consultation Paper Scope, 15.
1931 Vgl. EDPB, a. a. O., 5 f.
1932 Illustrativ EDPB, a. a. O., 15.
1933 EDPB, a. a. O., 3, 5 f., 8, 12, 16; ein entsprechender Hinweis findet sich auch in der einschlägigen Kommentarliteratur.
1934 Vertiefend zum Vollzugsdefizit im Sinne eines Einhaltungs- wie auch Durchsetzungsdefizites des DSG in der Schweiz dritter Teil, VII. Kapitel, A.
1935 Unter dem Titel «Koordinaten- und Navigationssystem» beschrieben von Pfaffinger, in: Emmenegger (Hrsg.), 18 ff., 21.

teure im Rahmen der Personendatenverarbeitungsprozesse in die Erwägungen einzubeziehen.[1936] Relevant ist, inwiefern als alleiniger Controller, als Co-Controller oder Processor verarbeitet wird. Je nachdem, in welcher Rolle der Verarbeitende agiert und aufgrund welchen Tatbestandes die DSGVO anwendbar ist, variieren die Rechtsfolgen: Es sind Differenzierungen mit Blick auf die resultierenden Pflichten zu beachten. Art. 4 Nr. 7 resp. Nr. 8, Art. 26 und Art. 28 DSGVO äussern sich punktuell zu den Rollen alleiniger Verantwortlicher (Controller), gemeinsamer Verantwortlicher (Co-Controller) oder Auftragsverarbeiter (Processor).[1937] Bedeutsam ist, dass Auftragsverarbeiter weiterreichend in die Pflicht genommen werden.[1938]

1477 Ob die Voraussetzungen für die Anwendbarkeit der DSGVO erfüllt sind, kann nur anhand der Kenntnis der Verarbeitungslandschaft resp. -prozesse beurteilt werden. Insofern ist ein neues datenschutzrechtliches Instrumentarium einschlägig, das sog. Verarbeitungsverzeichnis, Art. 30 DSGVO.[1939]

1478 In Bezug auf Art. 3 DSGVO empfiehlt sich eine *Stufenprüfung*. Wird der Anwendungsbereich nicht aufgrund von Art. 3 Abs. 1 DSGVO getriggert, kann die DSGVO gleichwohl aufgrund von Art. 3 Abs. 2 lit. a resp. lit. b DSGVO einschlägig sein.

1479 An erster Stelle figuriert das *Niederlassungskriterium* als Anknüpfungselement des räumlichen Anwendungsbereichs der DSGVO, Art. 3 Abs. 1 DSGVO.[1940] Sein *erstes Tatbestandselement ist die Niederlassung in der EU*. Ihr Vorliegen soll nicht anhand eines formellen Kriteriums geprüft werden.[1941] Entscheidungsrelevant sind vielmehr effektive Aktivitäten durch eine Einrichtung mit einer gewis-

1936 EDPB, Consultation Paper Scope, 4 f., 9 ff.

1937 Vgl. WP 29, Concept of controller and processor, *passim*; die nachfolgenden Ausführungen basieren zudem auf der einschlägigen Kommentarliteratur, z. B. Ingold, NomosKomm-DSGVO, Art. 26 ff.; zu diesen Rollen, spezifisch mit Blick auf den Bankbereich, vgl. Rosenthal/Epprecht, in: Emmenegger (Hrsg.), 127 ff.

1938 Die Anknüpfung datenschutzrechtlicher Pflichten und Verantwortlichkeiten anhand der Rollen wird auch mit der Totalrevision des DSG vorgesehen, vgl. nur zu den Definitionen Art. 5 j und k nDSG.

1939 Vgl. EDPB, Consultation Paper Scope, 10; gemäss Art. 3 DSGVO kann die DSGVO direkt anwendbar sein auch für Non-EU-Gesellschaften, sei es in der Rolle des Verantwortlichen (Controller) oder derjenigen des Auftragsverarbeiters (Processor). Mangels direkter Anwendbarkeit gestützt auf Art. 3 DSGVO ist weiter die indirekte Anwendbarkeit basierend auf Vertrag denkbar, vgl. Art. 28 Abs. 3 DSGVO; auch die Totalrevision führt die Pflicht zur Erstellung eines entsprechenden Verzeichnisses ein, vgl. Art. 12 nDSG.

1940 Der deutsche Wortlaut: «Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet»; derselbe Text in der englischen Version: «This regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.»

1941 EDPB, Consultation Paper Scope, 5.

sen Beständigkeit in der EU («arrangement»).[1942] Die Anforderungen insofern gelten als niedrig. Nicht erforderlich ist eine Tochtergesellschaft oder Zweigniederlassung.[1943] *Zweitens* hat die *Personendatenverarbeitung* im *Zusammenhang mit den Aktivitäten der Niederlassung* zu erfolgen.[1944] Diese Voraussetzung ist erfüllt, sofern die Verarbeitungshandlungen in einem untrennbaren Konnex zu den effektiven und tatsächlichen geschäftlichen Aktivitäten der Niederlassung in der EU stehen. Das Paper spricht insofern vom «inextricable link». Ob dieser Konnex zwischen geschäftlicher Aktivität und Personendatenverarbeitung besteht, sei weder zu restriktiv noch zu exzessiv anzunehmen. Geboten ist eine Analyse *in concreto*. Sie integriert sämtliche einschlägigen Elemente in die Erwägungen.[1945] Die Personendatenverarbeitung muss nicht von der Niederlassung selbst durchgeführt werden, womit das dritte Tatbestandselement und die Rechtsfolge angesprochen sind: Ungeachtet dessen, ob die beschriebene Personendatenverarbeitung inner- oder ausserhalb der EU durchgeführt wird, ist die DSGVO auf die beleuchteten Personendatenverarbeitungsprozesse anwendbar.[1946]

Eine Präzisierung findet sich in Bezug auf den Tatbestand hinsichtlich des Einsatzes eines (dritten, fremden) Auftragsverarbeiters als sog. Service Provider. Der Einsatz eines Auftragsverarbeiters als Service Provider triggert den Anwendungsbereich gemäss Art. 3 Abs. 1 DSGVO nicht. Mit anderen Worten wird damit keine Niederlassung begründet.[1947] 1480

Wird die Anwendbarkeit der DSGVO nach Art. 3 Abs. 1 DSGVO verworfen, kann diese gleichwohl gegeben sein.[1948] Zu prüfen ist in einer nächsten Etappe, ob die extraterritoriale Wirkung aufgrund des sog. *Targetingkriteriums gemäss Art. 3 Abs. 2 DSGVO* zu bejahen ist. 1481

Der *erste Untertatbestand gemäss Art. 3 Abs. 2 lit. a DSGVO* wird Angebotstatbestand resp. Marktortprinzip genannt.[1949] Sein Negativkriterium ist zunächst, 1482

1942 Ennöckl, NomosKomm-DSGVO, Art. 3 N 6 f.; weiter Klar, BeckKomm-DSGVO, Art. 3 N 40 ff.; EDPB, Consultation Paper Scope, 5.

1943 EDPB, Consultation Paper Scope, 5.

1944 Zum Kriterium vgl. Klar, BeckKomm-DSGVO, Art. 3 N 54 ff.; EDPB, Consultation Paper Scope, 6 ff.; vertiefend aufgeführt werden im Consultation Paper Personendatenverarbeitungen, die im Zusammenhang mit einem revenue raising stehen, vgl. EDPB, Consultation Paper Scope, 7 f.; mit Blick auf das Kriterium des inextricable link wird namentlich auch auf den Google-Spain-Entscheid hingewiesen, vgl. Google Spain SL, Google Inc. V AEPD, Mario Costeja González (C-131/12).

1945 EDPB, Consultation Paper Scope, 6.

1946 Für Beispiele vgl. Pfaffinger, in: Emmenegger (Hrsg.), 17 ff., 27, 30 f.

1947 EDPB, Consultation Paper Scope, 10 f.; hierzu Vasella, digma 2017, 220 ff., 221.

1948 Hierzu sowie zur Beschreibung des Abs. 2 mit dem Überbegriff des Targeting Criterion, vgl. EDPB, Consultation Paper Scope, 12.

1949 «Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist.» Auf Englisch: «This regulation applies to the processing of personal data of data subjects who are in the Union by

dass der Verantwortliche (resp. Auftragsverarbeiter) *keine Niederlassung in der EU* i. S. v. Art. 3 Abs. 1 DSGVO hat. Das Positivkriterium ist, dass *Personendatenverarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an Personen in der EU* erfolgen. Nicht relevant ist damit die Art der Gegenleistung (Währung) oder die Staatsangehörigkeit der Personen, an die sich das Angebot richtet. Einschlägig ist, ob sich das Angebot an Personen in der EU richtet. Das betroffene Datensubjekt befindet sich in der EU. Präzisierend und zugleich einer weiten Auslegung zugeführt wird der Tatbestand durch den Europäischen Datenschutzausschuss, wenn dieser vertritt, dass die manifestierte Absicht, Waren oder Dienstleistungen an Personen in der EU anzubieten («manifested intention to offer goods or services»), ein hinreichendes Kriterium sei. Auch insofern sind sämtliche Umstände des Einzelfalles und damit das Gesamtbild relevant.[1950] Zur Evaluation des Tatbestandes bedarf es damit einer Analyse der effektiven Organisation sowie der Produkt- und Vertriebsstruktur. Im Konsultationspapier werden Indizien für eine klare Angebotsabsicht aufgeführt – so die Sprache der Internetseite –, Angaben von Lieferkosten für den Versand in die EU, ein Lieferangebot in EU-Länder usf.[1951]

1483 Der *zweite Untertatbestand des Targetingkriteriums ist der sog. Monitoringtatbestand, Art. 3 Abs. 2 lit. b DSGVO*.[1952] Der Verantwortliche resp. Auftragsverarbeiter hat auch für diesen Tatbestand *erstens keine Niederlassung* in der EU, beobachtet indes – *zweitens – das Verhalten einer Person in der EU*, wobei eine *Personendatenverarbeitung im Zusammenhang mit dieser Verhaltensbeobachtung steht*.[1953] Präzisierend und hier einschränkend wird im Konsultationspapier des EU-Datenschutzausschusses darauf hingewiesen, dass es gewisser Auswertungsaktivitäten bedarf, damit der Tatbestand erfüllt wird.[1954]

---

a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union.»

1950 Zum Kriterium des offensichtlichen Beabsichtigens und der Notwendigkeit einer Gesamtschau Klar, BeckKomm-DSGVO, Art. 3, N 80 ff.; EDPB, Consultation Paper Scope, 14 f. m. w. H.; Ennöckl, NomosKomm-DSGVO, Art. 3 N 13 f.

1951 EDPB, Consultation Paper Scope, 15 f.

1952 «Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.» In der englischen Fassung: «This regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: […] (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.»

1953 Zum Tatbestand EDPB, Consultation Paper Scope, 17 f.

1954 Hierin lässt sich eine «Verengung» des Anwendungsbereiches der DSGVO sehen, vgl. EDPB, Consultation Paper Scope, 18; im Zusammenhang mit diesem Beispiel ist en passant auf die E-Privacy-Verordnung, auch Cookies-Verordnung genannt, hinzuweisen. Sie steht noch nicht in Kraft, wird allerdings als *lex specialis* zur DSGVO zu beachten sein; <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32009L0136> (zuletzt besucht am 30. April 2021).

Ist der Anwendungsbereich der DSGVO gegeben – was aufgrund der extraterritorialen Wirkung auch für Unternehmen in der Schweiz relevant sein kann –, ist hinsichtlich der einzuhaltenden Vorgaben zu differenzieren. Einschlägig ist die *Rolle*, in welcher Personendatenverarbeitungen erfolgen. Mit Blick auf die zahlreichen, weit- und tiefgreifenden, differenzierten und durchaus auch in der Umsetzung komplexen Pflichten sei auf die einschlägige (Kommentar-)Literatur verwiesen, soweit diese nicht im Rahmen der Darstellung der Strukturcharakteristika der DSGVO nachfolgend adressiert werden.[1955] 1484

Die Analyse der Tatbestandselemente zum räumlichen Anwendungsbereich mit der extraterritorialen Wirkung hat sichtbar gemacht, dass mit dem Regulierungsansatz der «Grenzenlosigkeit» von Personendatenverarbeitungsprozessen Rechnung getragen wird. 1485

Zugleich bringt die Gestaltung der extraterritorialen Wirkung der DSGVO eine beachtliche Neuanknüpfung: Einschlägige Kriterien sind *Geschäfts- sowie Handelsbeziehungen sowie -aktivitäten*, die sich in den EU-Markt richten und in deren Zusammenhang Personendaten verarbeitet werden. Wer Handels- und Geschäftsbeziehungen mit Akteuren im EU-Raum unterhält, hat die Vorgaben der DSGVO zu beachten, sofern damit zusammenhängend Personendatenverarbeitungen durchgeführt werden. 1486

Mit der Ankoppelung datenschutzrechtlicher Vorgaben an geschäftliche Aktivitäten, wie es anhand des Anwendungsbereiches der DSGVO beschrieben wurde, verändert sich zumindest punktuell ein Charakteristikum bisheriger datenschutzrechtlicher Anknüpfung: Seine bislang dominante zivil- und persönlichkeitsrechtliche Natur wird mindestens ergänzt. Das Datenschutzrecht wird konzeptionell näher an das Wirtschafts- und Handelsrecht herangerückt.[1956] Indem sich die Tatbestandselemente zum räumlichen Anwendungsbereich gemäss Art. 3 DSGVO an Handels- und Wirtschaftsaktivitäten orientieren, wird durchaus auch dem Bewusstsein um den ökonomischen Wert personenbezogener Daten Rechnung getragen. 1487

Die DSGVO installiert damit ein Konzept, wonach sich die Vorgaben und Erwartungen hinsichtlich eines *integren Geschäftsgebarens* ebenso auf den rechtmässigen Umgang mit Personendaten beziehen. Dieser Aspekt, der sich anhand des Anwendungsbereichs der DSGVO beschreiben lässt, wird anhand weiterer Elemente verdichtet. Dazu gehört die Ausrichtung des Datenschutzrechts als Com- 1488

1955 Einen guten Überblick liefern Passadelis/Roth, Jusletter vom 4. April 2016; Rosenthal/Vasella, digma 2018, 166 ff.; Baeriswyl, SZW 2021, 8 ff.; sodann die Beiträge von Rosenthal.

1956 In eine solche Richtung die Worte des kalifornischen Justizministers Becerra: «Unsere persönlichen Daten füttern die heutige datengetriebene Wirtschaft und den Wohlstand, den sie schafft. Es ist an der Zeit, dass wir die Kontrolle über unsere Daten haben – und auch entscheiden können, was privat ist», vgl. hierzu den Artikel von Sander, NZZ vom 30. Dezember 2019, 4.

pliance- und Governance-Aufgabe. Die DSGVO bereitet den Weg in eine Richtung, welche der Datenschutz-Compliance (eines Tages) ähnliche Bedeutung einräumt, wie dies für die Geldwäscherei oder die Kartellrechts-Compliance gilt.[1957] Diese Ausführungen zum Anwendungsbereich der DSGVO leiten harmonisch zur vertieften Auseinandersetzung mit der Diversifizierung datenschutzrechtlicher Schutzerwägungen über.

2.2. Zum Ansatz diversifizierter Schutzziele und -zwecke

1489 Dem Schutzzweck kommt für das Datenschutzrecht auch konzeptionell herausragende Bedeutung zu. Vertiefend gezeigt wurde dies namentlich im zweiten Teil dieser Arbeit im Rahmen der Analyse der generalklauselartigen Verarbeitungsgrundsätze, des Grundsatzes der Zweckbindung und einer Analyse des berühmten Volkszählungsurteils des Bundesverfassungsgerichts hierzu. Einige Schlaglichter zum Thema des datenschutzrechtlichen Schutzzweckes sind auch unter dem Titel der datenschutzrechtlichen Neuerungen in Europa angezeigt.[1958]

1490 Die Totalrevision des DSG übernimmt mit Art. 1 nDSG – abgesehen von der Beschränkung auf natürliche Personen – unverändert seinen bisherigen Zweckartikel. Das DSG bezweckt den Schutz der Grundrechte sowie der Persönlichkeit der von Personendatenverarbeitungen betroffenen Personen. Eine vertiefte Debatte über das Schutzobjekt oder den Schutzzweck datenschutzgesetzlicher Normierungen wurde im Zuge der Ausarbeitung des totalrevidierten DSG nicht geführt. Dass das DSG die Grundrechte sowie die Persönlichkeit des betroffenen Datensubjektes zu schützen hat, wurde kaum je zur Debatte gestellt. Explizit sind es nur dieser Schutzzweck und dieses Schutzobjekt, die in Art. 1 (n)DSG verbürgt werden. Im Zuge dieser Studie wurde aber unübersehbar, dass sich weitere Schutzaspekte – wie ein roter Faden und eher subkutan – ebenso durch die Datenschutznormierung ziehen.

1491 Dies erstaunt, zumal schon früh kritische Stimmen zur Verengung des Datenschutzrechts auf den Schutz der Persönlichkeit ertönten.[1959] Veranschaulichend die Worte von Fiedler zu den relevanten Zielsetzungen des Datenschutzes aus dem Jahr 1974:

> «Mag auch eine bestimmte Zielsetzung in den Vordergrund gestellt werden, so kann es doch beim Datenschutz nicht um eine einzige Zielsetzung alleine gehen.»[1960]

1492 Die DSGVO verzichtet auf eine Verwendung des Terminus des «Privaten» resp. der «Privacy» und dessen Verwendung im Schutzzweckartikel. Dasselbe ist für

1957 Vgl. Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 23.
1958 Grundlegend Lynskey, *passim*; zum Schutzgegenstand des Datenschutzes auch Bijok, 36 ff.
1959 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 und N 26.
1960 Fiedler, in: Podlech/Steinmüller (Hrsg.), 179 ff., 185.

das DSG und seine Totalrevision zu attestieren. Gleichwohl wird bis dato im Schrifttum in diesem Schirmbegriff die datenschutzrechtliche Basiskategorie und in der präzisen Fixierung seines Inhaltes die *conditio sine qua non* für ein wirksames Datenschutzrecht verortet.

Für den Schutz des Privaten erscheint es so, als ob jedermann und jedefrau wisse, was damit gemeint ist, und gleichwohl niemand weiss, was sein Inhalt ist. Ruft man sich den engen Konnex der Kategorie des Privaten mit derjenigen der Familie in Erinnerung, stellt sich die Frage, ob sich hier parallele Entwicklungen andeuten: Das Konzept einer fixen und monochromen Natur der Familie resp. des Privaten wird aufgeweicht durch Pluralisierungstendenzen. Nachfolgend wird skizziert, inwiefern sich in den datenschutzrechtlichen Neuerungen eine *Diversifizierung anerkannter Schutzdimensionen* den Weg bahnt.[1961] 1493

Insofern lässt sich eine Brücke zwischen den Erwägungen zum räumlichen Anwendungsbereich der DSGVO mit ihren Harmonisierungsbestrebungen zu den Argumenten betreffend die Bedeutung des Datenschutzrechts für den *wirtschaftlichen Fortschritt und den (digitalen) Markt* schlagen. Gemäss Erwägungsgrund 5 habe «die wirtschaftliche und soziale Integration als Folge eines funktionierenden Binnenmarkts zu einem deutlichen Anstieg des grenzüberschreitenden Verkehrs personenbezogener Daten geführt». Erwägungsgrund 7 statuiert, dass die Entwicklungen einen «soliden, kohärenten und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union (erfordern), da es von grosser Wichtigkeit ist, eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können». Ein gleichmässiges und hohes Datenschutzniveau, so Erwägungsgrund 10, beseitige Hemmnisse für den Verkehr personenbezogener Daten in der Union, woraus zugleich auf eine Beseitigung von Handelshemmnissen geschlossen wird.[1962] Demnach hängt wirtschaftliche Effizienz – entgegen der Vorstellung, wonach der Datenschutz ökonomische Zielerreichung erschwert – von einem griffigen Datenschutzrecht ab. Eine solche Argumentationslinie wurde in diesem dritten Teil, der sich unter anderem mit den ökonomischen Expansionstendenzen im Kontext von Personendatenverarbeitungen befasste, freigelegt.[1963] Ein wirksames Datenschutzrecht gilt – so wird es von der DSGVO deutlich gemacht – als relevant für den Schutz 1494

1961 Eigenständige Studien hierzu wären von grossem Interesse.

1962 Gerade für den Fall, dass Unternehmen in der Schweiz von Art. 3 Abs. 2 DSGVO erfasst werden, wird die Aufgabe, datenschutzrechtlich «compliant» zu sein, ein bedeutsames Element für den Marktanschluss von Schweizer Unternehmen an den EU-Markt bilden. Entsprechende wirtschaftliche Anreize effektuieren den Datenschutz und stellen damit eine wichtige Ergänzung zu allfälligen behördlichen Massnahmen und Sanktionen dar; zur Bedeutung des Datenschutzrechts auch als handfester wirtschaftlicher Erfolgsfaktor sowie zu seiner Bedeutung für den E-Commerce bereits früh Reding, digma 2001, 124 ff.

1963 Hierzu dritter Teil, VII. Kapitel, B.2.

des ökonomischen Kontextes. Allerdings: Es handelt sich dabei nicht um einen singulären Schutzauftrag.

1495 Die DSGVO verbürgt *an erster Stelle,* in Anknüpfung an die traditionelle Datenschutzgesetzgebung, *den Schutz natürlicher Personen* bei der Verarbeitung personenbezogener Angaben. In diesem Punkt vergleichbar die Fassung von Art. 1 nDSG. Nach der Bestimmung bezweckt das Gesetz den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Personendaten bearbeitet werden. Art. 1 DSGVO und Art. 1 (n)DSG dokumentieren, dass auch in Zukunft der *Subjektschutz* und die subjektivrechtliche Anknüpfung im Datenschutzrecht des kontinentalen Europas erhalten bleiben.

1496 Der Schutzaspekt, wonach die datenschutzrechtliche Regulierung *dem Schutz der (natürlichen) Person* dient, wird über den Zweckartikel hinausgehend im Ausbau der Betroffenenrechte resp. Ansprüche der Datensubjekte repräsentiert. Anders als im DSG wird in der DSGVO indes auf eine spezifische Verwurzelung des Datenschutzrechts der EU im Persönlichkeitsschutz verzichtet.

1497 Umgekehrt verzichtet das DSG auf eine Ergänzung, wie sie die DSGVO vorsieht. Neben dem Schutz natürlicher Personen, ihrer Grundrechte sowie Grundfreiheiten *wird in Art. 1 Abs. 1 DSGVO von einem Schutz personenbezogener Angaben der natürlichen Person* gesprochen. Die DSGVO inkludiert neuerdings den «Schutz von Personendaten». Das erstaunt, zumal doch in der vorangehenden Ära der Datenschutzgesetzgebung stets betont wurde, dass es *nicht* Personendaten seien, die vom Datenschutzrecht geschützt würden. Die fälschliche Titulierung der sog. Datenschutzgesetze wurde stets als symptomatisch für das Rechtsgebiet bezeichnet.[1964] Es sei die Persönlichkeit, die das Datenschutzrecht zu schützen habe.[1965]

1498 Im Passus der DSGVO, wonach es um den *Schutz von personenbezogenen Daten* ginge, wird in der Kommentarliteratur die Abwendung von einer langen, im Privatsphärenschutz gründenden Rechtstradition gesehen.[1966] Gleichwohl scheint der Autor dieser Kommentarstelle im Ergebnis offenzulassen, ob es sich bei der Integration des «Schutzes von Personendaten» in den Verordnungstext sowie

1964 Kritisch auch zur Verengung der Regelungsperspektive des Datenschutzrechts als Unterfall des allgemeinen Persönlichkeitsrechts sowie auf Daten Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 und N 26.

1965 Forstmoser, digma 2003, 50 ff., 51.

1966 Mit Hinweis auf die vorausgehenden Kommissionsentwürfe sowie die Rechtsprechung des EuGH, der den Schutz der Privatsphäre seit Jahrzehnten als allgemeinen Grundsatz des Europarechts anerkannt hat, Sydow, NomosKomm-DSGVO, Art. 1 N 10 f.; vgl. zum Prozess des Übergangs von einer Sphärenkonstruktion hin zum Autonomieschutz in den 1970er Jahren Schmidt, JZ 1974, 241 ff., 243 ff.

dem Verzicht einer Referenz auf den Privatsphärenschutz um eine rein terminologische Änderung oder um eine konzeptionelle Neuerung handle.[1967]

Nahezuliegen scheint zumindest, dass der Wortlaut von Art. 1 Abs. 1 DSGVO 1499
den Verfechtern eines «Eigentums an Daten» das Wort redet. Das Eigentumsparadigma kann als neuer Hauptlösungsansatz für die datenschutzrechtlichen Herausforderungen beschrieben werden.[1968] Gemäss Art. 1 Abs. 1 DSGVO sind es dem Wortlaut nach neu «Personendaten» als Quasi-Objekte, auf deren Schutz der Rechtstext explizit abzielt. Das Argument für die Verbürgung einer als-ob-eigentumsrechtlichen Position der Datensubjekte an Personendaten mit entsprechenden Herrschafts- resp. Verfügungskompetenzen des Datensubjektes liesse sich über weitere Regelungskonzepte der DSGVO erhärten: In der DSGVO kommt der Einwilligung des Datensubjektes im Vergleich zum eidgenössischen Datenschutzgesetz eine markant wichtigere Rolle zu. Sie hängt mit dem divergenten Konzept des prinzipiellen Verarbeitungsverbotes und Erlaubnistatbeständen gemäss DSGVO sowie mit prinzipieller Verarbeitungsfreiheit und Schranken gemäss DSG für den privaten Bereich zusammen.[1969]

Welche *Folgerungen* aus der Formulierung gemäss DSGVO in ihrem Schutz- 1500
zweckartikel zu ziehen sind, wird sich weisen. Weil der Erfassung des Schutzzwecks oder genauer der Schutzzwecke des Datenschutzrechts seit jeher hohe Relevanz zugemessen wird, wären vertiefte wissenschaftliche Analysen insofern von Interesse.

Unbestritten dürfte schon heute sein, dass die *systematische Auslegung* von be- 1501
sonderer Bedeutung für die Erfassung der datenschutzrechtlichen Schutzzwecke ist: Die Vorgaben und neuen Instrumente, welche die DSGVO vorsieht, geben Impulse für die Interpretation und Erfassung datenschutzrechtlicher Schutzerwägungen. Umgekehrt liefern die datenschutzrechtlichen Schutzzwecke einen Beitrag zur Interpretation der jeweiligen konkreten Datenschutzvorgaben und Verarbeitungsanweisungen.

Anhand dieser Kurzanalyse wurde deutlich, dass das *Datenschutzrecht mehr-* 1502
dimensionalen und verschiedenen Schutzzwecken dient. Namentlich eine systematische und kontextuelle Auslegung von Art. 1 DSGVO kann Entwicklungen

1967 Sydow, NomosKomm-DSGVO, Art. 1 N 12.

1968 Hierzu dritter Teil, VIII. Kapitel, B.3.; Miller beschreibt die Eigentumstheorie über die Privatsphäre unter dem Titel «Alter Wein in neuen Schläuchen», 256 ff.

1969 Vgl. bereits die Ausführungen zum Dualismus, zweiter Teil, IV. Kapitel; die DSGVO beantwortet die Frage nach dem Ausgangspunkt ähnlich, wie es Deutschland als Vorreiterland i. S. Datenschutz getan hat: Datenverarbeitungen benötigen einen Bearbeitungsgrund, weil der Ausgangspunkt das grundsätzliche Datenverarbeitungsverbot, vgl. Art. 5 DSGVO, ist. Anders dagegen die Schweiz, die weiterhin an ihrem dualen System festhält und für den privaten Sektor den Grundsatz der Verarbeitungsfreiheit mit Schranken vorsieht; vgl. zur Einwilligung als «Ersatzgrundlage» im öffentlich-rechtlichen Bereich Glass, 228 ff.

mit Blick auf den datenschutzrechtlichen Schutzzweck resp. die datenschutzrechtlichen Schutzzwecke freilegen. Die DSGVO erhebt *nicht* den Anspruch, «ihr Schutzobjekt» in einer engen und isolierenden Weise zu fixieren. Die Offenheit und Weite im Rahmen der Definierung des Schutzobjektes kann als Versäumnis taxiert werden. Oder aber sie werden als Errungenschaft für das Datenschutzrecht der Zukunft gelesen.

1503 Für die Anerkennung von ausdifferenzierten Schutzbestrebungen ist der bereits erwähnte, gleichzeitig verbürgte Schutz der Person und von Personendaten indikativ.[1970] Die Mehrdimensionalität und Diversität der Schutzzwecke erhellt sich somit anhand von Art. 1 DSGVO und seinen verschiedenen Absätzen: Art. 1 DSGVO ergänzt in seinem Abs. 1 den Schutz der Person sowie der Personendaten in einem ersten Satzteil mit der Gewährleistung des freien Personendatenverkehrs in einem zweiten Satzteil. Diese dualistische Schutzausrichtung – welche einen potentiellen Zielkonflikt offen adressiert[1971] – wird in den anschliessenden Abs. 2 und Abs. 3 ausgearbeitet, indem sich Art. 1 Abs. 2 DSGVO dem Subjekt- und Objektschutz widmet. Art. 1 Abs. 3 DSGVO adressiert den Schutz des freien Verkehrs von Personendaten. Damit wird erneut ein Aspekt des Schutzzweckes der DSGVO aufgegriffen, der bereits anhand des räumlichen resp. extraterritorialen Anwendungsbereichs der DSGVO nach Art. 3 DSGVO herausgearbeitet wurde: Der Erlass zielt auf eine Harmonisierung des Datenschutzrechts innerhalb des EU-Raums und unter Umständen über diesen hinaus ab. Damit will er auch der «digitalen Globalisierung» Rechnung tragen. «Das» Schutzziel der DSGVO erschöpft sich somit keineswegs in dem an erster Stelle und im ersten Satzteil deklarierten *Schutzaspekt*.

1504 Eine systematische Betrachtung fördert einen zusätzlichen Entwicklungstrend zu Tage, der relevant für die Erfassung datenschutzrechtlicher Schutzausrichtung(en) ist: Wie ein roter Faden lässt sich eine Zielsetzung nachverfolgen, der gemäss es darum geht, *Personendatenverarbeitungsprozesse zu strukturieren* und *regelkonforme Datenflüsse auch faktisch sicherzustellen*. Der im Wortlaut direkt bezeichnete Schutz «des Subjektes, der Person» sowie «des Objektes, der Personenangabe» wird damit zum finalen Schutzzweck, der in erster Linie durch *Handlungsanleitungen gegenüber den Verarbeitenden* und konkretisieren-

1970 Kritisch zu einem Begriff des Datenschutzes, der zu Unrecht als Ziel des Datenschutzes den Schutz von Personendaten suggeriert, Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 f. und N 26; vgl. Forstmoser, digma 2003, 50 ff., 51; Drechsler sprach in seinem Beitrag an der Konferenz zum Titel «Neue EU-Datenschutzgrundverordnung: Herausforderungen für Schweizer Unternehmen bei der Umsetzung», Europa Institut der Universität Zürich, Donnerstag, 24. Mai 2018, Zürich, auch von weit verbreiteten «fake news», also Missverständnissen resp. Fehlinformationen, was die Beschreibung und Interpretation des Datenschutzgesetzes und weiter des schweizerischen Datenschutzrechts anbelangt, vgl. dritter Teil, VII. Kapitel.

1971 Auch zum Verhältnis der beiden Ziele vgl. Sydow, NomosKomm-DSGVO, Art. 1 N 2 ff. und N 16 ff., insb. N 20 ff.

den Vorgaben für die Gestaltung von Verarbeitungsprozessen sichergestellt wird. Insofern rücken die *Datenverarbeitungsprozesse und Personendatenflüsse* mit einem Akzent auf die Implementierungsverantwortung der Verarbeitenden in den Vordergrund.[1972]

Mit der gesetzgeberischen Ausrichtung an Verarbeitungsprozessen sowie Datenflüssen geht der Ausbau *organisatorischer, prozeduraler sowie technischer Schutz- und Kontrollmechanismen sowie -massnahmen* einher. Sie sichern das im letzten Jahrhundert entwickelte materielle Datenschutzrecht ab. Damit findet neu die Positionierung des Datenschutzes und die Einhaltung der datenschutzrechtlichen Vorgaben als *Compliance- und Governance-Aufgabe* statt. 1505

Diese Entwicklung ist in Anbetracht der langjährigen und dominanten Prägung des Datenschutzrechts durch den zivil- und deliktsrechtlichen Persönlichkeitsschutz als Paradigmenwechsel für die Datenschutzregulierung zu qualifizieren.[1973] Indikativ für diesen ist die Figur des sog. «Verantwortlichen», vgl. Art. 7 Ziff. 7 DSGVO und Art. 5 lit. j nDSG. Mit der entsprechenden Terminologie wird von den neuen Datenschutzerlassen ausgedrückt, dass es nicht mehr erst und nur das von einer Personendatenverarbeitung in seiner Persönlichkeit verletzte Datensubjekt ist, das im Vordergrund der normativen Aufmerksamkeit steht. Vielmehr werden an erster Stelle die Verarbeitenden in der Rolle der Verantwortlichen oder der Auftragsverarbeitenden *proaktiv* in die Pflicht resp. Verantwortung genommen. Der datenschutzrechtliche Akzent wird damit verschoben: Das abwehrrechtliche resp. «defensiv-reaktive[1974]» Element rückt in den Hintergrund, wohingegen die proaktive Rolle der Verarbeitenden und ihre primäre Verantwortlichkeit sowie die präventiven Elemente in den Vordergrund rücken. 1506

Die Installierung des Datenschutzes als Compliance- und Governance-Aufgabe kann in Bezug auf die datenschutzrechtlichen Schutzerwägungen nicht nur als *Kontrapunkt* zum deliktsrechtlich ausgerichteten Persönlichkeitsschutz beschrieben werden. 1507

Eine andere Perspektive nimmt wahr, wie die Etablierung des Datenschutzes als Compliance- und Governance-Aufgabe die *Einhaltung des Datenschutzrechts in die jeweilige Organisation internalisiert*. Ebendiese *Internalisierungswirkung* ist erwähnenswert, zumal gerade in der Schweiz mit Blick auf die DSGVO in erster Linie die starke Behördenhand mit der Möglichkeit drakonischer Strafen zur Kenntnis genommen wurde. Eine Fokussierung auf diese sanktionierende staatli- 1508

1972 Vgl. zu dieser und damit einer Perzeption, die Datenflüsse in den Blick nimmt, anstatt in statischer Weise das Datensubjekt und Personendaten als Quasi-Objekte zu betrachten, insb. bereits erster Teil, I. und II. Kapitel, zweiter Teil, V. Kapitel, B.4.

1973 Vgl. zu diesem Strukturmerkmal zweiter Teil, VI. Kapitel.

1974 Vgl. zum Begriff im Zusammenhang mit der Datensicherheit und dem Datenschutz Bossardt, § 21, in: Passadelis/Rosenthal/Thür (Hrsg.), N 21.44.

che Rechtsdurchsetzung fängt das Schutzkonzept der DSGVO nur punktuell ein. Bedeutsam ist, dass die Datenschutz-Compliance in der *Eigenverantwortung der Verarbeitenden steht* – sie sind quasi organisch und von innen heraus für die Datenschutzrechtseinhaltung zuständig. Damit wird gleichzeitig die Einbettung der jeweiligen Organisation in ein spezifisches Milieu relevant. Ein solches Schutzkonzept, wonach die Verantwortlichkeit intrinsisch fixiert wird, zugleich indes stets auch die Einbettung der jeweiligen Organisation in ein bestimmtes Umfeld relevant wird, findet eine Abstützung über die Ansätze der Selbstregulierung. Für die DSGVO ist namentlich auf die sog. Verhaltensregeln, welche Besonderheiten der jeweiligen Verarbeitungsbereiche adressieren sollen, sowie die Zertifizierung gemäss Art. 40 ff. DSGVO hinzuweisen. Nach der Totalrevision sind Art. 11 und Art. 13 nDSG, letzterer mit Ausführungsverordnung, einschlägig.

1509 Resümierend lässt sich festhalten: Die *Schutz- und Zielrichtungen sind in der DSGVO in gut sichtbarer Weise ausdifferenziert, facettenreich und mehrdimensional.*[1975] Eine Beschränkung auf den Individualrechtsschutz der Person findet nicht statt. Vielmehr wird explizit der *Schutz von Personendaten verbürgt*. Zugleich transportiert die DSGVO den Schutzgedanken, wonach sie allem voran eine Garantenstellung für die (digitale) Wirtschaft, aber auch die Forschung, Sicherheit usf. einnimmt. Mehrere neue Instrumente sichern die Regelkonformität von Personendatenflüssen ab. Indem der Datenschutz gemäss DSGVO als Compliance- und Governance-Aufgabe installiert wird (ebenso in der Totalrevision des DSG), wird eine organische Funktionsweise etabliert. Der Datenschutz muss von innen heraus in die DNA der Datenverarbeitenden integriert werden. Hierbei gewinnen organisatorische und prozedurale Instrumente grosse Bedeutung. Die jeweiligen Unternehmen z. B. der Privatwirtschaft sind primär für das datenschutzrechtliche «Housekeeping» zuständig. Gleichzeitig ist relevant, dass die Organisationen stets in ihr spezifisches Milieu eingebettet sind. Die neuen Datenschutzerlasse adressieren dies, indem sie Instrumenten der Selbstregulierung einen nicht zu vernachlässigenden Platz einräumen.

1510 In der DSGVO, weniger ausgeprägt im totalrevidierten DSG, finden sich plurale und zugleich systemreflexive Schutzausrichtungen. Vertiefende wissenschaftliche Untersuchungen, namentlich auch rechtsvergleichend und zu den Entwicklungen der Schutzerwägungen, wären aufschlussreich.[1976]

1975 Die Mehrdimensionalität der Schutzausrichtungen gemäss DSGVO tritt m. E. an mehreren weiteren Stellen zu Tage, z. B. in Erwägungsgrund 2, wonach die vereinheitlichten Vorgaben für die Mitgliedstaaten der EU zur «Vollendung eines Raumes der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarktes sowie zum Wohlergehen natürlicher Personen beitragen»; der Zweck des Datenschutzrechts und der Befund der Mehrdimensionalität der Schutzzwecke wurden insb. im Zuge des Zweckbindungsgrundsatzes und namentlich einer Analyse des Volkszählungsurteils reflektiert, vgl. zweiter Teil, V. Kapitel, B.4.

1976 M. w. H. Buchner, 26 ff. und 41 ff.

2.3. Zum Dualismus in Europa – DSGVO-Monismus, DSG-Dualismus

Nach der *Tour d'Horizon* über die Ausdifferenzierung von *pluralistischen Schutzrichtungen* ist ein Vereinheitlichungsschritt zu thematisieren. Die DSGVO führt das *Datenschutzrecht einem monistischen Regime* zu, indem ihre Vorgaben *prinzipiell gleichermassen von privaten wie öffentlichen Stellen* zu beachten sind. 1511

Ein solcher Übergang zu einem *monistischen Regime* ist als ein entscheidendes Element zu taxieren, welches den datenschutzrechtlichen Paradigmenwechsel mitbegründet, der mit der DSGVO einhergeht. Die Frage nach der Vereinheitlichung der datenschutzrechtlichen Vorgaben für den privaten und den öffentlichen Bereich wurde allem voran in Deutschland lange vor der Ausarbeitung der DSGVO intensiv diskutiert. Als Argument für einen Monismus im Datenschutzrecht wurde primär ins Feld geführt, dass es für das Datensubjekt irrelevant sei, ob seine Personendaten durch private oder öffentliche Stellen verarbeitet würden. Umgekehrt wurde ein Dualismus mit grundlegenden (verfassungs-)rechtlichen Differenzen zwischen den beiden Bereichen begründet.[1977] 1512

Bis heute präsentiert sich die Situation anders für die Schweiz. Die Totalrevision des DSG hält am etablierten Dualismus fest. Obschon die Totalrevision auch von den Entwicklungen in der EU vorangetrieben wurde, folgt die Schweiz in diesem Aspekt nicht dem Konzept der DSGVO. Der Dualismus des DSG wurde als *erstes Strukturmerkmal* im zweiten Teil dieser Arbeit herausgearbeitet.[1978] Kernelement des schweizerischen Regimes des DSG bleibt auch nach der Totalrevision der *pointierte Dualismus mit entgegengesetztem Ausgangspunkt*. 1513

Pro memoria: Während für den öffentlichen Bereich des Bundes ein prinzipielles Verarbeitungsverbot mit Ausnahmen besteht, gilt für den privaten Bereich die prinzipielle Verarbeitungsfreiheit mit Schranken, vgl. Art. 30 ff. resp. Art. 33 f. nDSG. Die Schranken der Verarbeitungsfreiheit im privaten Bereich werden in erster Linie über die Verletzung der allgemeinen Verarbeitungsgrundsätze definiert, wobei eine Einbettung in die persönlichkeitsrechtliche Mechanik stattfindet, vgl. Art. 30 Abs. 2 i. V. m. Art. 6 resp. Art. 8 nDSG.[1979] Die Totalrevision rezipiert weitgehend Art. 12 f. i. V. m. Art. 4 resp. Art. 6 DSG. Ein materiellrechtlich markant strengeres Regime für den privaten Bereich sieht die DSGVO aufgrund des monistischen Regimes mit ihrem prinzipiellen Verarbeitungsverbot sowie Erlaubnisvorbehalten vor, vgl. Art. 6 DSGVO. Diese Regelungsdifferenzen 1514

1977 Zur zentralen und grundlegenden Bedeutung der Frage nach einer dualistischen resp. monistischen Datenschutzregelung vgl. Ders., a. a. O.

1978 Vgl. zweiter Teil, IV. Kapitel; vgl. zu den unterschiedlichen Regelungsansätzen gemäss DSGVO und DSG (auch nach Totalrevision) ebenso Auf der Mauer/Fehr-Bossard, in: Thouvenin/Weber (Hrsg.), ITSL 2017, 23 ff., 31.

1979 Vgl. hierzu zweiter Teil, VI. Kapitel.

begründen ein Delta im Schutzniveau gemäss schweizerischem DSG gegenüber demjenigen der DSGVO.

1515 In der Schweiz wurde ein *Wechsel zu einem monistischen System* und die Implementierung eines Regimes des prinzipiellen Verarbeitungsverbotes mit Erlaubnistatbeständen für den privatrechtlichen Bereich *nicht ernsthaft* in Betracht gezogen. Bis heute zeigt sich damit der Dualismus im schweizerischen DSG in seiner aktuellen sowie totalrevidierten Fassung *nur beschränkt als Ergebnis einer Evaluation von sachlogischen Argumenten*. Wie die Ausführungen im zweiten Teil dieser Schrift zum Dualismus nachwiesen, waren es in erster Linie die *politischen Kräfte, die ebendieses Regelungskonzept* motivierten. Der Datenschutznormierung für den privaten Bereich war heftiger Widerstand aus Wirtschaftskreisen erwachsen.[1980]

1516 Die Schweiz sieht damit auch nach der Totalrevision des DSG – anders als die EU mit der DSGVO, welche die Gleichschaltung der datenschutzrechtlichen Vorgaben für den öffentlichen und privaten Bereich vorsieht – eine *systemische Differenzierung innerhalb ihrer datenschutzrechtlichen Querschnittsgesetzgebung* vor. Ein solches dualistisches Regime wurde, wie bereits erwähnt, von Nissenbaum als «krude Version eines kontextuellen Ansatzes» bezeichnet.[1981]

1517 Aktuell weisen die Entwicklungen und Forderungen in den verschiedenen Rechtskreisen unter dem Aspekt der *Einschlägigkeit kontextueller Erwägungen für das Datenschutzrecht* in verschiedene Richtungen: Die DSGVO überwindet die bereichsspezifische Ausdifferenzierung anhand der beiden grossen Kammern und der Zweiteilung der Akteure in private Akteure und Behörden. Die Schweiz dagegen hält an einer dichotomischen Regelung fest. Damit implementiert sie selbst im DSG einen systembezogenen Ansatz. In den USA wird auf ein «allgemeines Datenschutzrecht» für den privaten Bereich verzichtet; datenschutzrechtlich wird über bereichsspezifische Spezialerlasse legiferiert.[1982] Wie anhand des *Fair Credit Reporting Act* veranschaulicht wurde, richtet sich dieser Erlass an erster Stelle auf den Schutz der Integrität des Banksektors und das Vertrauen der Allgemeinheit in die Integrität seines Handelns. Folglich ist das US-amerikanische Recht in ausgeprägter Weise ein Recht des informationellen Systemschutzes, wohingegen die Schweiz diesen im DSG nur ansatzweise anerkennt. Zwar lässt sich selbst in der DSGVO ein solcher Aspekt identifizieren; aufgrund des monistischen Regimes allerdings rückt die systemische Schutzdimension eher in den Hintergrund.

1980 Hierzu vertiefend zweiter Teil, IV. Kapitel.
1981 Vgl. Nissenbaum, 141.
1982 Vertiefend Buchner, 7 ff., insb. 15 ff.

2.4. Zum Ansatz der gestärkten Rechtsposition des Datensubjektes

Charakteristikum datenschutzrechtlicher Gesetzgebung ist seit jeher die Anknüpfung im Schutz der Person, des Subjektes resp. der Persönlichkeit. Diese traditionsreiche Anbindung des Datenschutzrechts wird trotz der beschriebenen Diversifizierungstendenzen mit Blick auf den Schutzzweck nicht nur beibehalten, sondern weiter gestärkt. Ursächlich für den Ausbau der Rechtsposition des Datensubjektes war nicht zuletzt die am bisher geltenden Datenschutzrecht angebrachte Hauptkritik am Datenschutzrecht: Personendatenverarbeitungen würden weitgehend an den Datensubjekten vorbei stattfinden, oft okkult bleiben und mit einer Degradierungswirkung des Datensubjektes zum Objekt konnotiert werden.[1983] Der Degradierung des Menschen zum Objekt durch die Technik entgegenzuwirken, dafür wurde und wird das Recht zuständig gemacht. 1518

Die Bestätigung und Stabilisierung des individualrechtlichen Ansatzes und des Paradigmas des Subjektschutzes lässt sich deutlich anhand der Entwicklungen im Rahmen der *Betroffenenrechte und im Ausbau der Transparenz- sowie Einwilligungsvorgaben nachweisen*. 1519

Eine der tragenden Säulen der DSGVO sowie des DSG in seiner aktuellen wie totalrevidierten Fassung, die das Subjekt schützen soll, bilden die sog. *Betroffenenrechte* resp. die Rechte, welche den Individuen – den Datensubjekten – zugestanden werden. Die *Betroffenenrechte verbürgen aktive Ansprüche* der Datensubjekte gegenüber den Verarbeitenden, vgl. Art. 12 ff. DSGVO und Art. 25 ff. nDSG, aber auch Art. 32 nDSG.[1984] Für den Fall der nicht korrekten Erfüllung durch die Verarbeitenden steht die Rechtsdurchsetzung über behördliche Massnahmen offen.[1985] 1520

Die Rechtsposition von Datensubjekten wird nicht isoliert und abschliessend über die sog. Betroffenenrechte definiert. Vielmehr lassen sich in Anbetracht des tradierten Schutzzweckes des Datenschutzrechts nahezu sämtliche datenschutzrechtlichen Vorgaben im Lichte einer individualrechtlichen Position lesen. Der Schutz des Datensubjektes wird von den Einwilligungs- und Transparenzvorgaben sowie den damit verbundenen Informationspflichten mitstrukturiert.[1986] Eine zentrale Rolle für den Schutz der Person nimmt das materielle Datenschutzrecht mit den allgemeinen Verarbeitungsgrundsätzen ein. Einige der neuen Instrumente und Datenschutzvorgaben, die dem Schutz des Datensubjektes und dem Subjekt- 1521

1983 Buchner, 119 ff.
1984 Zu den Betroffenenrechten nach Totalrevision statt vieler vgl. Bieri/Powell, Jusletter vom 16. November 2020, N 21 ff.
1985 Art. 79 DSGVO verbürgt das Recht auf einen wirksamen gerichtlichen Rechtsbehelf jeder betroffenen Person gegen Verantwortliche und Auftragsverarbeiter.
1986 Richtungsweisend mit Blick auf Schranken der Einwilligung als Erlaubnistatbestand: Entscheid i. S. PwC, August 2019.

schutz dienen, werden unter dem Titel der «Governance und Compliance» präsentiert werden.[1987]

1522 Die sog. *Betroffenenrechte* i. e. S. werden in der DSGVO in Kapitel III. unter dem Titel «Rechte der betroffenen Person» verbürgt. Identisch lautet in der Totalrevision des DSG das 4. Kapitel mit den Art. 25 ff. nDSG. Die Systematisierungen im Zusammenhang mit den Betroffenenrechten und die in engem Zusammenhang stehenden Einwilligungsvorgaben sowie Informationsrechte und -pflichten variieren: Während letztere in der DSGVO unter dem Titel der Betroffenenrechte abgehandelt werden, figurieren im totalrevidierten DSG die allgemeinen Informationspflichten unter dem Titel der Pflichten der Verantwortlichen und Auftragsverarbeitenden, vgl. Art. 19 nDSG, die Einwilligungsvorgaben innerhalb der allgemeinen Verarbeitungsgrundsätze, vgl. Art. 6 Abs. 6 und Abs. 7 nDSG. Wichtige individualrechtliche Behelfe finden sich in Art. 31 nDSG. Exemplarisch dafür, dass die Gesetzessystematik in der Totalrevision unter dem Titel der Betroffenenrechte nicht derjenigen der DSGVO entspricht, sind die Pflichten der Verantwortlichen bei automatisierten Einzelfallentscheidungen und Profiling, die teilweise auch gegenüber dem Datensubjekt wahrzunehmen sind.[1988] Kategorisierend liesse sich von Betroffenenrechten im engeren resp. weiteren Sinne sprechen.

1523 Unter dem Titel der *Betroffenenrechte* gemäss DSGVO werden zunächst unter den Vorgaben für die Informierung resp. Information die Anforderungen angehoben, vgl. Art. 12 ff. DSGVO. Das Auskunftsrecht oder «Right to Data Access» ist in Art. 15 DSGVO verbürgt, wobei die Unternehmen entsprechende Prozesse zur fristgerechten sowie regelkonformen Gewährleistung zu etablieren haben.[1989] Der Berichtigungsanspruch oder das «Right to Rectification» ist in Art. 16 DSGVO, der Löschungsanspruch resp. das «Recht auf Vergessenwerden», auch prominent diskutiert als «Right to be forgotten» resp. «Right to Erasure», in Art. 17 DSGVO verbürgt. Zudem wurde ein Recht auf Einschränkung der Bearbeitung eingeführt, vgl. Art. 18 DSGVO. Art. 19 DSGVO sieht eine Mitteilungspflicht bezüglich der Berichtigung und Löschung von Personendaten vor. Eine Neuschaffung ist das Recht auf Datenportabilität, Art. 20 DSGVO.[1990] Das Widerspruchsrecht findet sich in Art. 21 DSGVO. Der Widerspruch erfüllt, wie gezeigt, in einem Regime mit prinzipiellem Verarbeitungsverbot eine andere Funktion als im

1987 Hierzu Kresse, NomosKomm-DSGVO, Art. 97 N 1 ff.; vgl. zur Bedeutung der Technologien für die Compliance Bartuschka, CB 2019, 340 ff.

1988 Vgl. Art. 19 ff. nDSG. Sie werden unter den Pflichten der Verarbeitenden geregelt und nicht unter den Betroffenenrechten – anders dagegen Art. 21 f. DSGVO in diesem Zusammenhang unter dem Titel der Betroffenenrechte.

1989 Hierzu Griesinger, Jusletter vom 20. Januar 2020, N 4 ff.

1990 Zu diesem datenschutzrechtlichen Novum, welches das Datensubjekt pointiert ins Zentrum rücke, vertiefend Laux, digma 2019, 166 ff.

Regime der prinzipiellen Verarbeitungsfreiheit mit Schranken. Einschlägig sind weiter neu die Rechte der Datensubjekte resp. Pflichten der Verarbeitenden gegenüber den Datensubjekten im Zusammenhang mit der automatisierten Einzelfallentscheidung und dem Profiling, Art. 22 DSGVO.

Die Vorschläge gemäss bundesrätlichem Entwurf der Totalrevision des DSG zu den Betroffenenrechten entsprachen nur teilweise dem Regime der Betroffenenrechte gemäss DSGVO. In den parlamentarischen Beratungen im Jahr 2019 wurden mehrere Änderungen diskutiert. Die Betroffenenrechte werden in der verabschiedeten Version des totalrevidierten DSG im 4. Kapitel verbürgt. An erster Stelle steht das Auskunftsrecht, vgl. Art. 25 nDSG. Der Auskunftsanspruch wurde ausgebaut. Der Katalog der Angaben, über die informiert werden muss, fällt breiter aus als bisher, vgl. Art. 25 Abs. 2 nDSG. Auskunft zu erteilen ist über die Kategorien der bearbeiteten Angaben, die Identität des Verantwortlichen, die Dauer der Aufbewahrung, den Zweck der Verarbeitung sowie die Logik, auf welcher automatisierte Einzelfallentscheidung basieren. Während der Nationalrat dagegen Restriktionen vorschlug, sollte gemäss dem Entscheid des Ständerates wieder auf die bundesrätliche Fassung zurückgekommen werden, womit eine Differenzbereinigung erforderlich ist. Auch der Auskunftsanspruch verlangt von den Unternehmen die Entwicklung spezifischer Prozesse und Organisationen sowie Zuständigkeiten, wobei an deren Anfang die Identifizierung der das Auskunftsgesuch stellenden Person steht. Eine Neuschöpfung, wie sie die DSGVO im Bereich der Rechte der betroffenen Personen mit dem Recht auf Datenportabilität anerkennt, vgl. Art. 20 DSGVO, wurde gemäss bundesrätlichem Entwurf zur Totalrevision nicht in das DSG integriert. Eine Verankerung beschloss die staatspolitische Kommission des Nationalrates, Art. 25a E-DSG.[1991] Der Änderungsvorschlag wurde vonseiten des Ständerates nicht verworfen.[1992] Er findet sich neu in Art. 28 nDSG. Ein Pendant zum Recht der Betroffenen auf Einschränkung der Datenverarbeitung, wie ihn Art. 18 DSGVO vorsieht, fehlt soweit ersichtlich in der Totalrevision des DSG. Vorgeschlagen werden neuerdings auch in der Schweiz Vorgaben im Zusammenhang mit dem Profiling und der automatisierten Einzelfallentscheidung, insb. Art. 6 Abs. 7 lit. b und Art. 21 nDSG.[1993] Den Rechten auf Berichtigung und Löschung widmet sich Art. 31 nDSG. Darüber hinaus sollen nach totalrevidiertem DSG bei sog. Datensicherheitsvorfällen nicht nur Meldepflichten gegenüber den Behörden, sondern ebenso gegenüber dem Daten- 1524

1991 Vgl. Das Schweizer Parlament, Medienmitteilung, Kommission schliesst Beratung der Revision des Datenschutzgesetzes ab, Bern 2019, <https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-08-16-a.aspx> (zuletzt besucht am 30. April 2021).

1992 Vgl. Fahne DSG 17.059 – 3 – 2 n. Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz, mit den Anträgen der Staatspolitischen Kommission des Ständerates vom 19. November 2019, 28.

1993 Hierzu jüngst vertiefend Heuberger, *passim*.

subjekt greifen, vgl. Art. 24 nDSG. Die DSGVO sieht ein ähnliches Instrumentarium mit den Art. 33 f. DSGVO vor, wobei eine Meldepflicht gegenüber den Behörden besteht, bei qualifizierten Fällen zudem gegenüber den Datensubjekten. Wie der Name andeutet, greift die Meldepflicht bei sog. Datensicherheitsvorfällen in Konstellationen, in welchen die Sicherheit von Personendaten verletzt wurde, nicht dagegen bei einer allgemeinen Verletzung der datenschutzrechtlichen Verarbeitungsgrundsätze. Als Datensicherheitsvorfälle gelten die Verletzung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Personendaten. Die Gewährleistung dieser Notifikationspflichten bedingt bei den Unternehmen die Aufsetzung ausdifferenzierter und teilweise komplexer Prozesse sowie Organisationsstrukturen, wobei namentlich die Frist von 72 Stunden in der Praxis eine beträchtliche Herausforderung darstellt. Auch gemäss Art. 24 nDSG ist die Meldung an den EDÖB nach Abs. 1 von derjenigen an die Betroffenen, Abs. 4 nDSG, zu unterscheiden.

1525 Hinsichtlich der individualrechtlichen Position sind die Einwilligungsvorgaben von Interesse. Auf die suboptimale Systematisierung wurde im zweiten Teil für das geltende Recht hingewiesen. Die Totalrevision legt die Vorgaben an die gültige Einwilligung weiterhin innerhalb des Katalogs der Verarbeitungsgrundsätze nieder, Art. 6 Abs. 6 und Abs. 7 nDSG.

1526 Eine weitere Differenzbereinigung war bezüglich der Informationspflichten notwendig. Der Nationalrat wollte eine zurückhaltendere Regelung, die indes der Ständerat verwarf. Neu finden sich die Informationspflichten in erster Linie in Art. 19 ff. nDSG.

1527 Im bundesrätlichen Entwurf wurde sodann mit Art. 16 E-DSG und damit nicht unter dem Titel der Betroffenenrechte eine Bestimmung zum *Umgang mit personenbezogenen Angaben verstorbener Personen* vorgeschlagen. Die DSGVO regelt den «postmortalen Datenschutz» nicht spezifisch.[1994] Auch hier hat die staatspolitische Kommission des Nationalrates eine Änderung vorgenommen, diesmal im Sinne eines Verzichtes auf die Norm.[1995] Nach der ständerätlichen Debatte ergibt sich insofern keine Differenz. Die totalrevidierte Fassung des DSG sieht damit keine spezifische Regelung hierzu vor.

1994 In diesem Zusammenhang des digitalen Nachlasses ist auf eine Entscheidung aus Deutschland zu verweisen, mit der einer Mutter der Zugriff auf den Facebook-Account ihrer toten Tochter verweigert wurde. Das Mädchen war von einem Zug erfasst worden und tödlich verunglückt, wobei die Mutter wissen wollte, ob es ein Unfall oder Suizid war, <http://www.faz.net/aktuell/gesellschaft/ungluecke/facebook-muss-konto-der-toten-tochter-nicht-fuer-eltern-freigeben-15040618.html> (zuletzt besucht am 30. April 2021); zum digitalen Nachlass vgl. z. B. Künzle, successio 2015, 39 ff.

1995 Vgl. Das Schweizer Parlament, Medienmitteilung, Kommission schliesst Beratung der Revision des Datenschutzgesetzes ab, Bern 2019, <https://www.parlament.ch/press-releases/Pages/mm-spk-n-2019-08-16-a.aspx> (zuletzt besucht am 30. April 2021).

Aus *konzeptioneller Sicht* seien unter dem Titel der Betroffenenrechte im Zuge der jüngsten Rechtsentwicklungen folgende Aspekte herausgestellt: 1528

Erstens sind die *Betroffenenrechte* im eigentlichen Sinne *eine stabil etablierte Säule der Datenschutzgesetzgebung*, die mit den jüngsten rechtlichen Neuerungen gestärkt und fortentwickelt wurde.[1996] 1529

Zweitens lässt sich der Katalog der Betroffenenrechte verschieden lesen: zum einen als aktive resp. passive, individualrechtliche Ansprüche des einzelnen Datensubjektes. Diese Perspektive richtet den Fokus auf das Datensubjekt und setzt an der Kognition an, wonach es dem Datenschutz und seinem Recht namentlich auch darum geht, einer *Degradierung des Datensubjektes zu einem rechtlosen Informationsobjekt* entgegenzutreten. Die Betroffenenrechte lassen sich zum anderen in ihrer Funktion beschreiben, wonach diese die Einhaltung der allgemeinen Verarbeitungsgrundsätze absichern. Letztere formulieren Handlungsanleitungen der Verarbeitenden und bilden eine zweite tragende Säule der Datenschutzgesetzgebung. Die den Datensubjekten eingeräumten Betroffenenrechte haben damit ebenso eine Gewährleistungs- resp. Garantenfunktion für die allgemeinen Verarbeitungsgrundsätze und damit das Datenschutzrecht an sich, vgl. Art. 5 DSGVO und Art. 6 und 8 nDSG.[1997] 1530

Drittens konstituiert sich die Rechtsposition des Datensubjektes nicht abschliessend anhand der Betroffenenrechte in diesem III. Kapitel der DSGVO resp. dem 4. Kapitel totalrevidiertes DSG. Vielmehr finden sich wichtige Elemente, welche die Rechtspositionen des Datensubjektes strukturieren und garantieren, namentlich im Zusammenhang mit den Normen zur Einwilligung, weiter z. B. auch im Rahmen des Instituts der sog. Data Breach Notification. Hier wird für bestimmte Konstellationen auch eine Informationspflicht gegenüber dem Datensubjekt statuiert. 1531

Viertens ist die Erhöhung der Transparenz ein Kernelement der jüngsten datenschutzrechtlichen Neuerungen, auch, aber nicht nur unter dem Titel der Betroffenenrechte. In der Botschaft zur Totalrevision des DSG wird besagtes Ziel spezifisch thematisiert.[1998] Innerhalb des Trends der Erhöhung der Transparenz steht 1532

1996 Wie dargelegt variiert die Systematik. So werden in der DSGVO gewisse Ansprüche unter dem Titel der Betroffenenrechte aufgeführt, die im schweizerischen DSG nicht unter diesem Titel aufgeführt werden. Stellt man das Datensubjekt und seine Rechte sowie die ihm gegenüber bestehenden Pflichten der Verarbeitenden in den Vordergrund, schliessen sich sodann noch weitere Ansprüche an dieser Stelle in die Betrachtung ein, z. B. die Informationspflicht gegenüber dem Datensubjekt bei Datenschutzvorfällen.

1997 Zu dieser individualrechtlichen Durchsetzungsverantwortlichkeit vertiefend zweiter Teil, VI. Kapitel, C.; die Totalrevision will ebenso die Position des Datensubjektes ausbauen, Botschaft DSG 2017–1084, 17.059, 6941 ff., 7076.

1998 Hierzu auch EuGH, C-362/14, Urteil vom 6. Oktober 2015 – Schrems, E 105, wonach «verlangt wird, dass das Drittland […] tatsächlich ein Schutzniveau gewährleistet, das dem in der Union auf-

die Transparenzerhöhung gegenüber dem Datensubjekt.[1999] Ausgebaut werden vorab die Informationspflichten gegenüber dem Datensubjekt, vgl. Art. 13 ff. DSGVO und Art. 19 nDSG, wobei für die Schweiz die Statuierung einer allgemeinen Informationspflicht eine markante Schutzerhöhung resp. Änderung darstellt. Bislang beschränkte sich diese auf spezifische Konstellationen. Im Zusammenhang mit dem Ausbau der Transparenzvorgaben sind die Anforderungen an die datenschutzrechtliche Einwilligung und ihre Untervoraussetzung der «Informiertheit» einschlägig.[2000] Gemäss Art. 5 Abs. 1 i. V. m. Art. 6 DSGVO braucht es zur Durchbrechung des prinzipiellen Verarbeitungsverbotes mit Erlaubnistatbestand entweder die Einwilligung des Datensubjektes gemäss Abs. 1 lit. a DSGVO oder eines anderen nachfolgend aufgeführten Erlaubnistatbestandes. Die Voraussetzungen an eine gültige Einwilligung werden durch Art. 7 f. DSGVO fixiert und liegen hoch.[2001] Zu generische oder pauschale Einwilligungserklärungen im Kleingedruckten von AGB genügen den Anforderungen gemäss DSGVO nicht mehr.[2002] Vielmehr bedarf es einer granularen Auffächerung der Verarbeitungszwecke mit jeweils spezifischen Einwilligungserklärungen.

1533 Der Einwilligung wird selbst nach der Totalrevision des DSG keine mit dem Regime der DSGVO vergleichbare Rolle zukommen.[2003] Sie wird auch künftig für den privaten Bereich nicht als Erlaubnistatbestand innerhalb eines prinzipiellen Datenverarbeitungsverbotes figurieren. Sie wird weiterhin als Rechtfertigung im Regime der prinzipiellen Verarbeitungsfreiheit mit Schranken angesiedelt sein.

1534 Eine Stärkung der Transparenz und Informierung gegenüber Datensubjekten bringt die Totalrevision dennoch. Erhöhte Transparenz gegenüber dem Datensubjekt schafft der Ausbau der Informationspflichten.[2004] Hinzu treten weitere und teilweise neue Instrumente. Zu nennen ist das bereits erwähnte Instrument der sog. *Data Breach Notification*, wobei hier gegenüber den Behörden, ggf. aber

grund der Richtlinie 95/46 im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist».

1999 Zur Bedeutung von Treu und Glauben als Katalysator für die Herausbildung von Transparenzvorgaben und den datenschutzrechtlichen Trend, Transparenzvorgaben auszubauen, vgl. zweiter Teil, V. Kapitel, B.2.

2000 Vgl. Art. 4 Nr. 11 DSGVO; hierzu Jandt, BeckKomm-DSGVO, Art. 4 Nr. 11 N 1 ff.; zur Informiertheit Radlanski, 16; Fasnacht, N 241 ff. m. w. H.; Heuberger, N 303 ff.; sodann die einschlägige Kommentarliteratur; allgemeiner unter dem Titel des Persönlichkeitsrechts Haas, N 637 ff.; noch allgemeiner zur Einwilligung im Privatrecht und der Aufklärungspflicht Ohly, 372 ff., 473 ff.; vgl. einige Jahre vor Inkrafttreten der DSGVO Giesen, JZ 2007, 918 ff., 926 f., der die Heimlichkeit von Personendatenverarbeitungen, mit der daraus resultierenden Durchsichtigkeit der Person, als Problem beschreibt.

2001 Hierzu Buchner/Kühling, BeckKomm-DSGVO, Art. 7 N 2 und N 20 ff.; vgl. auch Passadelis/Roth, Jusletter vom 4. April 2016, N 29 ff.

2002 Vgl. zur Bestimmtheit Art. 5 Abs. 1 lit. b und Art. 6 Abs. 1 lit. a DSGVO; Buchner/Kühling, BeckKomm-DSGVO, Art. 7 N 61 ff.; Ingold, NomosKomm-DSGVO, Art. 7 N 37 ff.

2003 Vgl. zweiter Teil, VI. Kapitel.

2004 Vgl. Art. 19 ff. nDSG.

zudem gegenüber dem Datensubjekt Informationspflichten statuiert werden.[2005] Auch das Verarbeitungsverzeichnis sowie die Datenschutz-Folgenabschätzung sind Instrumente zur Erhöhung der Transparenz.[2006] Wesentlich für die Verwirklichung des Zieles, Personendatenverarbeitungen transparenter zu machen, ist der in der DSGVO explizit verankerte Accountability-Ansatz, Art. 5 Abs. 2 und Art. 24 DSGVO. Die Totalrevision sieht keine ausdrückliche Rechenschaftspflicht vor. Gleichwohl gilt diese in der Praxis als Standard.

1535 Wenn die Erhöhung der Transparenz als Charakteristikum der aktuellen datenschutzrechtlichen Neuerungswellen auch mittels neuer Instrumente wie dem Inventar oder dem Accountability-Ansatz beschrieben wird, erschliesst sich, dass der individualgüterschutzrechtliche Aspekt gleichzeitig gestärkt und ergänzt wird. Die erhöhten Transparenzvorgaben und teilweise neu etablierten Instrumente werden ihrerseits (wie allgemein die Betroffenenrechte) zwar von einer Kognition geprägt, wonach es zu verhindern gilt, dass der Mensch im Kontext undurchsichtiger Informationsverarbeitungstechnologien («Blackbox») zum orientierungslosen Informationsobjekt degradiert wird. Allerdings erhellt sich anhand der Entwicklungen unter dem Dachbegriff der Transparenz, dass die *persönlichkeitsrechtliche Dimension* erweitert wird. Es geht um *Transparenz und Rechenschaft der Verantwortlichen sich selbst gegenüber* und unter Umständen gegenüber den Behörden, aber auch der Gesellschaft und ihren Institutionen. Transparenz wird datenschutzrechtlich damit in einem deutlich weiteren Sinne angelegt. Der Aspekt findet, ergänzend zur individualrechtlichen Dimension, Relevanz im Rahmen der sog. Data Governance und Datenschutz-Compliance. Für diese sind in erster Linie die jeweiligen Verarbeitenden eigenverantwortlich zuständig.[2007] Informationen und Informationspflichten resp. -ansprüche figurieren stets als Garant für Vertrauen. Vertrauen – eine Kategorie, die für das Informations- und damit auch Datenschutzrecht eine besondere Bedeutung hat.[2008] Namentlich die grossen Technologiekonzerne werden sich in der kommenden Zeit um dieses Vertrauen verdient machen müssen.

2.5. *Zum Ansatz der faktischen Effektuierung*

1536 Der den datenschutzrechtlichen Neuerungen attestierte Paradigmenwechsel liegt sodann in den Massnahmen und Instrumenten begründet, die auf die Sicherstel-

2005 Vgl. Art. 24 nDSG; Art. 33 f. DSGVO.
2006 Vgl. Art. 12 und Art. 22 nDSG; Art. 30 und Art. 35 f. DSGVO.
2007 Vgl. neben der Kommentarliteratur zur Data Governance resp. Datenschutz-Compliance Morgan/Boardman, 3 ff.; Soares, 1 ff.; zur gestiegenen Bedeutung der Datenschutz-Compliance im Zuge der DSGVO Passadelis/Roth, Jusletter vom 4. April 2016, N 77; Rosenthal/Vasella, digma 2018, 166 ff., 166 f.
2008 Hierzu bereits die Ausführungen unter dem allgemeinen Verarbeitungsgrundsatz von Treu und Glauben im zweiten Teil, V. Kapitel, B.2.

lung der *faktischen Verwirklichung der Regelung* abzielen. Anders ausgedrückt: Die jüngsten Revisionsentwicklungen sollen dazu führen, dass die Datenschutzgesetzgebung im 21. Jahrhundert ihren Status als Symbolgesetzgebung hinter sich lässt. Mehrere Elemente und Instrumente von DSGVO sowie DSG sollen an dem für das bisherige Datenschutzrecht symptomatischen und neuralgischen Problem, dem Vollzugsdefizit resp. der ungenügenden Griffigkeit datenschutzrechtlicher Vorgaben in der Realität resp. Praxis, ansetzen. Insofern einschlägig sind ebenso die Installierung des Datenschutzrechts als Compliance-Aufgabe sowie der Ausbau und die Stärkung der behördlichen Kompetenzen – zwei Aspekte, die in Anbetracht ihrer Bedeutung unter einem eigenen Titel dargestellt werden.

1537 Da verstärkt auf die *faktische Implementierung* abgezielt wird, bedeutet dies zugleich, dass eine isoliert formelle Umsetzung durch die personendatenverarbeitenden Stellen und Unternehmen mittels sog. Paper Work den datenschutzrechtlichen Vorgaben nicht mehr genügt. Dies gilt ungeachtet dessen, dass Rechenschaftspflichten, aber auch Transparenz- und Einwilligungsvorgaben ihrerseits zur Verdichtung der Dokumentationsprozesse führen.

1538 Ein von der DSGVO kreiertes Instrument, das vom totalrevidierten eidgenössischen Datenschutzgesetz übernommen wird, ist das *Verarbeitungsverzeichnis*, vgl. Art. 30 DSGVO und Art. 12 nDSG. Für dieses lässt sich, inspiriert von einer für das Privatrecht entwickelten Lehrformel, der sog. Anspruchsmethode, ein datenschutzrechtlicher Leitsatz in Frageform ableiten: Wer verarbeitet welche Personendaten wie und wozu (sowie wie lange)? Die Pflicht zur Inventarisierung der in der Organisation stattfindenden Personendatenverarbeitungen und ihrer Prozesse ist ein wirkungsmächtiges Instrument, um an der Wurzel des faktischen Vollzugsdefizites anzusetzen: Nur in Kenntnis der Personendatenverarbeitungsprozesse wird eine datenschutzrechtskonforme Datenschutzverarbeitung realisierbar. Die Einhaltung der Verarbeitungsgrundsätze und weiterer Datenschutzvorgaben, die Gewährleistung der datenschutzrechtlichen Compliance lässt sich nur bewerkstelligen, wenn die Verarbeitungslandschaft bekannt ist.[2009]

1539 Das *Verarbeitungsverzeichnis mit der sog. Inventarisierungspflicht* von Personendatenverarbeitungsprozessen, vgl. Art. 30 DSGVO und Art. 12 nDSG, ist ein innovatives Novum des aktuellen Datenschutzrechts. Mehrere Anbieter haben mittlerweile entsprechende Computerprogramme auf den Markt gebracht. Sehr grosse Unternehmen entwickeln ihre eigenen Scanner-Verfahren entsprechend ihrer Geschäftsprozesse. Das Instrument ist mit einem beträchtlichen administrativen Aufwand verbunden. Die relativ reibungslose Verabschiedung im Zuge der Totalrevision des DSG vermag zu überraschen, zumal in der Schweiz datenschutzrechtliche Massnahmen regelmässig mit dem Argument bekämpft wurden,

2009 Insofern auch Passadelis/Roth, Jusletter 4. April 2016, N 78.

dass diese einen unzumutbaren Aufwand für die Verarbeitenden bringen würden. Auch hierzulande scheint es ausser Frage zu stehen, dass datenschutzkonformes Handeln nur dann möglich ist, wenn die Topografie der Personendatenverarbeitungsprozesse in einer Art Landkarte erfasst wurde. Das Verarbeitungsverzeichnis ist als eine Innovationsleistung des Gesetzgebers und damit als eine Errungenschaft für das Datenschutzrecht und seine faktische Verwirklichung zu taxieren. Die Einhaltung des Datenschutzrechts wird damit effektuiert.

Mit dem neuen, rechtlich innovativen Instrument des Verarbeitungsverzeichnisses wird zugleich sichtbar, inwiefern dem Datenschutzrecht inklusive seiner stabil etablierten materiellen Grundsätze durch die Entwicklung eines *prozeduralen Instruments* Nachachtung verschafft werden kann und soll. Zugleich ist das Instrument illustrativ dafür, dass die Entwicklung neuer technischer Programme einen wirkungsmächtigen Beitrag zur Gewährleistung der Vorgaben eines Rechtsgebietes liefert, das von den Technologien auf den Prüfstand gestellt wird. 1540

Rechtlich betrachtet ist die Erstellung eines Verarbeitungsverzeichnisses vorab eine *eigenständige Pflicht* gemäss DSGVO und totalrevidiertem DSG. Die Missachtung kann Sanktionen nach sich ziehen, vgl. Art. 83 Abs. 4 lit. a DSGVO. In der Schweiz wird die Verletzung der Verzeichnispflicht nicht in den strafrechtlichen Bussenkatalog gemäss Art. 60 f. nDSG aufgenommen. Eine behördliche Anordnung durch den EDÖB zur Durchsetzung ist denkbar, vgl. Art. 49 ff. nDSG. 1541

Darüber hinaus stellt das Verarbeitungsverzeichnis ein Hilfsinstrument dar, das in Anbetracht seiner Bedeutung als *conditio sine qua non und Basis-Analyse-Instrument für die gesamte Datenschutz-Compliance* zu qualifizieren ist. Es dient vorgeschaltet dem Scope-Assessment bezüglich des Anwendungsbereichs der DSGVO, vgl. Art. 3 DSGVO, aber auch der Qualifikation der Rollen als Verantwortliche resp. Auftragsverarbeiter.[2010] Zudem ist es unverzichtbar zur Gewährleistung weiterer Pflichten, namentlich der Einhaltung der allgemeinen Verarbeitungsgrundsätze gemäss Art. 5 DSGVO resp. Art. 6 und Art. 8 nDSG. Denn wie sollen z. B. die Transparenzvorgaben oder der Zweckbindungsgrundsatz eingehalten werden, wenn unbekannt ist, wer welche Personendaten zu welchem Zweck in einer Organisation verarbeitet? 1542

Die *faktische Effektuierung* der neuen Datenschutzerlasse wird über weitere Instrumente zum Paradigma verdichtet: Bereits im Rahmen der Präsentation des langen Arms der DSGVO mit ihrer extraterritorialen Wirkung wurde dargelegt, dass z. B. unter dem Niederlassungskriterium nicht die formelle Registrierung einschlägig ist. Auch die Schweiz sieht über Art. 3 nDSG und seine international privatrechtlichen Bestimmungen eine extraterritoriale Wirkung vor. Unter der 1543

2010 Zur Notwendigkeit dieser Analyse EDPB, Consultation Paper Scope, 4.

DSGVO sind die faktischen Geschäftsaktivitäten zur Beurteilung relevant, womit das neue Datenschutzrecht auch in diesem Punkt den Fokus auf *Realitäten* legt.

1544 Dasselbe gilt für die *Rollendefinierung und -fixierung:* Sie ist aufgrund der realen Verhältnisse und unter Berücksichtigung sämtlicher konkreter Umstände vorzunehmen.[2011]

1545 Viele der datenschutzrechtlichen Pflichten wie z. B. die Data Breach Notification, aber auch das Auskunftsbegehren des Datensubjektes bedingen die Entwicklung und Implementierung entsprechender Prozesse und Organisationsstrukturen resp. -zuständigkeiten. Mit ihrer Schaffung wird dem Datenschutzrecht in der Realität weiter Griffigkeit verliehen.

1546 Die DSGVO wie auch die Totalrevision sind massgeblich vom Ziel motiviert, datenschutzrechtliche Vorgaben *in der Realität* wirksam werden zu lassen und das Datenschutzrecht seiner rein formellen Existenz in Papierform zu entheben. Der Aspekt wird sogleich weiter ausgebreitet. Inkludiert werden mehrere neue Ansätze, die als Strukturmerkmale dem neuen Datenschutzrecht signifikant ergänzende Charakteristika verleihen: Sowohl der Compliance-, Governance- und Accountability-Ansatz als auch der risikobasierte Ansatz sowie derjenige der starken Behördenhand leisten einen Beitrag, um das Datenschutzrecht faktisch wirksam werden zu lassen. Damit soll ein Schlusspunkt hinter eine Datenschutzgesetzgebung gesetzt werden, die weitgehend als Symbolgesetzgebung bezeichnet werden musste.

2011 (Alleiniger) Verantwortlicher ist, wer über Zweck und Mittel der Personendatenverarbeitung entscheidet, also wesentliche Entscheidungsbefugnisse hat, warum, wofür und wieweit verarbeitet wird. Relevant ist zudem ein Weisungs- und Aufsichtsrecht, aber auch das Auftreten nach aussen. Der Controller resp. Verantwortliche ist Adressat der umfassenden Pflichten gemäss DSGVO. Sind mehrere Parteien in Personendatenverarbeitungen involviert, kann es sich um eine gemeinsame Verantwortlichkeit oder aber um ein Auftragsverhältnis handeln. Gemäss Art. 4 Nr. 7 und Art. 26 DSGVO sind gemeinsame Verantwortliche (Co-Controller) möglich. In der Praxis sind Co-Controller-Konstellationen gerade in Konzernen und Unternehmensverbünden häufig. Sind mehrere Parteien an Personendatenverarbeitungen beteiligt, kann es sich indes auch um ein Auftragsverhältnis handeln. Auftragsverarbeiter (Processors) sind natürliche oder juristische Personen oder Stellen, die Personendaten im Auftrag («on behalf») des Verantwortlichen verarbeiten. Den Auftragsverarbeiter treffen nach DSGVO bei direkter Anwendbarkeit deutlich mehr direkte Pflichten im Vergleich zur EU-Datenschutzrichtlinie und dem aktuellen DSG. Er kann für Pflichtverletzungen direkt sanktioniert werden. Im Rahmen der Auftragsverarbeitung ist zudem an die indirekte Anwendbarkeit gemäss Art. 28 Abs. 3 DSGVO zu erinnern. Hier geht es in erster Linie um die Konstellation, in der ein EU-Verantwortlicher einen Non-EU-Auftragsverarbeiter und nicht direkt unter die DSGVO fallenden Auftragsverarbeiter beizieht. Festzuhalten ist, dass nach DSGVO und auch nach nDSG der Auftragsverarbeiter stärker in die Pflicht genommen wird; zum Ganzen WP 29, Concept of controller, 1, 9 f., 11, 16, 18, 27 und 32; Hartung, Beck-Komm.-DSGVO, Art. 4 N 6 ff. und Art. 28 N 26 ff.; BLD, FAQ Auftragsverarbeitung, 1 ff.; CNIL, Guide sous-traitant, *passim*; insofern auch Passadelis/Roth, Jusletter vom 4. April 2016, N 46 ff.

2.6. Zum Compliance-, Governance- und Accountability-Ansatz

2.6.1. Allgemeines

Dieser neue Ansatz wurde bereits an verschiedenen Stellen erwähnt. In Anbetracht seiner Relevanz soll er einen *eigenen Titel* erhalten. Es geht um die Entwicklung, wonach die jüngsten Rechtsneuerungen den *Datenschutz als Compliance- und Governance-Aufgabe installieren*. Die Gewährleistung der Datenschutz-Compliance wird in den kommenden Jahren und Jahrzehnten markant an Bedeutung gewinnen. Damit wird sie sich in die Reihe der etablierten Compliance-Aufgaben, insb. die Geldwäscherei-Compliance, die Kartellrechts-Compliance oder die korrekte Rechnungslegung einfügen. Mit den Begriffen «Datenschutz-Compliance» und «Datenschutz-Governance» sind sämtliche Massnahmen gemeint, die zu ergreifen sind, um die datenschutzkonforme Personendatenverarbeitungen zu gewährleisten.[2012] Über die Einhaltung der Verarbeitungsgrundsätze gehören dazu die Etablierung von organisatorischen Zuständigkeiten, die Entwicklung von Prozessen, Dokumentationen, Schulungen, technischen Massnahmen usf. 1547

Verbunden wird das Compliance- und Governance-Paradigma in der DSGVO explizit mit entsprechenden *Dokumentations- und Rechenschaftspflichten*, was auch als *Accountability-Ansatz* bezeichnet wird.[2013] 1548

Unter dem Dachbegriff des Compliance- und Governance-Ansatzes werden zahlreiche Massnahmen verschiedenster Natur und Couleur eingefangen. Dazu gehören gemäss Art. 24 DSGVO allem voran technische, bauliche, organisatorische und prozedurale sowie informationelle und schulische Massnahmen. Sie alle zielen auf die Einhaltung der mannigfaltigen datenschutzrechtlichen Pflichten und Vorgaben ab. Art. 24 DSGVO ist allgemeiner Natur; sein Verhältnis zu den weiteren, konkreten Pflichten der DSGVO lässt sich nicht trennscharf umreissen. So werden z. B. technische Massnahmen zwecks Datenschutzes weiter spezifisch durch die Normen über «privacy by design» resp. «privacy by default» erfasst, vgl. Art. 25 DSGVO. Unbestritten verleiht das Compliance- und Governance-Paradigma verbunden mit dem Accountability-Aspekt dem Datenschutzrecht konzeptionell eine neue Dimension sowie Bedeutung. Im Schweizer DSG ist das 1549

2012 Passadelis, NZZ vom 7. November 2019, NZZ-Verlagsbeilage, 3; eine gute Orientierungshilfe für die Praxis findet sich bei Kranig/Sachs/Gierschmann, *passim;* vgl. Raschauer, NomosKomm-DSGVO, Art. 24 N 1 ff.; sodann Pfaffinger/Balkanyi-Nordmann, Schweizer Bank Mai 2018, 21.

2013 Angesprochen sind Rechenschaftspflichten, vgl. auch Art. 5 Abs. 2 DSGVO; Herbst, BeckKomm-DSGVO, Art. 5 N 77 ff.; Hartung, BeckKomm-DSGVO, Art. 24 N 20; EDÖB, EU-DSGVO und die Schweiz, 1 ff., 8; Pfaffinger, in: Emmenegger (Hrsg.), 17 ff., 22; die Rechenschaftspflicht gilt auch mit Blick auf das Verarbeitungsverzeichnis, Organisationspflichten, und im Rahmen von Schadenersatzansprüchen; hierzu die einschlägige Kommentarliteratur.

Konzept nach seiner Totalrevision weniger explizit als in der DSGVO. Gleichwohl ist es ebenso im neuen DSG angelegt.

1550 Der Ansatz hängt untrennbar mit den datenschutzrechtlichen Vorgaben an sich zusammen und richtet sich auf deren Einhaltung. Damit knüpft er an die weiteren in diesem Teil beschriebenen Entwicklungstrends und -aspekte im Datenschutzrecht an. Zugleich dient er der Absicherung der tradierten Elemente, insb. der Einhaltung der materiellrechtlich fest verankerten Verarbeitungsgrundsätze. Zwei Aspekte sind hervorzuheben:

1551 *Erstens:* Die Installierung des Datenschutzrechts im Compliance- und Governance-Portfolio verleiht *gerade auch dem vorangehend bezeichneten Ansatz der faktischen Effektuierung* Nachdruck. Der Datenschutz mit seinen rechtlichen Vorgaben ist *proaktiv in die DNA* der jeweiligen Organisation zu integrieren. Hierbei sind es mehrere ausdifferenzierte Massnahmen, die einen Beitrag dazu leisten, dass der Datenschutz in der Realität wirksam wird.[2014]

1552 *Zweitens:* Der unter diesem Titel präsentierte Ansatz ist als *Kontrapunkt zu der bisher individual- resp. subjektivrechtlichen sowie persönlichkeits- und deliktsrechtlichen Prägung des Datenschutzrechts* zu beschreiben. Bereits die Ausführungen unter dem Titel der Betroffenenrechte sowie der neueren Instrumente zur faktischen Verwirklichung datenschutzrechtlicher Vorgaben haben sichtbar gemacht, dass das neue Datenschutzrecht den bisher weitgehend in einer hegemonialen Stellung herrschenden Ansatz des Persönlichkeitsschutzes (für den privaten Bereich) relativiert resp. ergänzt. Der Subjektschutz und individualrechtliche Ansatz spielt zwar weiterhin eine wichtige Rolle und wurde, wie dargelegt, gestärkt und ausgebaut. Gleichwohl setzen die Neuerungen markante weitere Akzente, indem der Datenschutz im Katalog der Compliance- und Governance-Aufgaben figuriert. Neu werden die Verarbeitenden nachdrücklich und an erster Stelle in die Pflicht genommen, datenschutzkonform zu handeln. Eine reaktive und ebenso deliktsrechtlich verhaftete Konzeption des bisherigen Datenschutzrechts wird überwunden oder zumindest aufgebrochen. Fokus des Datenschutzrechts ist nicht mehr isoliert das – in einer analogen Denkweise zu dem bei einem Autounfall verletzten Menschen – qua Personendatenverarbeitung verletzte Datensubjekt. Der Datenschutz gehört neu in das Compliance-Portfolio jeder personendatenverarbeitenden Stelle. Der bislang alleine tragenden Säule des Subjektschutzes wird eine starke weitere Säule zur Seite gestellt.

1553 *Drittens:* Durch die Vorgaben, wonach Datenverarbeitende stets in der Lage sein müssen, die Einhaltung datenschutzrechtlicher Vorgaben zu belegen, fin-

2014 Kritisch, ob die Neuerungen ebendies bewerkstelligen werden, Rosenthal/Vasella, digma 2018, 166 ff.; von einer Compliance-Bürokratie sprechen Vasella/Sievers, digma 2017, 44 ff., 48 f.; Pfaffinger/Balkanyi-Nordmann, Private – Das Geld-Magazin 2019, 22 ff., 23; Dies., RR-CO 2019, 2 ff., 3.

det die *datenschutzrechtliche Transparenz* eine neue Dimension. Neu müssen Verarbeitungsprozesse und Datenflüsse in einem Verzeichnis sichtbar gemacht werden. Massnahmen zur Gewährleistung der Datenschutzkonformität (resp. der Entscheidungsprozess für den Verzicht auf bestimmte Massnahmen) sind *stets zu dokumentieren*, um Rechenschaftspflichten nachkommen zu können. Das Ziel, Transparenz zu erhöhen, ist damit nicht eindimensional im Sinne einer individualrechtlich ausgerichteten Zielrichtung zu verstehen. Zwar sollen die Transparenzvorgaben die Datensubjekte über Personendatenverarbeitungen ins Bild setzen, womit die persönlichkeits- und individualrechtliche Anknüpfung des Datenschutzes verankert wird. Neu sollen Personendatenverarbeitungsprozesse sowie getroffene Massnahmen, Strukturen und Prozesse bewusst und in nachvollziehbarer Weise rechtskonform gestaltet werden – durch die personendatenverarbeitenden Stellen und Organisationen. Das ist als zentrales Element zu taxieren, um Vertrauen zu etablieren, das durch das Agieren gerade der Internetgiganten mit ihrer Monopolstellung verspielt wurde.

Bezeichnend für diese Entwicklung ist die Neuschöpfung des *Verantwortlichen*. 1554
Die (neue) «Hauptperson» im Datenschutzrecht ist der «Verantwortliche». Sowohl die DSGVO als auch das neue DSG sehen die Figur – neben dem Auftragsverarbeiter und dem Datensubjekt – vor, vgl. Art. 4 Ziff. 7 i. V. m. Art. 24 ff. DSGVO (u. U. gemeinsame Verantwortung, Art. 26 DSGVO) und Art. 5 lit. j nDSG. Auf sie richtet sich in erster Linie die Aufmerksamkeit des Datenschutzgesetzgebers sowie der durchsetzenden Behörde. Ein Abwarten, bis ein Datenschutzsubjekt eine datenschutzrechtliche Persönlichkeitsverletzung im Einzelfall geltend macht – was kaum je geschieht –, genügt den neuen regulatorischen Konzepten nicht mehr.

Im Zentrum des nunmehr das Datenschutzrecht mitprägenden Compliance- und 1555
Governance-Ansatzes steht Art. 24 DSGVO, zudem Art. 5 Abs. 2 DSGVO. Art. 24 DSGVO verlangt unter dem Titel der Verantwortung des Verantwortlichen *angemessene Datenschutzvorkehrungen* und damit eine eigentliche Datenschutz-Compliance, welche *sämtliche betrieblichen Massnahmen organisatorischer, rechtlicher, technischer und baulicher Art* meint.[2015] Art. 24 DSGVO ist generellen Charakters. Er verpflichtet den Verantwortlichen in Abs. 1 allgemein zur umfassenden Datenschutz-Compliance.[2016] Obschon die Totalrevision des DSG kein Pendant zu dieser Bestimmung vorsieht, wird die *Data Governance* auch hierzulande zu einer wichtigen Aufgabe gerade der privatwirtschaftlichen Unternehmen arrivieren. Folglich gewinnen die Dokumentations- und Rechenschaftspflicht – die Accountability – sowie das Audit an Bedeutung. Die DSGVO, aber nicht das totalrevidierte DSG, sieht neu explizit eine Rechenschaftspflicht vor,

2015 Raschauer, NomosKomm-DSGVO, Art. 24 N 10.
2016 Ders., a. a. O.

vgl. Art. 5 Abs. 2 sowie Art. 24 Abs. 1 DSGVO. Nach dem sog. *Accountability-Ansatz* müssen die Verantwortlichen stets in der Lage sein, den Nachweis zu erbringen, dass ihre Verarbeitungshandlungen die datenschutzrechtlichen Vorgaben einhalten, woraus auch eine entsprechende Dokumentationspflicht resultiert. Der Ansatz, dessen Bedeutung nicht gänzlich zutreffend als Beweislastumkehr beschrieben wird, macht es für die datenverarbeitenden Stellen unumgänglich, sich umfassend und grundlegend mit ihren Personendatenverarbeitungsprozessen und ihrer Konformität mit dem Datenschutzrecht auseinanderzusetzen.

1556 Die erwähnten Ansätze und Umsetzungsinstrumente sind in einem jungen Rechtsgebiet, in dem viele Fragen offen sind, eine *Hilfestellung* für die Verarbeitenden. Sie liessen sich als Entlastungsstrategie beschreiben und keineswegs bloss als Traktieren vonseiten des Gesetzgebers wahrnehmen.[2017] Vielmehr sollten sie als Massnahmen verstanden werden, die nicht nur einen Beitrag zur Effektuierung des Datenschutzrechts, sondern auch zum leichteren Navigieren in einer teilweise unklaren Landschaft leisten:

1557 Der Nachweis, dass man sich mit einer datenschutzrechtlichen Herausforderung befasst hat – beispielsweise die Prüfung, ob man in den Anwendungsbereich der DSGVO fällt –, und ein Argumentarium, warum welche Massnahmen (nicht) ergriffen wurden, versetzen einen nicht nur gegenüber den Behörden, sondern auch gegenüber den Datensubjekten in eine ungleich bessere Position als Untätigkeit, Ignoranz oder Optimieren zulasten des Datenschutzrechts.

1558 Mit den Neuerungen, welche die Verantwortung für den Datenschutz an erster Stelle den jeweiligen Verarbeitenden zuweisen und die damit einen Kontrapunkt zur abwehrrechtlichen und schadensrechtlichen Perzeption der persönlichkeitsrechtlichen Anknüpfung setzen, wird erneut die *systemische Dimension des Datenschutzes* sichtbar.

1559 Obschon die DSGVO – anders als das (n)DSG – kein duales System der datenschutzrechtlichen Vorgaben vorsieht, ist hier eine bereichsspezifische Konturierung auszumachen. Denn die Verantwortung wird im Sinne einer *Eigenverantwortung für die Data Governance den datenverarbeitenden Akteuren zugewiesen*. Das sog. Housekeeping für die eigene Datenschutzkonformität wird in die Hände des Verursachers, des Verantwortlichen gelegt. Nimmt man die Privatunternehmen als datenverarbeitende Organisationen, so stärkt die DSGVO ihre *Eigen- und Selbstverantwortung* für die Einhaltung des Datenschutzes durch diese selbst. Sie haben Zuständigkeiten, Organisationen, Prozesse und Dokumente zu schaffen, welche der Einhaltung datenschutzrechtlicher Vorgaben zum Durchbruch verhelfen.

2017 Dessen ungeachtet wird die hohe Bedeutung des Datenschutzrechts und seiner Einhaltung mit Blick auf die Sicherung robuster Institutionen spätestens im letzten Kapitel dieser Arbeit sichtbar.

Eine erschöpfende Darstellung sämtlicher Massnahmen, welche für eine umfassende Datenschutz-Compliance geboten sind, ist an dieser Stelle weder möglich noch sinnhaft. Insofern sei auf die mittlerweile etablierte Kommentarliteratur namentlich zur DSGVO verwiesen. Selektiv werden einige Elemente herausgegriffen, die sich innerhalb des Compliance-Titels zu eigenständigen Charakteristika des neuen Datenschutzrechts verdichten. 1560

2.6.2. *Zum Ausbau prozeduraler und organisatorischer Elemente*

Innerhalb des Entwicklungstrends, wonach das Datenschutzrecht als Compliance-Aufgabe ausgeformt wird, lässt sich die *Weiterentwicklung organisatorischer und prozeduraler Instrumente feststellen*.[2018] Die eigentlichen Neuerungen der jüngsten Revisionswellen bestehen damit *weniger in materiellrechtlichen Innovationen* – im Kern bleiben es die Verarbeitungsgrundsätze, die das materielle Datenschutzrecht konstituieren. Vielmehr liegt ein Akzent auf Organisations- und Prozessaspekten, welche die Implementierung des Datenschutzes in die datenverarbeitende Institution bewerkstelligen sollen. 1561

Am Anfang steht wiederum das bereits präsentierte *Verzeichnis über die Verarbeitungstätigkeiten*, vgl. Art. 30 DSGVO und Art. 12 nDSG. Es ist Herzstück der Data Governance und bildet das Basis-Instrument zur Verwirklichung der meisten datenschutzrechtlichen Vorgaben. Das Inventar ist ein Basisinstrument, um die datenschutzrechtlichen Vorgaben, insb. die allgemeinen Verarbeitungsgrundsätze, einhaltbar zu machen. Damit lässt es sich als *Navigationsinstrument* mit dem Ziel des datenschutzrechtskonformen Handelns beschreiben. 1562

Unter dem neuen Recht und mit dem Ziel der Implementierung eigentlicher Datenschutz-Compliance kommt *organisatorischen Aspekten* eine zentrale Rolle zu. Insofern sind zunächst der interne Datenschutzbeauftragte resp. die Datenschutzberaterin zu erwähnen. Die Bestellung ist unter den Vorgaben gemäss Art. 37 DSGVO, nicht aber nach Art. 10 nDSG zwingend. Gleichwohl genügt die Funktion in organisatorischer Hinsicht nicht, um die Integration des Datenschutzes in die DNA der Verarbeitenden zu gewährleisten. Vielmehr bedarf es der Etablierung einer angemessenen *Organisationsstruktur*. Eine Vorstellung, wonach es mit der Besetzung der Funktion des internen Datenschutzbeauftragten getan ist und dieser im Alleingang die Implementierung des Datenschutzes gewährleisten kann, geht fehl. Dem Datenschutzbeauftragten kommt zwar eine wichtige Rolle bei der strategischen Planung der zu treffenden Massnahmen, der Beratung und Schulung sowie Kommunikation zu. Eine umfassende Datenschutz-Compliance und 1563

2018 Präzisierend zur Begrifflichkeit der Prozeduralisierung Donos, 126 ff., wobei der Autor unter Integration entsprechender Erkenntnisse das Recht auf informationelle Selbstbestimmung nicht als subjektives Recht verstanden wissen will.

Data Governance ist allerdings darüber hinaus auf den tone from the top angewiesen; weiter kommt den Linien und Bereichen hohe Relevanz bei der Implementierung des Datenschutzes zu. Auch im Bereich des Datenschutzrechts etabliert sich in der Praxis das für andere Compliance-Themen entwickelte «three lines of defense»-Modell.[2019] Ein Element ist hierbei, dass je nach Position und Aufgabe der Mitarbeitenden datenschutzrechtliche Kenntnis und Sensibilität vermittelt wird. Solche Schulungen finden rollenspezifisch statt, wobei ein Mindestbewusstsein bei jeder einzelnen Mitarbeiterin sicherzustellen ist.

1564 Dass die datenschutzrechtlichen Neuerungen das *Organisationsregime* zu einer tragenden Säule machen, wird anhand zusätzlicher Elemente sichtbar, so anhand der Neuordnung der *Rolle des Auftragsverarbeiters*, Art. 28 DSGVO und Art. 9 nDSG, sowie seiner Pflichten. Die DSGVO unterwirft den Auftragsverarbeiter weitgehend der Einhaltung derselben Rechte und Pflichten, wie sie der Verantwortliche selbst beachten müsste. Zudem haben Verantwortlicher und Beauftragter einen Vertrag zu schliessen, vgl. Art. 28 Abs. 3 DSGVO, und das *entsprechende Verhältnis* einer verbindlichen und präzisierten *lex contractus* zu unterwerfen. Die Neuregelung will verhindern, dass durch Delegation an eine andere Person datenschutzrechtliche Vorgaben «verwässert» werden resp. dass deren Einhaltung der Intransparenz durch Inklusion einer weiteren, externen Person anheimfällt.[2020]

1565 Unter dem Titel der Datenschutz-Governance sowie dem Trend, organisatorische Vorgaben zwecks Effektuierung des Datenschutzes auszubauen, ist die Figur der EU-Vertreterin, Art. 27 DSGVO, zu erwähnen. Für die Konstellationen extraterritorialer Anwendung der DSGVO gemäss Art. 3 Abs. 2 DSG ist eine Person zu bezeichnen, wobei die Umsetzung in der Schweiz kontrovers diskutiert wurde.[2021] Verabschiedet wurde die Totalrevision mit einem Pendant in Art. 14 nDSG.

1566 Zur rechtskonformen Umsetzung von Betroffenenrechten und z. B. deren Auskunfts- oder Löschungsbegehren, aber auch der Data Breach Notification sind ebenso entsprechende Zuständigkeiten und Prozesse zu definieren und implementieren.

1567 Im Rahmen der Anhebung der *organisatorischen Vorgaben* im Interesse einer wirksamen Implementierung datenschutzrechtlicher Vorgaben darf die Ausdifferenzierung sowie Verschärfung behördlicher Kompetenzen nicht unerwähnt blei-

2019 Vgl. Pfaffinger/Balkanyi-Nordmann, RR-CO 2019, 2 ff.; zum Datenschutz als Chefsache Reding, digma 2001, 124 ff., 124.

2020 Vgl. Ingold, NomosKomm-DSGVO, Art. 28 N 1 ff., N 5 ff. und N 11 ff.; WP 29, Opinion 1/2010 on the concepts of «controller» and «processor» 00264/10/EN; zum Verantwortlichen sowie Auftragsverarbeiter; hierzu auch Rosenthal/Epprecht, in: Emmenegger (Hrsg.), 127 ff.

2021 Hierzu Hartung, BeckKomm-DSGVO, Art. 27 N 1 ff.; Pfaffinger, in: Emmenegger (Hrsg.), 17 ff., 32 f.

ben. Gemäss den *neuen behördlichen Organisation* nach DSGVO wacht diese über die Einhaltung datenschutzrechtlicher Vorgaben, berät, informiert, nimmt Dokumentationen entgegen und erlässt unter Umständen Verfügungen, auch im Sinne von Sanktionen. Zudem ist die *Kooperation zwischen den Behörden* deutlich differenzierter gestaltet; zu nennen sind unter dem Regime der DSGVO nicht nur die Vielfältigkeit der mit datenschutzrechtlichen Fragen betrauten Stellen, sondern ebenso die Koordinierung von Zuständigkeitsfragen und Kooperationspflichten.[2022]

1568 Auch die Totalrevision bringt eine Anhebung und Verschärfung der vonseiten der Behörden verhängbaren Massnahmen und Sanktionen, vgl. in Bezug auf den EDÖB Art. 49 ff. nDSG und hinsichtlich der strafrechtlichen Bussen, die durch die kantonalen Behörden verhängt werden, Art. 60 ff. nDSG.

1569 Trotz der «gestärkten Hand der Behörden» ist festzustellen, dass die beschriebenen Neuerungen allesamt – selbst im Monismus der DSGVO – zugleich einen *systemischen Ansatz* integrieren, indem sie die *Eigenverantwortung* der jeweils verarbeitenden Verantwortlichen akzentuieren. Die datenschutzrechtliche Handlungsverantwortung ist an ein erweitertes System resp. Milieu oder eine Branche angebunden, woraus weitere, kontextspezifische Datenschutzvorgaben resultieren.

1570 In diesem Zusammenhang sind abrundend die Instrumente der Selbstregulierung zu nennen. So die *Zertifizierungsverfahren* gemäss Art. 43 DSGVO und Art. 13 nDSG mit ausführender Verordnung sowie die *branchenspezifischen Verhaltenskodizes,* vgl. Art. 40 DSGVO und Art. 11 nDSG, mit den ebenda vorgesehenen Empfehlungen der guten Praxis. Bei diesen Instrumenten der Selbstregulierung handelt es sich um solche, welche den systemischen Schutzaspekt durch und im Datenschutz anerkennen. Eine fundierte Auseinandersetzung mit ihrer Tauglichkeit würde eine eigenständige Untersuchung verdienen. An dieser Stelle sei immerhin attestiert, dass diese dem in dieser Arbeit entwickelten Paradigma des Systemschutzes als eine den Subjektschutz ergänzende resp. unter- oder überlagernde Kernaufgabe datenschutzrechtlicher Regelungen zumindest *prima vista* zuträglich sind.[2023]

2022 Vgl. insb. Art. 50 ff. DSGVO und Art. 49 ff. sowie Art. 60 ff. nDSG.

2023 Indes ebenso kritisch Pärli, digma 2011, 67 ff.; zur jüngsten Stärkung deskriptiv und ohne Evaluierung Hofmann/Meyer, Expert Focus 2017, 424; zu den jüngsten Entwicklungen insofern auch <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/datenschutzzertifizierung.html> (zuletzt besucht am 20. September 2021).

2.6.3. Zum Datenschutz qua Technik

1571 Das Verhältnis zwischen Technologie und Recht ist komplex, wobei an dieser Stelle kein rechtstheoretischer Beitrag geleistet wird.[2024] Nachfolgend wird lediglich ein weiterer Trend jüngster datenschutzrechtlicher Neuerungen beschrieben. Er erinnert an ein homöopathisches Rezept, wonach «Gleiches mit Gleichem» zu behandeln ist. Technologien sind demnach nicht nur Gefährder, sondern auch Garanten des Datenschutzrechts.

1572 Parallel zur Stärkung des Organisations- und Prozessregimes zur Effektuierung des Datenschutzes tritt die erhöhte Bedeutung *technischer Massnahmen*. Illustrativ für die Verknüpfung beider Stossrichtungen (Organisation und Technik) sind die gemäss Art. 32 Abs. 1 DSGVO und Art. 7 nDSG verlangten organisatorischen und technischen Massnahmen (TOM). Sie dienen der Gewährleistung der Sicherheit der Daten resp. der Verarbeitung.[2025]

1573 Anknüpfend an die Bedeutung der Organisationsstruktur stellen sich unternehmensintern anspruchsvolle Koordinations- und Abgrenzungsfragen hinsichtlich der Verantwortlichkeiten zwischen «Security», Datenschutzbeauftragtem, Risk Management sowie Legal und Compliance.

1574 Für den *Datenschutz qua Technik* sind mehrere Bestimmungen einschlägig. So lautet der Auftrag gemäss Art. 24 DSGVO ebenso, umfassende Datensicherheitsmassnahmen nach dem Stand der Technik zu implementieren. Dieser Auftrag wird an anderer Stelle präzisiert, u. a. in Art. 25 und Art. 32 DSGVO.[2026] Art. 25 DSGVO verankert die sog. «privacy by design» und «privacy by default», also die Gewährleistung des Datenschutzes durch Technikgestaltung sowie datenschutzfreundliche Voreinstellungen.[2027] Auch die Schweiz widmet besagten Massnahmen spezifische Bestimmungen, vgl. Art. 7nDSG. Die Bestimmung steht unter dem Titel «Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen».

1575 Der Grundsatz der Datensicherheit bildet einen festen Bestandteil der Datenschutzregulierung, vgl. Art. 5 lit. f DSGVO sowie Art. 32 DSGVO und Art. 8

2024 Hierzu Nissenbaum, Berkeley Tech. L.J. 2011, 1367 ff.; Gruber, *passim*.
2025 Hierzu Kessler/Oberli, CB 2020, 89 ff., 94.
2026 Raschauer, NomosKomm-DSGVO, Art. 24 N 9.
2027 Vgl. Enisa, Privacy by design in big data; Leitfaden der spanischen Datenschutzbehörde: <https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf> (zuletzt besucht am 30. April 2021); Reber, 41 ff.; zur Relevanz im Rahmen der Nutzung einer künstlichen Intelligenz in Bewerbungsverfahren Herdes, CB 2020, 95 ff., 96; als Elemente des Risikomanagements Kessler/Oberlin, CB 2020, 89 ff., 93 f.; Niemann/Scholz, in: Peters/Kersten/Wolfenstetter (Hrsg.), 109 ff., insb. 113 ff.; zu «privacy by design» vgl. z. B. Cavoukian, *passim*; die Autorin beschreibt mehrere Prinzipien und Charakteristika von «privacy by design», z. B. die proaktive anstelle einer reaktiven, die präventive anstelle einer reparatorischen Natur; hierzu auch Cavoukian/Chibba/Williams/Ferguso, Jusletter IT vom 21. Mai 2015, N 3 ff.

nDSG. Die Gewährleistung der Datensicherheit gemäss Art. 8 nDSG findet eine Konkretisierung auf Verordnungsstufe. Es handelt sich um Pflichten des Bearbeiters (neu: des Verantwortlichen resp. Auftragsverarbeiters), welche sich nicht nur auf die Datenschutzvorgaben und Verarbeitungsgrundsätze an sich richten, sondern wesentlich auch auf die sog. Informationssicherheit.[2028] Damit geht es u. a. um Massnahmen zum Schutz vor Angriffen und Bedrohungen wie Hacking, Manipulation, Verlust usf. Sicherzustellen sind die Vertraulichkeit (verhindert unbefugte Weiterverbreitung), die Verfügbarkeit (Zugriff, wenn benötigt) und Integrität (keine unbefugte Veränderung) von Personendaten sowie der Schutz vor unbefugter oder zufälliger Vernichtung, unbefugtem oder zufälligem Verlust, technischen Fehlern, Fälschung, Diebstahl, widerrechtlicher Verwendung, unbefugtem Ändern, Kopieren, Zugreifen, Bearbeiten.[2029]

Zur Gewährleistung besagter Aspekte hat der Bearbeitende angemessene technische (und organisatorische) Massnahmen zu ergreifen. Als angemessen gelten Massnahmen, wenn der Zweck der Datenbearbeitung, die Art und der Umfang der Datenbearbeitung, eine Einschätzung der möglichen Risiken für die betroffenen Personen sowie der gegenwärtige Stand der Technik berücksichtigt wurden.[2030] Im Zusammenhang mit dem Ergreifen angemessener Sicherheitsmassnahmen findet eine risikobasierte Betrachtungsweise statt. 1576

Der EDÖB hat insofern einen Leitfaden erlassen.[2031] Was zu den technischen und organisatorischen Massnahmen gehört, führt er in der noch nicht revidierten Fassung Art. 9 VDSG aus. Dazu gehören die Zugangskontrolle (Personen, z. B. mittels Badge), die Personendatenträgerkontrolle (Kontrolle von Trägermedien wie Papier oder Memorystick), die Transportkontrolle (z. B. Schutz von Daten bei Übermittlung mittels Passwort), die Bekanntgabekontrolle (der Empfänger muss identifizierbar sein und feststellbar), die Speicherkontrolle (sie soll unbefugte Eingaben und Änderungen verhindern), die Benutzerkontrolle (Firewalls), die Zugriffskontrolle (Beschränkungen durch Zugriffsrechte) sowie die Eingabekontrolle mit ihrer Nachvollziehbarkeit. Die Aufgaben und Pflichten überschneiden sich teilweise. Technische Massnahmen sind heute ein zentrales Instrument, um datenschutzrechtliche Vorgaben zu implementieren. Als weitere Elemente sind technikbasierte Anonymisierungs- und Pseudonymisierungsprozesse, zudem die 1577

2028 Zum Verhältnis von Datenschutz und Informationssicherheit Schnabl, Jusletter IT vom 24. Mai 2018.

2029 Vgl. Hussein, in: Passadelis/Rosenthal/Thür (Hrsg.), § 3 N 3.100 ff.; vgl. die jüngst ebenso revidierte Datenschutzverordnung.

2030 In Bezug auf die DSGVO Mantz, NomosKomm-DSGVO, Art. 32 N 9 ff.

2031 EDÖB, Leitfaden zu den technischen und organisatorischen Massnahmen zum Datenschutz vom August 2015, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/technische-und-organisatorische-massnahmen-des-datenschutzes.html> (zuletzt besucht am 30. April 2021).

Entwicklung automatisierter Löschungsprozesse zur Gewährleistung des Verhältnismässigkeitsgrundsatzes zu nennen.

2.7. Zum risikobasierten Ansatz

1578 Die Angemessenheit der gerade vorgestellten Massnahmen der Datensicherheit sowie technischer Massnahmen misst sich an Risikoerwägungen. Es ist nicht unwesentlich die Beurteilung des Risikos für das betroffene Datensubjekt, an dem sich dieser Ansatz mitausrichtet. Gleichwohl wird, an den Compliance- und Governance-Aspekt mit seinen Unterfacetten anknüpfend, ein risikobasierter Ansatz allgemeiner und verstärkt in das Datenschutzrecht integriert. Mit diesem wird die Aufgabe intensiviert, präventiv und proaktiv mitigierende Massnahmen zu definieren und zu implementieren.

1579 So hat eine Risikoanalyse Basis für die Definierung der konkreten Pflichten gemäss Art. 24 Abs. 1 DSGVO zu sein.[2032] Die datenschutzrechtlichen Vorgaben und die zu treffenden Massnahmen hängen von bestimmten Risiken ab, die anhand der Natur der Personenangaben, der Anzahl betroffener Personen, einer Minderjährigkeit der Datensubjekte, aber auch des Kontextes, in dem Personendaten verarbeitet werden, skaliert werden. Für die Totalrevision des DSG wies Bundesrätin Keller-Sutter im Ständerat explizit auf diesen Ansatz hin, wobei Art und Weise der Bearbeitung risikobasiert relevant seien und nicht die Grösse der Unternehmen.[2033]

1580 In der Praxis wird folglich vom Risikomanagement bezogen auf die Data Governance gesprochen. Entsprechend spielen neben Verarbeitungsverzeichnissen auch Risikoverzeichnisse resp. Risikoanalysen für die Massnahmen, die im Rahmen der Datenschutz-Compliance zu treffen sind, eine zentrale Rolle.[2034]

1581 Der risikobasierte Ansatz verleiht dem Datenschutzrecht mit seinem bisherigen persönlichkeits-, abwehrrechtlichen und deliktsrechtlichen Ansatz *eine neue Ingredienz*. Zwar lässt sich der Aspekt bereits im bisherigen Recht nachweisen: Allem voran die Einteilung zwischen sog. gewöhnlichen und besonders schutzwürdigen Personenangaben sowie die hieran anknüpfenden milderen resp. strengeren Datenschutzvorgaben sind Ausdruck einer risikobasierten Herangehensweise.[2035]

2032 Hartung, BeckKomm-DSGVO, Art. 24 N 13 ff.; ebenso Raschauer, NomosKomm-DSGVO, Art. 24 N 18 ff.

2033 Das Schweizer Parlament, AB, Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse des Datenschutzes, Bern 2019, <https://par-pcache.simplex.tv/subject?themeColor=AA9E72&subjectID=48166&language=de> (zuletzt besucht am 30. April 2021).

2034 Vgl. Hartung, BeckKomm-DSGVO, Art. 24 N 13 ff. und Art. 25 N 20; wissenschaftlich findet sich das Vorgehen basierend auf einer Risikoanalyse mit Blick auf das Webtracking jüngst namentlich bei Wenhold, 95 ff.

2035 Von wissenschaftlicher Seite wurde eine Neukonzeptionierung des Datenschutzrechts als Risikorecht und damit eine Abkehr vom schadens- resp. deliktsrechtlichen Denken vorgeschlagen, na-

Auch die Vorgaben in Bezug auf die angemessenen Sicherheitsmassnahmen integrieren Risikoerwägungen.

Allerdings verleihen in den neuen Erlassen mehrere Normen und Instrumente dem Ansatz eine markante Dimension. Die risikobasierte Methodologie ist charakteristisch für den Compliance- und Governance-Bereich. Data Governance bedingt ein Risikomanagement in Bezug auf den Umgang mit Personendaten. Die Definierung der erforderlichen Massnahmen hängt von den spezifischen Datenverarbeitungen im Unternehmen sowie den verorteten Risiken ab, wozu namentlich der Kreis der betroffenen Personen gehört.[2036] Offensichtlich ist, dass Unternehmen und Stellen gewisser Kontexte und Branchen bezüglich ihrer datenschutzrechtlichen Risiken deutlich exponierter sind als andere: Eine Krankenversicherung oder eine Bank haben regelmässig höhere Datenschutzrisiken als ein Logistikunternehmen, das Warenspeditionen vornimmt. 1582

Eine vertiefende wissenschaftliche Untersuchung zum Datenschutzrecht als Risikorecht wäre von Interesse. An dieser Stelle mögen die folgenden weiteren Hinweise genügen: 1583

Erwähnenswert ist vorab Art. 24 Abs. 1 DSGVO und Erwägungsgrund 77, Art. 33 f. sowie Art. 35 DSGVO. Von besonderem Interesse ist die sog. Datenschutz-Folgenabschätzung, die ein datenschutzrechtliches Novum darstellt, vgl. Art. 35 DSGVO resp. Art. 22 nDSG. Die Schweiz hat sich im Vergleich zum Vorentwurf (Art. 16 VE-DSG) dem EU-Recht angeglichen, indem nunmehr beide Rechtstexte eine Datenschutz-Folgenabschätzung verlangen, wenn ein «hohes Risiko» besteht. Der Vorentwurf wollte ein erhöhtes Risiko genügen lassen. Ziel der Datenschutz-Folgenabschätzung ist es, Herausforderungen und Risiken der Verarbeitungsprozesse zu identifizieren. Die Art. 29 Working Party hat eine Guideline datierend auf den 4. April 2017 vorgelegt, welche für die Beurteilung der Frage, ob ein hohes Risiko vorliegt, konkretisierende Hinweise gibt:[2037] Aufgeführt sind zehn Kriterien, die durchzugehen sind, um die Risikohöhe zu identifizieren und ggf. in der Folge eine Datenschutz-Folgenabschätzung durchzuführen sowie den Konsultationspflichten nachzukommen. Liegen drei oder mehr Kriterien vor, ist von einem hohen Risiko auszugehen, wobei namentlich die Angehörigkeit einer Person zu einer bestimmten «Personengruppe» und damit die 1584

mentlich von Ladeur, Datenschutz 2.0 – Für ein netzgerechtes Datenschutzrecht, wobei der Wissenschaftler Grundbegriffe und -annahmen des Datenschutzrechts kritisch hinterfragt, abrufbar unter: <https://www.dailymotion.com/video/x36gpsg> (zuletzt besucht am 30. April 2021); vgl. diesen Ansatz auch bei Wenhold, 94 ff., 283; vgl. die Forderung auf Rekonzeptionalisierung des Datenschutzrechts basierend auf einer Analyse neuer Risiken Baeriswyl, digma 2003, 48 f.; hierzu weiter Donos, 179 ff.

2036 Raschauer, NomosKomm-DSGVO, Art. 24 N 12 und N 21.

2037 Abrufbar unter: <https://ec.europa.eu/newsroom/article29/items/611236> (zuletzt besucht am 20. September 2021).

Rollen der involvierten Personen und die Kontexte der Datenverarbeitung relevant werden (zur Relevanz des Kontextes für eine Neukonzeptionierung des Datenschutzrechts vgl. dritter Teil, IX. Kapitel, wo ein Recht auf informationellen Systemschutz vorgeschlagen wird). Spezifisch genannt werden spezielle Arten der Datenverarbeitungen wie systematische, umfassende Datenverarbeitung oder sehr tiefe und sehr breite Datensammlungen sowie Verarbeitungen von Personendaten von Minderjährigen, Arbeitnehmenden, Patientinnen usf. Kein hohes Risiko liegt vor, wenn keines oder nur eines, maximal zwei der qualifizierenden Kriterien der Guideline vorliegen, wenn eine Bearbeitung spezifisch auf einer weissen Liste rangiert. Sodann muss keine Datenschutz-Folgenabschätzung durchgeführt werden betreffend Bearbeitungen, die zwar als hohes Risiko gelten, allerdings bereits implementiert wurden. Mit anderen Worten entfaltet die Regelung keine Rückwirkung: Eine Datenschutz-Folgenabschätzung muss nicht nachgeholt werden. Sofern allerdings Prozesse oder Systeme wesentlich verändert oder neu eingeführt werden, ist eine Datenschutz-Folgenabschätzung durchzuführen, sofern diesen ein hohes Risiko immanent ist. Die Abfolge einer solchen Analyse wird von Art. 35 Abs. 7 DSGVO genauer fixiert: Vorbereitungsphase, Bewertungsphase, Massnahmenphase und Berichtsphase. Sofern der Verantwortliche zu dem Ergebnis kommt, dass eine Datenverarbeitung ein hohes Risiko darstellt, welches durch die Implementierung von besonderen Massnahmen nicht gedämmt werden kann, greifen Konsultationspflichten gemäss Art. 37 DSGVO resp. Art. 23 nDSG.

1585 Eine Orientierung an den im Rahmen der Datenschutz-Folgenabschätzung etablierten Kriterien ist im Zuge der Etablierung der unternehmensinternen *Compliance- und Datensicherheitsstrategie* hilfreich. Die Stärkung einer risikobasierten Herangehensweise im Datenschutzrecht zeigt sich nicht nur anhand des datenschutzrechtlichen Novums, der sog. *Datenschutz-Folgenabschätzung*.

1586 Auch die Datensicherheit, die durch geeignete technische und organisatorische Vorkehrungen zu gewährleisten ist, muss im Verhältnis zum *Risiko* angemessen sein, vgl. Art. 32 Abs. 1 DSGVO und Art. 8 nDSG. Zudem tragen der erwähnte Accountability-Ansatz sowie das Inventar dem risikobasierten Ansatz Rechenschaft.[2038] Mit ihnen werden Risiken qua Personendatenverarbeitung identifiziert sowie evaluiert, woraufhin risikobasiert Massnahmen zu definieren, priorisieren, implementieren, dokumentieren und kontrollieren sind. Inwiefern das Datenschutzrecht nicht nur unter dem Risiko des Aspekts der Persönlichkeitsverletzung, sondern in einem weiteren Verständnis gelesen werden wird, wird sich zeigen.

2038 Hierzu Pfaffinger/Balkanyi-Nordmann, Schweizer Bank Mai 2018, 21.

2.8. Zum Ansatz der starken Behördenhand

Ein letztes und bereits erwähntes Element, welches der Verwirklichung des Datenschutzrechts Nachachtung verschaffen will, liegt im Ausbau des Massnahmenkatalogs sowie der *Verschärfung der Sanktionen*. Weil damit dem Datenschutzrecht ein weiteres neues Charakteristikum verliehen wird, ist ein eigenständiger Titel angezeigt. Die bislang schwache behördliche Durchsetzung galt als ein Hauptgrund dafür, dass bisherige Datenschutzerlasse weitgehend toter Buchstabe blieben. 1587

Eine Gegenüberstellung von DSGVO und totalrevidiertem DSG zeigt eklatante Differenzen hinsichtlich der Gestaltung und Schlagkraft behördlicher Kompetenzen sowie Massnahmen. 1588

Nach der DSGVO verfügt die Aufsichtsbehörde gemäss Art. 83 Abs. 1 lit. i i. V. m. Art. 83 i. V. m. Art. 58 Abs. 1 lit. i DSGVO Bussen in einer Höhe, die eine neue Dimension in das Datenschutzrecht tragen. Es werden drei Gruppen von Verstössen kategorisiert und unterschiedlich bewertet: Der Verstoss gegen formelle Vorgaben der DSGVO wird gemäss Art. 83 Abs. 4 DSGVO mit max. 10 Millionen Euro oder im Fall eines Unternehmens mit zwei Prozent des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres – je nachdem, was höher ist – gebüsst. Noch höher liegen der Maximalsatz bei einem Verstoss gegen materielle Vorgaben und damit auch die Bearbeitungsgrundsätze. Gemäss Art. 83 Abs. 5 DSGVO sind Bussen von bis zu 20 Millionen Euro oder vier Prozent des gesamten weltweiten vorangegangen Jahresumsatzes denkbar. Sodann sieht Art. 83 Abs. 6 DSGVO vor, dass für nicht befolgte Anweisungen die Busse wie bei Abs. 5 bei maximal 20 Millionen Euro oder vier Prozent des gesamten im vorangegangenen Jahr weltweit erzielten Umsatzes liegt. Gemäss DSGVO sind nicht nur vorsätzliche Verletzungen der datenschutzrechtlichen Vorgaben durch die Verantwortlichen, sondern auch fahrlässige Verstösse zu büssen.[2039] Nicht zugelassen ist ein sog. Opportunitätsentscheid, sprich ein Ermessen der zuständigen Stelle, *ob* eine Busse bei einer vorsätzlichen oder fahrlässigen Verletzung auszusprechen sei oder nicht. Werden der objektive und subjektive Tatbestand erfüllt, so ist eine Busse zu erlassen. Das Busssystem ist damit strikt angelegt. Die Höhe der Busse allerdings hat verhältnismässig zu sein, wobei für deren Fixierung eine Ermessensentscheidung sämtliche Umstände des Einzelfalles zu berücksichtigen hat.[2040] 1589

2039 Vgl. WP 29, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 11 f.

2040 Vgl. hierzu Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bussgeldzumessung in Verfahren gegen Unternehmen vom 14. Oktober 2019, abrufbar unter: <https://www.datenschutzkonferenz-online.de/media/ah/20191016_bußgeldkonzept.pdf> (zuletzt besucht am 30. April 2021).

1590 Die Bussenhöhe für Datenschutzverstösse, die in eine Richtung gehen, die mit dem Kartellrecht assoziiert wird, stand ganz im Vordergrund der öffentlichen Diskussionen rund um die DSGVO. Seit ihrem Inkrafttreten und dem Ablauf ihrer Umsetzungsfrist sind zahlreiche Bussen ergangen.[2041] Eine erste Busse wurde, soweit ersichtlich, wohl von der österreichischen Datenschutzbehörde bereits im Spätsommer 2018 gesprochen.[2042] Ende 2019 wurden die ersten Millionen-Bussen erteilt.[2043] Im Dezember 2019 verhängte der deutsche Bundesdatenschutzbeauftragte eine Busse in der Höhe von 9.5 Millionen Euro gegen einen Telekom-Anbieter.[2044] Am 17. August 2019 wurde PwC Griechenland zu einer Busse in der Höhe von 150'000.00 Euro verurteilt.[2045]

1591 Die Zeiten, in denen Datenschutzverstösse maximal zu einem Reputations- und Vertrauensverlust infolge einer Presseberichterstattung führten, sind zumindest im Anwendungsbereich der DSGVO vorbei. Markante und abschreckende Sanktionen in Gestalt von nennenswerten Bussen (wie sie nunmehr die DSGVO vorsieht) erscheinen als wirksames Instrument, um der Einhaltung des Datenschutzrechts Nachdruck zu verleihen.[2046] Umgekehrt wurde gezeigt, dass auch (aber nicht nur) die schwache Ausgestaltung behördlicher Massnahmen mitursächlich dafür war, dass das Datenschutzrecht nur ungenügend respektiert wurde.

1592 Die DSGVO geht weit darüber hinaus, «scharfe Bussen» zu formulieren. Der umfassende und tiefgreifende Massnahmenkatalog der zuständigen Aufsichtsbehörde wird in Art. 58 DSGVO definiert. Die gesetzlich vorgesehenen behördlichen Kompetenzen sind facettenreich. Zunächst wird der Beratung hohe Bedeutung beigemessen.[2047] Unter Umständen gravierender als eine hohe Busse kann

2041 Sicherheitsforum, DSGVO-Sünder und ihre Strafzahlungen, Zürich 2019, <https://www.sicherheitsforum.ch/dsgvo-verstoesse-und-ihre-bussen/> (zuletzt besucht am 30. April 2021).

2042 Daten:recht, Erste Busse unter der DSGVO verhängt, Zürich 2018, <https://datenrecht.ch/erste-busse-unter-der-dsgvo-verhaengt/> (zuletzt besucht am 30. April 2021).

2043 Die Zeit online, Datenschutz, Millionenbussgeld gegen 1&1 verhängt, Hamburg 2019, <https://www.zeit.de/digital/datenschutz/2019-12/datenschutz-1-und-1-telekommunikation-interent-bussgeld> (zuletzt besucht am 30. April 2021); DataGuard, Warum die ersten DSGVO-Millionenstrafen verhängt wurden, München 2020, <https://www.dataguard.de/magazin/die-ersten-millionenstrafen-aus-der-dsgvo/> (zuletzt besucht am 30. April 2021).

2044 Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Möglichkeiten der Corona-Warn-App nutzen, Bonn 2021, <https://www.bfdi.bund.de/SiteGlobals/Modules/Buehne/DE/Startseite/Pressemitteilung_Link/HP_Text_Pressemitteilung.html> (zuletzt besucht am 30. April 2021).

2045 Noch bemerkenswerter als die Höhe der Busse – sie liegt keineswegs an der oberen Limite – ist der Inhalt des Entscheides. Er bezieht sich auf die Einwilligung als Erlaubnistatbestand im Regime eines prinzipiellen Verarbeitungsverbots und zwar im Beschäftigtenkontext. PwC hatte Mitarbeiterdaten auf Basis einer Einwilligung bearbeitet, was die griechische Datenschutzbehörde als «falsche» Rechtsgrundlage beurteilte. Die Bearbeitung sei unrechtmässig und intransparent, weil sie gerade nicht auf der «vermeintlichen» Einwilligung basiere. Gleichzeitig missglückte der Nachweis der Einhaltung der Grundsätze, womit ebenso gegen den Accountability-Grundsatz von Art. 5 Abs. 2 DSGVO verstossen wurde.

2046 Vgl. Rosenthal/Vasella, digma 2018, 166 ff., 171.

2047 Vgl. Passadelis/Roth, Jusletter vom 4. April 2016, N 4, N 62 und N 70.

die Anordnung eines Verarbeitungsverbotes, vgl. Art. 58 Abs. 2 lit. f DSGVO, sein.

Gleichwohl sollten die jeweiligen Datenschutzbehörden im Regime der DSGVO nicht nur als Sanktionsinstanzen gesehen werden. Sie sind ebenso Treuhänder im Dienste der Erhöhung des Datenschutzes: So können sie Untersuchungen durchführen und Empfehlungen aussprechen, was ein Unternehmen dabei unterstützt, das Datenschutzniveau zu verbessern. 1593

Um das Charakteristikum der starken Behördenhand gemäss DSGVO kompletter abzubilden, ist sodann der Ausbau sowie die Ausdifferenzierung der behördlichen Organisation, Zusammenarbeit und der Verfahren vor Augen zu führen.[2048] Die DSGVO hebt nicht nur die organisatorischen und prozeduralen Vorgaben gegenüber den Verarbeitenden an. Vielmehr bringt die DSGVO mit Blick auf die *behördliche Rechtsdurchsetzung* einen markanten Ausbau hinsichtlich der Behördenorganisation sowie -kooperation und der vorgesehenen Instrumente sowie Massnahmen. In diesem Zusammenhang ist, wenn nunmehr der Fokus in die Schweiz schwenken soll, Art. 27 DSGVO in Erinnerung zu rufen. 1594

Inwiefern aber wird die «Behördenhand» gemäss totalrevidiertem DSG gestärkt und der behördlichen Rechtsdurchsetzung Nachachtung verliehen? 1595

Anknüpfend an das *persönlichkeitsrechtliche Paradigma* mit der individualrechtlichen Durchsetzungsverantwortung wird neu die Unentgeltlichkeit der zivilrechtlichen Verfahren im Rahmen der Durchsetzung datenschutzrechtlicher Streitigkeiten gewährleistet– vergleichbar mit dem Regime zum Gleichstellungsgesetz resp. im Kontext des Arbeits- oder Mietrechts.[2049] Die entsprechenden Neuerungen finden sich in der ZPO.[2050] 1596

Dem EDÖB werden sodann Aufgaben zugewiesen im Zusammenhang mit den neuen Instrumenten der Datenschutz-Folgenabschätzung, aber auch bei Datensicherheitsvorfällen. Weiter werden die Befugnisse sowie Aufgaben des EDÖB gestärkt und ausgebaut, Art. 49 ff. nDSG, sowie die strafrechtlichen Sanktionsmöglichkeiten geschärft.[2051] 1597

Neu kann der EDÖB im Anschluss an eine Untersuchung, die von Amtes wegen oder auf Anzeige hin durchgeführt wurde, Verfügungen erlassen, vgl. Art. 49 ff. nDSG. Der Erlass verbindlicher Anordnungen gegenüber personendatenverarbeitenden Verantwortlichen resp. Auftragsverarbeitenden ist für den privaten Bereich eine Neuerung. Anders als die Aufsichtsbehörden im EU-Ausland wird in- 1598

2048 Vgl. Art. 51 ff. DSGVO und Art. 77 ff. DSGVO.
2049 Vgl. zu den zivilrechtlichen Ansprüchen des Datensubjektes Art. 32 nDSG.; Botschaft DSG 2017–1084, 17.059, 6941 ff., 7076.
2050 Vgl. neu Art. 113 Abs. 2 lit. g ZPO.
2051 Vgl. Art. 49 ff. nDSG und Art. 60 ff. nDSG.

des dem *EDÖB keine Kompetenz eingeräumt, Verwaltungssanktionen zu erlassen*.

1599 Der Ausbau der Strafbestimmungen des DSG, vgl. Art. 60 ff. nDSG, soll auch die fehlende Verwaltungssanktionskompetenz des EDÖB zumindest teilweise kompensieren.[2052] Der Höchstbetrag der Bussen wird auf CHF 250'000.00 angesetzt. Allerdings wird die Busse irritierenderweise nicht dem Unternehmen, sondern der *privaten Person* auferlegt. Eine solche Konstruktion entspricht nicht dem Regime gemäss DSGVO und wurde zu Recht kritisiert.[2053] Das bereits im Vorentwurf skizzierte Sanktionssystem wurde in der Vernehmlassung namentlich unter dem Aspekt negativ bewertet, dass die Strafbestimmungen primär die natürlichen Personen treffe. Plädiert wurde in der Vernehmlassung dafür, dass ausschliesslich die Unternehmen über Verwaltungssanktionen des EDÖB (ggf. einer zu diesem Zweck neu geschaffenen Kommission) sanktioniert werden sollten. Zudem wurde die Höhe der Bussen negativ beurteilt.[2054] Art. 60 ff. nDSG enthält die 2023 in Kraft tretenden einschlägigen Strafbestimmungen.

1600 Die strafrechtliche Verfolgung der natürlichen Person liegt bei der kantonalen Strafbehörden, vgl. Art. 65 Abs. 1 nDSG. Die Liste der strafbewehrten Verhaltensweisen wird an die neuen Pflichten der Verantwortlichen angepasst. Bemerkenswerterweise nicht im Katalog der Straftatbestände figuriert der Verstoss gegen die Basisgarantien eines jeden Datenschutzrechts, die *Generalklauseln als Minimal-Standard einer fairen Datenverarbeitung*. Nach welchen Bewertungskriterien gewisse Normverstösse in den Katalog von Art. 60 ff. nDSG aufgenommen wurden, andere dagegen nicht, ist nicht gänzlich nachvollziehbar. Eine fahrlässige Verletzung der Vorgaben, die strafrechtlich bewehrt sind, genügt nicht, um eine Busse zu verhängen.

1601 Neu als Übertretung gilt das Missachten von Verfügungen des Beauftragten oder von Entscheiden der Rechtsmittelinstanzen, Art. 63 nDSG. Der EDÖB kann in Strafverfahren die Rechte einer Privatklägerschaft wahrnehmen, Art. 56 Abs. 2 nDSG. Zudem wird die Verfolgungsverjährungsfrist bei Übertretungen verlängert, Art. 66 nDSG.

1602 Die Stärkung und der Ausbau der Behördenkompetenzen wurden als tragende Pfeiler beurteilt, um vonseiten der EU als Drittstaat mit äquivalentem Schutzniveau taxiert werden zu können.[2055] Ob das nunmehr vorgesehene Durchset-

2052 Vgl. Botschaft DSG 2017–1084, 17.059, 6941 ff.; zu den neuen Strafbestimmungen Rosenthal/Gubler, SZW 2021, 52 ff.
2053 Glatthaar, SZW 2020, 43 ff.
2054 Vgl. BBl 2017–1084, 17.059, 6941 ff., 6941 ff., 6974.
2055 Das Schweizer Parlament, AB, Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz, Bern 2019, <https://par-pcache.simplex.tv/subject?themeColor=AA9E72&subjectID=48166&language=de> (zuletzt besucht am 30. April 2021).

zungsregime gemäss Totalrevision den Erwartungen vonseiten der EU an ein äquivalentes Datenschutzniveau zu genügen vermag, wird sich weisen. Sie differiert sowohl bezüglich der Verantwortlichkeit und der Höhe der Bussen, aber auch mit Blick auf den Katalog der sanktionswürdigen Datenschutzverstösse. Mit anderen Worten weist die Totalrevision signifikante Differenzen zum Regime gemäss DSGVO auf. In Bezug auf das Sanktionssystem ist zu betonen, dass zwar beide Rechtstexte neuerdings auch für Verletzungen gegen das Datenschutzrecht «abschreckende» Sanktionen vorsehen (wollen). *Allerdings ist damit etwas ganz Unterschiedliches gemeint:* Die DSGVO statuiert ein Modell der unmittelbaren Verbandshaftung. Es ist das Unternehmen, für das der Verantwortliche agierte, das gebüsst wird. Unter Umständen denkbar ist ein Regress auf den Verantwortlichen. Anders dagegen die Schweiz: Sie implementiert die *persönliche Strafbarkeit des Verantwortlichen*. Das Konzept scheint dem Datenschutzrecht abträglich zu sein: Denn welche kompetente und erfahrene Person, welche die notwendige und noch heute rare datenschutzrechtliche Expertise hat, wird bei entsprechendem Risiko eine datenschutzrechtlich relevante Funktion wahrnehmen?

Zudem bildet das gewählte Regime die Interessen- und Verantwortlichkeitslagen 1603
nicht korrekt ab. Die Personendatenverarbeitungsprozesse dienen stets dem Unternehmen und nicht den mit den datenschutzrechtlichen Vorgaben betrauten Individuen in der Organisation. Ein Fehlverhalten ihrerseits wäre einzig über einen Rückgriff nach primärer Verantwortung des Unternehmens zu adressieren. Die Totalrevision vermag insofern nicht zu überzeugen und verleiht der behördlichen Durchsetzung keine mit dem europäischen Recht vergleichbare Stärke.

2.9. Resümee

Analog zum Vorgehen im zweiten Teil, in dem *drei Strukturmerkmale des DSG* 1604
herausgearbeitet wurden, verfolgten die vorangehenden Ausführungen das Ziel, die jüngsten rechtlichen Entwicklungen anhand von *Trends* zu charakterisieren. Dies geschah anhand eines Blickes auf die DSGVO sowie die Totalrevision des DSG. Letztere wurde kursorisch integriert, zumal die Verabschiedung des Gesetzes mit dem Abschluss dieser Schrift zusammenfiel.

Trotz zahlreicher offener Einzelfragen, die in den kommenden Jahren und Jahr- 1605
zehnten einer Klärung durch Lehre und Praxis zuzuführen sind, lassen sich heute *neue resp. ergänzende Charakteristika des Datenschutzrechts in Europa* feststellen. Der Erkenntnisgewinn liegt auch darin, die *neu implementierten Ansätze in Bezug und Ergänzung zu den bisherigen Strukturmerkmalen* zu lesen. Die Beschreibung der wichtigsten Entwicklungslinien, die sich zu konzeptionellen Ansätzen datenschutzrechtlicher Regulierung verdichten, schützt – dies am Ran-

de – davor, sich in der Weite der Begriffe, in der Enge des Fokus oder in der Komplexität zu verlieren. Die Skizzierung der neuesten datenschutzrechtlichen Entwicklungstrends vermittelt ein Bewusstsein für einige der datenschutzrechtlichen Kernherausforderungen.

1606 Die Beschäftigung mit den rechtlichen Neuerungen, wie sie mit der DSGVO, aber auch der Totalrevision des DSG einhergehen, hat gezeigt, dass die bedeutsamsten Entwicklungen *nicht* in Anpassungen des materiellen Datenschutzrechts zu verorten sind. Auch in Zukunft werden die im *zweiten Teil beschriebenen Strukturmerkmale* und insb. die allgemeinen Verarbeitungsgrundsätze in zentraler Weise das materielle Datenschutzrecht konstituieren. Der Akzent der Neuerungen liegt auf dem Ausbau prozeduraler sowie organisatorischer Vorgaben und Instrumente. Mit ihnen soll die Einhaltung des Datenschutzrechts effektuiert werden.

1607 Die jüngste rechtliche Neuerungswelle wurde anhand von *acht Entwicklungstrends*, teilweise mit Teilaspekten, beschrieben. Diese hängen teilweise eng zusammen, weshalb innerhalb der Betrachtungen der einzelnen Trends resp. Charakteristika gewisse Redundanzen unvermeidbar waren.

1608 *Das erste Kernelement ist der sog. lange Arm der neuen Erlasse:* Der Fokus lag auf dem *extraterritorialen Ansatz der DSGVO*. Mit ihm wird der Befund der Grenzenlosigkeit von Personendatenverarbeitung adressiert. Der Globalisierung, die gemeinsam mit modernen Datenverarbeitungstechnologien eine besondere Dimension erlangt, wird über die räumlichen Anwendungsbereiche zeitgemässer Datenschutzgesetze Rechnung getragen. Anhand der Analyse des extraterritorialen Anwendungsbereiches der DSGVO wurde gezeigt, inwiefern eine Ablösung resp. Lockerung des Datenschutzrechts in seiner traditionellen Verortung im individualrechtlichen Subjekt- resp. Persönlichkeitsschutz stattfindet. Die DSGVO macht die *geschäftlichen und wirtschaftlichen Aktivitäten zu einem zentralen Anknüpfungselement des räumlichen Anwendungsbereichs*. Wer im EU-Raum Geschäfts- oder Beobachtungsaktivitäten entfaltet, der hat sich an die datenschutzrechtlichen Vorgaben der EU zu halten. Damit wird neben einer zivil- und persönlichkeitsrechtlichen Ingredienz auch eine wirtschaftsrechtliche Ingredienz deutlich. Zudem sind für die Evaluierung des Anwendungsbereichs keine Formalien, sondern die faktischen Realitäten relevant. Das Empören in der Schweiz betreffend den langen Arm der DSGVO ist nicht gerechtfertigt, zumal das DSG nicht erst nach Totalrevision über das IPRG extraterritoriale Wirkung entfaltet, vgl. Art. 3 nDSG. Zudem werden die Anforderungen für private Datenbearbeitende im Ausland und die Bekanntgabe von Personendaten ins Ausland angehoben, vgl. Art. 14 und Art. 16 nDSG.

1609 Hieran anknüpfend wurde ein *zweiter Entwicklungstrend* nachgezeichnet. Die *Pluralisierung von Schutzzwecken* zeigt sich klar in der DSGVO: Zwar wird dem

Schutz der *Person* mit der DSGVO weiterhin ein zentraler Stellenwert eingeräumt. Gleichwohl wird bereits anhand des Schutzzweckartikels sichtbar, dass mit dem Erlass weitere Schutzzwecke, so etwa die Funktionstüchtigkeit des Marktes, gewährleistet werden sollen. Die Kriterien der territorialen Anwendbarkeit richten sich ebenso an Geschäfts- und Marktaktivitäten aus. Eine dergestalt offene Anerkennung diversifizierter Schutzstossrichtungen datenschutzrechtlicher Regulierung wird im DSG auch nach der Totalrevision nicht erfolgen, vgl. Art. 1 nDSG.

Als *dritte paradigmatische Entwicklung wurde der durch die DSGVO vollzogene Übergang zu einem monistischen Regime* beschrieben. Der Schritt zu einer Vereinheitlichung des allgemeinen Datenschutzrechts für den privaten und den öffentlichen Sektor wurde in den Jahren vor den Revisionswellen namentlich in Deutschland diskutiert.[2056] Anders hält die Schweiz im Zuge der Totalrevision an ihrem *Dualismus* fest.[2057] Immerhin führt die Schaffung neuer Instrumente für beide Bereiche zu einer gewissen Annäherung. Am entgegengesetzten Ausgangspunkt für den öffentlichen gegenüber dem privaten Bereich ändert dies allerdings nichts. Eine umfassende Vereinheitlichung der Vorgaben für den privaten gegenüber dem öffentlichen Bereich stand nicht ernsthaft zur Debatte. Die Vereinheitlichung der datenschutzrechtlichen Vorgaben für öffentliche resp. private Akteure in der EU ist in Anbetracht der Kontroverse, die das Thema seit jeher auslöste, als Paradigmenwechsel zu qualifizieren. Indem die EU von einem Monismus mit prinzipiellem Verarbeitungsverbot und Erlaubnistatbeständen für den öffentlichen wie den privaten Bereich ausgeht, die Schweiz dagegen von einem Dualismus mit konträren Ausgangspunkten, kennt Kontinentaleuropa kein einheitliches Regelungskonzept in Bezug auf die rechtlich traditionsreiche Zweiteilung zwischen öffentlichem Recht und Privatrecht. In Erinnerung zu rufen ist, dass der Dualismus in der Schweiz weniger von sachlogischen als vielmehr von politischen Motiven getragen war. Die datenschutzrechtliche Differenzierungswürdigkeit aus fach- und sachbasierenden Gründen und vor dem Hintergrund eines neuen datenschutzrechtlichen Schutzkonzeptes wird im letzten Kapitel dieser Schrift erneut thematisiert werden.[2058] Insofern ist der dem US- 1610

2056 Vgl. Buchner, der indes für eine Zweiteilung plädiert, wobei im privaten Bereich konsequent der Grundsatz der Privatautonomie zu verwirklichen sei.

2057 Vertiefend hierzu zweiter Teil, IV. Kapitel.

2058 Verdeutlicht wurde sie indes im Laufe dieser Arbeit. Besonders eindrücklich wird die Relevanz in Worte gefasst von einer Pionierin des Datenschutzes, Nissenbaum. In ihrem die Richtung weisenden Werk «Privacy in Context» bezeichnet sie ein duales Regelungsregime als «krude Version» eines kontextuellen Ansatzes, der plurale gesellschaftliche Bereiche anerkennt und auch informationell voneinander abgrenzt resp. die Informationsflüsse zwischen den Bereichen sorgfältig koordiniert. Nur ein solcher kontextueller Ansatz vermag die Aufgaben und Anliegen des Datenschutzes in Zukunft angemessen zu adressieren; vgl. zur Rezeption des Bildes der Informationsflüsse und des kontextuellen Ansatzes für den medizinischen Bereich Nagenborg/El-Faddagh, IRIE 2006, 40 ff., 42; früh schon Fiedler, in: Podlech/Steinmüller (Hrsg.), 179 ff., 191 f., der ein allgemeines

amerikanischen Recht entstammende Ansatz relevant, den Datenschutz keiner allgemeinen Gesetzgebung, stattdessen bereichsspezifischen Erlassen zuzuführen. Die bereichsdifferenzierende Würdigung fällt damit global betrachtet heterogen aus.

1611 Als *viertes Charakteristikum* der rechtlichen Neuerungen wurde die *Stärkung der individualrechtlichen Position und in einem weiteren Sinne die Stärkung der Position des Datensubjektes* genannt. Der Ansatz setzt am traditionsreichen subjektivrechtlichen Anknüpfungspunkt der ersten Datenschutzgesetze an und baut diesen aus.[2059] Besagter Trend, die Position des Datensubjektes auszubauen, wurde insb. durch eine Ausweitung der Betroffenenrechte sowie eine Anhebung der Transparenz- sowie Einwilligungsvorgaben bewerkstelligt. Die hier ansetzenden Entwicklungen stehen allerdings, selbst wenn sie ein etabliertes Paradigma bestärken, nicht isoliert da.

1612 *Fünftes Kernmerkmal der Neuerungen ist das Abzielen auf die faktische Verwirklichung:* Sowohl die DSGVO als auch die Totalrevision des DSG zielen darauf ab, eine Hauptschwäche bisheriger datenschutzrechtlicher Regelung zu beseitigen: das faktische *Vollzugsdefizit*.[2060] Beide Erlasse sehen neue Instrumente vor, mit dem Ziel, das Datenschutzrecht faktisch wirksam werden zu lassen. Datenschutzrecht soll in der Realität griffig werden und seine Existenz nicht nur auf dem Papier fristen. Damit wird die Existenz des Datenschutzrechts auch nicht mehr erst und höchstens im Falle seiner Missachtung oder Verletzung sichtbar. Neu greifen Pflichten, welche die proaktive Implementierung des Datenschutzes in die DNA jeder Organisation, Institution oder Stelle, die Personendaten verarbeitet, fordern. Hierzu gehören die Pflichten zur Entwicklung einer Datenschutzorganisation sowie von Prozessen, welche die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen. Auch die Pflicht zur Inventarisierung der Verarbeitungshandlungen sowie von Verarbeitungsrisiken, das Instrument der Risikofolgenabschätzung, die Notifikationspflichten bei Datenschutzvorfällen, «privacy by design» und «privacy by default» sowie die Rechenschaftspflichten hinsichtlich der Datenschutz-Compliance wollen das bisherige datenschutzrechtliche Wirkungsdefizit in der Realität mildern. Alle diese Instrumente stärken die *Eigenverantwortung* der Verarbeitenden und ihre Pflicht zu datenschutzrechtlich proaktivem und präventivem Agieren.

1613 Als *sechstes Merkmal* der jüngsten datenschutzrechtlichen Neuerungswellen wurde die Ausgestaltung des Datenschutzes als *Compliance- und Governance-Aufgabe* beschrieben. Damit wird das bisherige persönlichkeits- und individualrecht-

Recht der Information fordert, wobei der Umgang mit Daten in enger Abhängigkeit zu einzelnen Sachgebieten zu erfolgen habe.

2059 Vertiefend hierzu zweiter Teil, VI. Kapitel.

2060 Vertiefend hierzu dritter Teil, VII. Kapitel.

liche Paradigma in signifikanter Weise neu positioniert. Zwar dient ein Recht, das Datenschutz als Compliance- und Governance-Aufgabe definiert, ebenso dem Schutz des Datensubjektes. Mit der Entwicklungslinie, wonach die DSGVO wie das totalrevidierte DSG den Datenschutz als Compliance- und Governance-Aufgabe installieren, fügt sich der Datenschutz neuerdings – vergleichbar mit den Vorgaben zur Verhinderung von Geldwäsche, für das Kartellrecht oder die Rechnungslegung – in den Palmarès von Compliance-Verantwortlichkeiten. Mehrere der bereits unter der Zielsetzung der Effektuierung des formellen Datenschutzrechts erwähnten Instrumente sind erneut unter diesem Aspekt relevant, so der Ausbau der Vorgaben betreffend Prozessgestaltung und Organisation oder der Einsatz technischer sowie schulischer Massnahmen. Im Zusammenhang mit der Ausgestaltung des Datenschutzrechts als Compliance- und Governance-Aufgabe ist zudem der *Grundsatz der Accountability* relevant. Sämtliche Massnahmen, die zwecks Einhaltung des Datenschutzrechts getroffen wurden, sind zu dokumentieren.[2061] Es sind neu die Datenverarbeitenden, die betreffend die Einhaltung der datenschutzrechtlichen Vorgaben rechenschaftspflichtig sind. Auch hierin zeigt sich, dass die bisherige individual- und persönlichkeitsrechtliche und damit defensivrechtliche Konzeption des Datenschutzrechts ganz neu eingebettet wird.

1614 Als *siebtes Kernelement der jüngsten Rechtsentwicklungen* wurde die Einführung des *risikobasierten Ansatzes* beschrieben. Das Risikoparadigma der datenschutzrechtlichen Neuerungen wird anhand mehrerer Instrumente sichtbar. Namentlich zu nennen ist die Datenschutz-Folgenabschätzung; allgemeiner orientiert sich die Angemessenheit der zu ergreifenden Datenschutz-Compliance-Massnahmen an Risikoerwägungen. Neben dem Verarbeitungsverzeichnis werden Risikoevaluationen und Risikoverzeichnisse relevant. Das Risikoparadigma setzt ebenso einen Kontrapunkt zu dem bislang persönlichkeitsrechtlich geprägten Datenschutzrecht.

1615 Der *achte Trend,* der besonders mit den Neuerungen qua DSGVO eingeleitet wird, ist die *Stärkung der Behördenhand.* Die DSGVO gibt den Behörden einen umfassenden Katalog von durch- und tiefgreifenden Massnahmen in die Hand, um der Einhaltung datenschutzrechtlicher Vorgaben Nachachtung zu verschaffen. Die Möglichkeit, Datenschutzverstösse mit hohen Bussen zu ahnden, ist ein Element mit Signalwirkung für die aufgewertete Bedeutung des Datenschutzrechts. Auch mit der Totalrevision des DSG werden die behördlichen Massnahmen verschärft, allerdings in einer nicht mit der DSGVO vergleichbaren Weise.

1616 Damit wurden die jüngst vonseiten der Regulatoren formulierten Antworten auf die aktuellen datenschutzrechtlichen Herausforderungen *anhand von acht Trends in nicht abschliessender Weise herausgearbeitet*. Die Elemente im Verbund be-

2061 Der Ansatz ist in der DSGVO, anders als im totalrevidierten DSG, explizit verankert.

trachtet verifizieren und bestätigen die Evaluation, wonach die DSGVO, aber auch das totalrevidierte DSG einen *datenschutzrechtlichen Paradigmenwechsel* nach sich ziehen.[2062] Es handelt sich bei den Rechtsneuerungen in der EU nicht um Retuschen. Die *paradigmatischen Veränderungen* lassen sich für Schutzzweck, Regelungsmechanik und -ansätze sowie Umsetzungsinstrumente beschreiben.

1617 Die bisherigen Ausführungen haben weiter sichtbar gemacht, dass die DSGVO, aber auch die Totalrevision des DSG *Etabliertes mit Neuem* kombinieren. In den Erlassen bleiben die generalklauselartigen Bearbeitungsgrundsätze und der Subjektschutz tragende Säulen. Zugleich werden neue Instrumente und Ansätze eingefügt, die den defensivrechtlichen Subjektschutz aufweichen resp. flankieren oder ergänzen. Ein isoliert defensiv- und abwehrrechtlicher Subjektschutz wird überwunden. Personendatenverarbeitende haben neuerdings proaktiv und risikobasiert organisatorische, prozedurale und technische Massnahmen der Datenschutz-Compliance und -Governance umzusetzen. Damit werden die *Lasten des Datenschutzes neu verteilt*, und zwar in Anlehnung an eine Idee des Verursacherprinzips und Interessenprinzips im Sinne einer primären Verantwortung der Verarbeitenden. Sie werden sich in Zukunft immer weniger auf die Position zurückziehen, wonach die Einhaltung des Datenschutzes nicht ernst zu nehmen sei, weil eine Persönlichkeitsverletzung wegen unrechtmässiger Personendatenverarbeitungen sowieso folgenlos bleibt.

1618 Etablierte Basiskonzepte wie die materiellrechtlichen Verarbeitungsgrundsätze oder der Subjektschutz werden zwar nicht ersetzt, aber durch neue Ansätze und Instrumente nachhaltig verändert und in eine andere Landschaft eingebettet. Das *Datenschutzrecht befindet sich damit in einer Phase der Transition*. An den die ersten Erlasse prägenden Konzepten wird teilweise festgehalten (in der Totalrevision des DSG mehr als mit der DSGVO); teilweise werden sie weiterentwickelt (z. B. die Betroffenenrechte) und ausnahmsweise fallengelassen (der Dualismus wird durch die DSGVO überwunden). Etablierte Strukturmerkmale werden sodann durch neue Ansätze und Akzente zwar nicht ersetzt, doch aber flankiert und ergänzt. Damit erhält das Datenschutzrecht in Europa neue und differenziertere Gesichtszüge. Sein Charakter erschöpft sich nicht mehr darin, eine *lex specialis* zum grund- und zivilrechtlichen Persönlichkeitsschutz zu sein.

1619 Drei Bemerkungen runden die Charakterisierung der jüngsten Rechtsentwicklungen ab:

1620 *Erstens* steckt auch im Datenschutzrecht der «Teufel im Detail». Die Implementierung in die Unternehmenspraxis verlangt regelmässig ein gewisses Mass an

2062 Die DSGVO führe das Datenschutzrecht in Europa in eine neue Ära, so Passadelis/Roth, Jusletter vom 4. April 2016, N 3.

Pragmatismus. Eine hundertprozentige Einhaltung der Vorgaben ist nicht erreichbar. Aber selbst die Umsetzung eines guten Niveaus an Datenschutzrechtskonformität bindet beträchtliche Ressourcen. Zudem wurden anhand der Beschreibung der jüngsten Entwicklungen mittels Trends und Entwicklungslinien die unzähligen dogmatischen Einzelfragen nicht sichtbar. Nicht nur im Anwendungsbereich der DSGVO, auch die Totalrevision des DSG wird unzählige, teilweise rechtlich anspruchsvolle Rechtsfragen nach sich ziehen. Als Beispiel sei nur die Frage nach der Ausdrücklichkeit der Einwilligung angesprochen.

1621 Für diese Arbeit von besonderem Interesse ist – *zweitens* – die Feststellung, wonach selbst die DSGVO, wie auch das DSG, Elemente des Systemschutzes beinhaltet. Solche systemschutzrelevanten Aspekte sind in der DSGVO, die zu einem *monistischen Regime* übergeht, weniger offensichtlich. Gleichwohl greifen verschiedene Normen und Instrumente – so der interne Datenschutzbeauftragte, Zertifizierungsverfahren, die Instrumente der Selbstregulierung usf. – die Einschlägigkeit kontextspezifischer Erwägungen und Besonderheiten auf. Sie stärken die *Eigenverantwortung* der jeweiligen Akteure mittels Einschlägigkeit der branchen- und sektorrelevanten Vorgaben. Damit werden sich diese von innen heraus, organisch und eingebettet ins Milieu datenschutzrechtskonform institutionalisieren. Insofern liesse sich von einer Institutionalisierung des Datenschutzes sprechen. Eine Institutionalisierung, die dazu führt, dass die Verantwortung und Aufgabe, datenschutzkonform zu handeln, in die jeweiligen gesellschaftlichen Bereiche zurückgespielt und von dort aus, quasi von innen heraus, konturiert, implementiert sowie herausgebildet wird. Über dieses Neuerungsmerkmal zeigt sich, wie der subjektiv- und defensivrechtlichen Säule des bisherigen Datenschutzrechts eine weitere Säule zur Seite gestellt wird.

1622 *Drittens* zeigt sich für die Schweiz mit der Totalrevision, dass an den drei im zweiten Teil dieser Arbeit herausgearbeiteten Leitprinzipien des DSG festgehalten wird: pointierter Dualismus für den öffentlichen und privaten Bereich mit entgegengesetztem Ausgangspunkt, weitgehend generalklauselartiges Regelungsregime sowie persönlichkeitsrechtliche Anknüpfung des DSG für den privaten Bereich. Allerdings resultiert aus der Einführung mehrerer neuer Instrumente und Ansätze, die teilweise gleichermassen für den öffentlichen wie den privaten Bereich gelten, eine neue Gesamtlandschaft. Die Veränderungen, die mit der Totalrevision einhergehen, sind keineswegs bloss Retuschen. Gleichwohl bleiben sie im Vergleich zu den Neuerungen, wie sie mit der DSGVO einhergehen, weniger markant.[2063] Dies gilt namentlich auch in Bezug auf die behördlichen Durchsetzungsinstrumente.

2063 Die Totalrevision installiert einige der neuen Instrumente, Rechte und Ansätze, wie sie mit der DSGVO verankert wurden – z. B. das Verarbeitungsverzeichnis, die Rollen von Verantwortlichen und Auftragsverarbeitenden, Vorgaben im Zusammenhang mit Datensicherheitsvorfällen, automati-

1623 Nach diesem Überblick über die Kernelemente resp. Strukturmerkmale der aktuellen gesetzgeberischen Entwicklungen im Datenschutzrecht folgt eine *Tour d'Horizon* über die rechtswissenschaftlich präsentierten Lösungsansätze. Punktuell werden vonseiten der jüngsten Rechtsprechung ausgehende und zukunftsweisende Impulse einbezogen. Für die Jurisprudenz, die sich mit der Digitalisierung, dem Informations- und Datenschutzrecht befasst, ist die gängige subjektivrechtliche Anknüpfung weiterhin der nächstliegende Bezugspunkt. Er begründet und markiert – gemeinsam mit der durch die Technologien vollzogenen Fragmentierung des Menschen, den Kommerzialisierungspraktiken in Bezug auf Personendaten und dem Narrativ der Degradierung des Subjektes zum reinen Informationsobjekt – eine spezifische Sichtweise, einen vordefinierten Ausgangs- und Ansatzpunkt und hieraus abgeleitete Lösungskonzepte.[2064]

B. Ansätze der (zivil-)rechtlichen Lehre und Praxis

«Punkt, Punkt, Komma, Strich,
fertig ist das Angesicht.
Haare kommen oben dran,
Ohren, dass er hören kann,
Hals und Bauch hat er auch,
hier die Arme, dort die Beine,
fix und fertig ist der Kleine.»

1. Vorbemerkung

1624 Ein Kinderreim mit seiner schlichten, fast digitalen Sprache leitet die Ausführungen ein, die sich mit den in jüngerer Zeit entwickelten, rechtswissenschaftlichen Analysen zum Datenschutzrecht befassen. Der einleitende Kinderreim ist als Metapher gemeint, wonach der Mensch immer stärker in seine informationellen und stofflichen Einzelbestandteile zerlegt wird.[2065] Es folgt ein Abriss über Lösungs-

sierten Einzelfallentscheidungen oder dem Profiling; zu Algorithmen, künstlicher Intelligenz und automatisierten Einzelfallentscheidungen insb. auch die Studien von Lohmann; Wildhaber/Lohmann; Heuberger; vgl. zu den Kernelementen der Totalrevision Auf der Mauer/Fehr-Bossard, in: Thouvenin/Weber (Hrsg.), ITSL 2017, 23 ff., 34 ff.

2064 Dass indes die rechtliche und rechtswissenschaftliche Konzentration auf das Individuum, die Person und ihren Schutz (sei es in Gestalt einer Selbstbestimmung, sei es in Gestalt einer Missbrauchsnormierung) resp. das Personendatum als Quasi-Objekt zu kurz greift, um die datenschutzrechtlichen Herausforderungen angemessen und wirksam zu adressieren, wird auch durch die kritische Reflexion der wissenschaftlich entwickelten Lösungsansätze zu zeigen sein. Zudem wird das dritte und letzte Kapitel dieses dritten und letzten Teils dieser Studie einen Perspektivenwechsel vorschlagen, welcher das Paradigma der Systemrelevanz des Datenschutzrechts herausarbeitet.

2065 Lesenswert in diesem Zusammenhang auch der Essay von Meckel, 4 ff.

ansätze, die den Fragmentierungs-, Kommerzialisierungs- und Exklusionstendenzen, welche mit neuen Technologien assoziiert werden, entgegengesetzt werden.

An Personendaten bestehen, wie gezeigt, vielseitige und facettenreiche Interessen. Die Rechtslage bleibt wissenschaftlich umstritten: Wenn personenbezogene Daten zugleich Persönlichkeits- und Wirtschaftsgut sind, wie soll das Recht damit umgehen? Ist ein Datenschutzrecht, verstanden als ein Recht zur Verteidigung der Privatsphäre, das richtige Instrumentarium, um diesen Herausforderungen gerecht zu werden? Finden die jüngsten Entwicklungen angemessene Antworten auf die Herausforderungen, mit denen man sich konfrontiert sieht? Sind sie lediglich als Hindernis des effizienten Geschäftsganges zu sehen oder können sie als Chance gelesen werden? Sollte rechtlich nicht eher ein Herrschaftsrecht des Datensubjektes anerkannt werden, z. B. in Gestalt eines (geistigen) Eigentumsrechts an Daten? Welche Rolle spielt in diesem Zusammenhang das Recht auf informationelle Selbstbestimmung? Und wie soll eine Kollision des Rechts auf informationelle Selbstbestimmung mit der Informations- und Wirtschaftsfreiheit bewältigt werden? Mit diesen und anderen Fragen beschäftigte sich die Rechtswissenschaft in den letzten Jahren. 1625

Ansatzpunkte für die wissenschaftliche Analyse von datenschutzrechtlichen Herausforderungen liefern der Privatrechtswissenschaft *die subjektiven Rechte*. Die Privatrechtslehre greift zur Bewältigung datenschutzrechtlicher Herausforderungen auf zwei grosse Kategorien des Zivilrechts zurück: das Persönlichkeitsrecht sowie das Eigentumsrecht. Beide subjektiven Rechte sollen so gestaltet werden, dass sie auch Personendaten erfassen. 1626

Die Weiterentwicklung der für die analoge Welt etablierten Rechtskategorien wird von spezifischen, anhand des kleinen Gedichts poetisch eingeleiteten Narrativen mitgestaltet: Die formulierten Antworten verfolgen insb. das Ziel, der *informationellen Fragmentierung und Degradierung des Menschen* als Person und vom Subjekt zum Objekt entgegenzutreten. Weiter sollen rechtlich wirksame Antworten formuliert werden hinsichtlich der faktischen Transformation von Informationen in digitale Güter. Dabei geht es auch darum, die Kommerzialisierung von Personendaten zu adressieren.[2066] 1627

Lange war die *persönlichkeitsrechtliche Begründung des Privatheits- und Datenschutzes* unbestritten. Allerdings hat diese Studie an mehreren Stellen sichtbar gemacht, dass ein delikts- und damit defensivrechtlich strukturierter Persönlichkeitsschutz als Quellrecht des Datenschutzrechts Defizite aufweist und entspre- 1628

2066 Vgl. zum Begriff der digitalen Güter und Verträge darüber Grünberger, AcP 2018, 123 ff.; Benhamou/Tran, sic! 2016, 571 ff.; Auer, ZfPW 2019, 130 ff.; unlängst zu Lösungsansätzen mit Blick auf den zivilrechtlichen Umgang mit digitalen Gütern Pfaffinger, Digitale Güter: Knotenpunkte des Privat- und Zivilrechts, Vortrag vom 6. November 2019, HSG/Universität St. Gallen.

chend Anpassungen erfährt. Die Aussage, wonach Datenschutz nicht Daten, sondern die Persönlichkeit schütze, hat in ihrer Pauschalität an Gültigkeit verloren.

1629 Sukzessive an Bedeutung gewonnen hat die Formulierung eines Zieles, wonach das Datensubjekt nicht nur demokratisch, sondern auch ökonomisch verstärkt in die Prozesse und dergestalt rechtlich zu inkludieren sei. Damit verbunden ist eine Diskussion über die wirtschaftlichen Verwertungsaspekte im Lichte eines (vermeintlich) defensiv-ideell konstruierten Persönlichkeitsrechts. Datenschutzrechtliche Herausforderungen könnten folglich als ein Unterthema innerhalb des Diskurses zur Kommerzialisierung des Persönlichkeitsrechts verortet werden.[2067] Allerdings bleibt eine solche Analyse in den zivilrechtlichen Konstruktionen, wie sie für die analoge Welt entwickelt wurden, verhaftet.[2068] Entsprechend geht es in den nachfolgenden Ausführungen nicht darum, die unzähligen dogmatischen Raffinessen der rechtswissenschaftlichen Auseinandersetzungen zur Kommerzialisierung der Persönlichkeit, des Persönlichkeitsrechts oder von Persönlichkeitsgütern zu reflektieren, die gerade in Deutschland eine beachtliche Fülle erreicht haben.[2069]

1630 Vielmehr soll in einem ersten Schritt anhand der Beschreibung von *Lösungsparadigmen* eine Strukturierung der spezifisch datenschutz- resp. informationsrechtlichen Beiträge erreicht werden. Die anschliessenden Ausführungen sind damit auch deskriptiv. Das Spektrum der vorgeschlagenen Strategien reicht von einer weiterhin defensiv-abwehrrechtlichen und ontologisch geprägten Konzeptionierung eines im Persönlichkeitsrecht gründenden Privatheitsbegriffs hin zu einem ebenfalls im Persönlichkeitsrecht anknüpfenden Recht an eigenen Daten. Es folgt eine Betrachtung der Nomenklatur und Zuweisungsordnung nach Zech, der sich mit Information als Schutzgegenstand befasst und damit auch, aber nicht nur den Umgang mit Personendaten analysiert. Weil sein Beitrag differenzierte Zuordnungsmodelle für unterschiedliche Informationskategorien und in der Fol-

2067 Spezifisch in Bezug auf Personendaten zu den Konsequenzen der Ökonomisierung der informationellen Selbstbestimmung und zur zivilrechtlichen Erfassung des Datenhandels Specht, 11 ff.; Unseld, 1 ff.; für das britische Common Law Westkamp, *passim*; Buchner, DuD 2010, 39 ff.; Bunneberg, *passim*; Weichert, in: Bäumler (Hrsg.), 158 ff.; zum Handel mit Personendaten auch Schwartz, Harv. L. Rev. 2004, 2055 ff., 2057 ff.; Schmidt, digma 2019, 178 ff.

2068 «Digitalisierung und Vernetzung bringen strukturelle technische Veränderungen mit sich, auf die zu reagieren das weitgehend an einer analogen, unvernetzten Welt gebildete Recht oft jedoch nur schlecht vorbereitet ist», so Dreier, in: Hilty/Drexl/Nordemann (Hrsg.), 67 ff., 67; spezifisch mit Blick auf die Herausforderungen im Zusammenhang mit dem Urheberrecht Ders., in: Ohly/Bodewig/Dreier/Götting u. a. (Hrsg.), 283 ff.

2069 Vgl. z. B. Forkel, GRUR 1988, 491 ff.; Beuter, *passim*; Ullmann, AfP 1999, 209 ff.; Freitag, *passim*; spezifisch mit Blick auf die Persönlichkeitsrechte Verstorbener Gregoritza, *passim;* Klüber, *passim*; für die Schweiz insb. Meyer, *passim*; m. w. H. Büchler AcP 2006, 300 ff.; in Bezug auf den Körper, Körpersubstanzen, Körperfragmente sowie Bioinformationen zu den Qualifikationsansätzen, die Kommerzialisierungsproblematik sowie einen Ansatz zu einem inklusiven Biomedizinrechts vgl. die Studie von Karavas, Körperverfassungsrecht, *passim;* Roth, *passim;* Taupitz, *passim*.

ge eine Stufenordnung entwickelt, wird sein Lösungskonzept in dieser Studie systematisch nach dem Persönlichkeitsparadigma, aber vor dem Eigentumsparadigma dargestellt. Es folgt ein Blick auf die wissenschaftliche Diskussion zum Dateneigentum. Ein eigentumsrechtlich begründetes Recht an Personendaten hat rechtswissenschaftlich in der Schweiz neuerdings auffallend viel Aufmerksamkeit auf sich gezogen. Ungeachtet des Quellrechts – Persönlichkeitsrecht oder Eigentumsrecht – bildet die informierte Einwilligung des Datensubjektes in Konstruktionen von (Herrschafts-)Rechten an eigenen Daten ein Kernelement. Allerdings sind gerade auch für die rechtswissenschaftliche Forschung in der Schweiz die kritischen Erkenntnisse zum Konzept der informierten Einwilligung im Datenschutzrecht sowie zu demjenigen der Anonymisierung aufschlussreich. Diese Kritik an den wissenschaftlich entwickelten Hauptlösungsansätzen bereiten den Boden zur Fortentwicklung datenschutzrechtlicher Konzepte der Zukunft.

Vor dem Hintergrund der originären Anknüpfung des Datenschutzrechts im Persönlichkeitsrecht werden zunächst die unter dieser Rechtskategorie in jüngerer Zeit präsentierten Vorschläge zur datenschutzrechtlichen Weiterentwicklung dargestellt.[2070] 1631

2. Zum Persönlichkeitsparadigma

2.1. Der deliktsrechtlich begründete Anspruch auf informationelle Privatheit

Eine der wenigen Monografien aus der Schweiz, die sich in allgemeiner Weise mit dem Schutz personenbezogener Angaben im Privatrecht befasst, ist die Habilitationsschrift von Aebi-Müller aus dem Jahr 2005. Die Schrift rückt, wie es bereits der Titel sowie die Forschungsfrage deutlich machen, Art. 28 ZGB in das Zentrum. Eine Darstellung der Normen des DSG für den privaten Bereich, welche *lex specialis* zu Art. 28 ZGB sind, findet am Rande statt. Die Monografie beruht somit offensichtlich auf einem persönlichkeitsrechtlichen Ansatz, der von einer defensiv-ideellen Dogmatik des zivilrechtlichen Persönlichkeitsschutzes geprägt wird. Zentral für die Studie Aebi-Müllers ist das Unterfangen, das Schutzobjekt, die «Privatheit» als Rechtsbegriff neu zu definieren. 1632

Die Autorin beschreibt in ihrer Habilitationsschrift die Schwächen der *Sphärentheorie*, an der das Bundesgericht bis heute festhält.[2071] Zugleich statuiert sie, dass das DSG das Recht auf informationelle Selbstbestimmung gewährleiste, was jedoch in ihren Augen zu weit gehe.[2072] Aebi-Müller skizziert in der Folge einen 1633

2070 Vgl. zu einer rechtlichen Analyse auch mit Blick auf eigentumsrechtliche sowie persönlichkeitsrechtliche Ansätze für Deutschland Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 204 ff.
2071 M. w. H. Aebi-Müller, N 512 ff.
2072 Dies., N 51, N 360, N 546, N 570, N 591 ff. und N 773.

eigenen Ansatz, der an die konkret betroffenen Persönlichkeitsbereiche anknüpft. Inspiriert ist der Ansatz von der Studie der Philosophin Rössler.[2073]

1634 Rössler legt in ihrer Schrift zum Wert des Privaten dar, dass ebendieser Wert im Schutz der autonomen Lebensführung liege. Im Werk Rösslers steht damit der Schutz der *Autonomie*, des *selbstbestimmten Lebens* und der Selbstbestimmung im Zentrum.[2074] Ausgangspunkt ist für die Autorin der staatsrechtlich-politische Kontext, wobei eine vertiefte Auseinandersetzung mit den Theorien des Liberalismus stattfindet.[2075] Die Studie ist in ihrer Auseinandersetzung mit der Kategorisierung des Privaten aus einer Gender-Perspektive zugleich kritisch.[2076]

1635 Die Selbstbestimmung hat bekanntermassen für das Recht – namentlich in den Rechtsgebieten, welche die Herausforderungen neuer Technologien (Bio- und Informationstechnologien) zu bewältigen haben – in den vergangenen Jahren und Jahrzehnten eine Sonderposition erlangt.[2077] Selbstbestimmungsrechte werden insb. für die Bereiche des (Bio-)Medizinrechts sowie das Informationsrecht intensiv diskutiert.[2078]

1636 Gleichwohl tritt Aebi-Müller mit ihrer Anlehnung an Rössler, nach welcher Privatheit geschätzt wird und schutzwürdig ist, *weil* sie für ein selbstbestimmtes Leben unabdingbar ist, *nicht* für die Gewährleistung eines Rechts auf informationelle Selbstbestimmung ein. Ein Recht auf informationelle Selbstbestimmung oder ein Herrschaftsrecht an eigenen Daten sei zwar im eidgenössischen Datenschutzgesetz angelegt – allerdings gehe ein solches zu weit.[2079] Einschlägig sein solle – basierend auf einer in erster Linie terminologischen Anlehnung an eine

2073 Vgl. Aebi-Müller, N 621 ff., insb. N 646 ff.; früher auf Rössler referierend bereits Rudin, in: Sutter-Somm/Hafner/Schmid/Seelmann (Hrsg.), 415 ff., 421 ff.

2074 Rössler, 10 f., 39 f., 83 ff.; Dies., digma 2002, 106 ff.; vgl. zur bedrohten Entscheidungsfreiheit infolge von Beobachtungen qua EDV früh aus rechtlicher Perspektive auch Schmidt, JZ 1974, 241 ff.; Rudin, in: Sutter-Somm/Hafner/Schmid/Seelmann (Hrsg.), 415 ff., 421 ff.

2075 Dies., 27 ff.; zur Privatsphäre als Konzept der liberalen politischen Philosophie auch Hotter, 12 ff.; in diesem Zusammenhang ist auf den Beitrag zum Wert von Personendaten durch Karg, digma 2011, 146 ff., hinzuweisen. Der Autor hält fest, dass der Wert von Personendaten nicht isoliert wirtschaftlich betrachtet werden darf.

2076 Dies., 41 ff., insb. 49 ff.

2077 Vgl. Schweizer, in: Schweizer/Burkert/Gasser (Hrsg.), 907 ff.; Simitis, NJW 1984, 394 ff.; Stämpfli, *passim*; Vogelsang, *passim*; Waldmeier, *passim*; Welsing, *passim*; Wente, NJW 1984, 1446 ff.; Albers, *passim*; Amelung, *passim*; zudem für die Schweiz vgl. auch die facettenreichen Beiträge in Festschriften, z. B. Rosch/Wider (Hrsg.) sowie Sutter (Hrsg.), Simon/Weiss (Hrsg.).

2078 Vgl. für den biomedizinischen Kontext z. B. van Spyk, *passim;* für den datenschutzrechtlichen Kontext z. B. Buchner, *passim*.

2079 Aebi-Müller, N 546 und N 591 ff., vgl. aber zur Privatheit als Voraussetzung für Autonomie, N 646 ff.

der drei von Rössler bezeichneten Dimensionen des Privaten – die *informationelle Privatheit*.[2080]

Aebi-Müller plädiert dafür, unter dem (rechtlichen) Begriff der informationellen Privatheit jeweils die «konkreten massgeblichen Interessen des persönlich Betroffenen» als ausschlaggebend zu beurteilen.[2081] Insofern verweist sie auf verschiedene einschlägige Bereiche resp. Aspekte der Persönlichkeit, Verarbeitungszusammenhänge, Rechtsgüter mit entsprechenden Interessen wie die Menschenwürde, den Arbeitskontext, die Autonomie, die Identität und den Schutz der Gefühlswelt usf.[2082] Ebendiese Definierung des Privaten resp. des Privatheitsschutzes bettet sie dann in die Dogmatik und das persönlichkeitsrechtliche Regime von Art. 28 ff. ZGB ein. 1637

Im Ergebnis läuft die vorgeschlagene Methodologie – m. E. vergleichbar zum aktuellen Regime – auf eine *Interessenabwägung im Einzelfall* hinaus. Sie soll zur Beantwortung der Frage, ob eine Datenverarbeitung zulässig sei oder nicht, ausschlaggebend sein. So bleibt der Ansatz letzten Endes der persönlichkeitsrechtlichen Dogmatik und Struktur von Art. 28 ZGB mit stark abwehrrechtlicher und ideeller Prägung verpflichtet. Die Herausforderungen im Zusammenhang mit dem geldwerten Charakter der Persönlichkeitsrechte will die Autorin nicht abschliessend beleuchten.[2083] Der Ansatz soll die Sphärentheorie überwinden.[2084] 1638

2.2. Das Recht auf informationelle Selbstbestimmung

2.2.1. Vorbemerkungen

Für das Recht auf informationelle Selbstbestimmung ist das Volkszählungsurteil des Bundesverfassungsgerichts Ausgangspunkt. Nach seinem Vorbild ist eine Konstruktion und Gewährleistung des *prinzipiellen Verarbeitungsverbotes* ausschlaggebend.[2085] Ebendieses kann durch Erlaubnistatbestände durchbrochen werden, insb. eine gesetzliche Grundlage oder überwiegende Interessen. Zudem 1639

2080 Rössler unterscheidet neben der informationellen Privatheit die dezisionale Privatheit sowie die lokale Privatheit, vgl. 144 ff., 201 ff. und 255 ff.; vgl. Aebi-Müller, N 628 ff.; früher bereits auf Rössler referierend Rudin, in: Sutter-Somm/Hafner/Schmid/Seelmann (Hrsg.), 415 ff., 421 ff.

2081 Aebi-Müller, N 621 ff.

2082 Dies., N 646 ff. und N 652 ff.

2083 Aebi-Müller, N 24 ff.; kritisch gegenüber einer Warnung, Art. 28 ZGB wirtschaftlichen Interessen nutzbar zu machen, früh Riemer, sic! 1999, 103 ff.109, auch unter Hinweis, dass Art. 28 ZGB verschiedene wirtschaftliche Aspekte aufweise.

2084 Das Bundesgericht allerdings hält an dieser weiterhin fest. Auch das DSG bleibt für den privaten Bereich eine Missbrauchsgesetzgebung, die von der Struktur des Art. 28 ZGB geprägt ist. Entsprechend ist der Schweiz auch im Jahr 2020 ein Konzept informationeller Selbstbestimmung, das diesen Namen verdient, fremd; überzeugend auch Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), 19 ff., 34 ff.; Ziegler/Vasella, digma 2019, 158 ff., 158.

2085 Vertiefend die Analyse des Urteils im zweiten Teil, V. Kapitel, B.4.

figuriert die *Einwilligung* des Datensubjektes als ein Erlaubnistatbestand, sofern kein anderer angenommen werden kann.[2086] Die datenschutzrechtliche Einwilligung ist intuitiv und assoziativ ein konstituierendes Element für die informationelle Selbstbestimmung. Im Recht auf informationelle Selbstbestimmung nehmen die Autonomie und der Wille des Datensubjektes eine zentrale Rolle ein.

1640 Der Weg aus einer Verhaftung, wonach sich der Datenschutz als Persönlichkeitsschutz in passiven Abwehr- und Ausschliessungsbefugnissen oder in der Verhinderung missbräuchlicher Verarbeitungshandlungen manifestiert, führt über die Idee des Rechts auf Selbstbestimmung, auf «informationelle Selbstbestimmung». Mit der Figur eines «Rechts auf informationelle Selbstbestimmung» wird indes Verschiedenes gemeint.[2087] Anders gewendet: Unter ein und demselben Titel werden diverse Rechtskonstruktionen eingefangen, die dem Datensubjekt ganz unterschiedliche Rechtspositionen vermitteln.[2088]

1641 Der Rolle, Funktion und den Voraussetzungen der datenschutzrechtlichen Einwilligung wird vonseiten der Jurisprudenz insb. in Deutschland viel Aufmerksamkeit geschenkt. Mehrere Dissertationen befassen sich mit der zivilrechtlichen Erfassung eines Rechts an Daten, einer informationellen Selbstbestimmung auch im Privatrecht, die auf das Persönlichkeitsrecht zurückgeführt wird, wobei auch die datenschutzrechtliche Einwilligung thematisiert wird.[2089] Damit ist von wissenschaftlicher Seite her dokumentiert, dass die Konstruktion im Zentrum der wissenschaftlichen Auseinandersetzung mit dem Datenschutzrecht steht. Ihre Bewertungen allerdings fallen unterschiedlich aus. Gerade jüngst finden sich auch kritische Beiträge zur Tragfähigkeit des Konzepts.

1642 Für den Ansatz des Rechts auf informationelle Selbstbestimmung im Datenschutzrecht des privaten Sektors ist insb. Buchner richtungsweisend. Mit seiner Habilitationsschrift leistet er einen bedeutsamen Beitrag zur dogmatischen Durchdringung des Datenschutzrechts (bevor es von den Neuerungswellen ergrif-

2086 Richtungsweisend jüngst ein Entscheid der griechischen Datenschutzbehörde gegen PwC wegen unrechtmässigen und intransparenten Einsatzes der Einwilligung vgl. <https://edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_en> (zuletzt besucht am 30. April 2021).

2087 Ebendies wurde an verschiedenen Stellen dieser Untersuchung deutlich, insb. aber im zweiten Teil, VI. Kapitel, A.–C.

2088 Vgl. vertiefend dritter Teil, VII. Kapitel, A.2.; neuerdings auf Diskrepanzen hingewiesen hat m. w. H. Fasnacht, N 99 ff.; m. w. H., auch auf die Lehrmeinungen, Belser sowie Gächter/Werder; Ziegler/Vasella, digma 2019, 158 ff.; vgl. für Deutschland sodann namentlich die Beiträge von Specht; Liedke, *passim*; Rogosch, *passim*; Radlanski, *passim*.

2089 Für die Schweiz mit Blick auf ein Grundrecht auf informationelle Selbstbestimmung auch kritisch zur Funktionstüchtigkeit von Einwilligungskonstruktionen vgl. Waldmeier, 14 ff., 21 ff., 46 ff., 120 ff.; Fasnacht, *passim*; Heuberger mit Blick auf das Profiling, N 267 ff.; Ziegler/Vasella, digma 2019, 158 ff.; für Deutschland neben Buchner, 173 ff.; Liedke, *passim*; Rogosch, *passim*; Radlanski, *passim*.

fen wurde). Seiner Habilitationsschrift zum Recht auf informationelle Selbstbestimmung im Privatrecht aus dem Jahr 2006 widmen sich die folgenden Zeilen.

2.2.2. Der Ansatz des privatautonomen Ausgleichs von Buchner

Buchner gibt mit seiner Studie nicht nur ein Panorama über die vor den Revisionswellen anzutreffenden faktischen Herausforderungen.[2090] Er widmet sich spezifisch einer datenschutzrechtlichen Grundsatzfrage, derjenigen nach dem *Ausgangspunkt* – Freiheit der Verarbeitung mit Schranken oder Verarbeitungsverbot mit Erlaubnistatbeständen. Hieran schliesst die Frage an, inwiefern eine Vereinheitlichung oder Zweiteilung des datenschutzrechtlichen Regimes für den öffentlichen gegenüber dem privaten Bereich angezeigt ist.[2091] Für die Beantwortung sei die Drittwirkung des Grundrechts auf informationelle Selbstbestimmung auf den privaten Sektor relevant.[2092] 1643

Buchners Forderung, den privaten Bereich dezidiert an der für das Privatrecht geltenden Privatautonomie auszurichten, präsentiert sich aus heutiger Perspektive gegenüber der der seit 2016 in Kraft stehenden DSGVO als teilweise gegenläufig.[2093] Letztere vollzog einen Vereinheitlichungsschritt, wohingegen Buchner für die *bereichsspezifische Differenzierung* eintritt. Er plädiert für die Anerkennung eines Rechts auf informationelle Selbstbestimmung im privaten Bereich und tritt für einen privatautonomen Interessenausgleich ein.[2094] 1644

Buchner analysiert vertieft, ob es sich empfehle, für den öffentlichen und privaten Sektor ein einheitliches Datenschutzrecht zu implementieren – oder nicht. Wie gezeigt sieht die DSGVO ersteres vor. Der Autor spricht sich nach einer detaillierten Analyse der faktischen und rechtlichen Herausforderungen *gegen eine Vereinheitlichung* aus. Buchner konstatiert für den privaten Bereich nach seinen Erwägungen zur indirekten Drittwirkung der Grundrechte eine *Unauflösbarkeit des Konfliktes zwischen Datenschutz und Informationsfreiheit*. Weder die Individualrechte noch Allgemeinbelange sprächen für den Vorrang des Datenschutzes oder den Vorrang der Verarbeitungsfreiheit. Sämtliche Argumente liessen sich jeweils auf beiden Seiten anführen. Damit zeigt der Autor ebenso die Problematik von Interessenabwägungen, nicht nur im Einzelfall, sondern auch generell-abstrakt aufseiten der Gesetzgebung. Der beschriebenen Konflikthaftigkeit könne die Schärfe genommen werden, wenn die jeweils den Ausgangspunkt 1645

2090 Buchner, 118 ff.
2091 Ders., 5 ff.
2092 Ders., 32, 41, 46 ff. und 83.
2093 Vgl. dritter Teil, VIII. Kapitel, A.2.3.
2094 Buchner, 103 ff. und 201 ff.

korrigierenden Ausnahmebestimmungen mehr oder weniger weitreichend zur Relativierung eingesetzt würden.

1646 Zech vertritt in diesem Zusammenhang, dass nicht die Informationsfreiheit als Ausgangspunkt, sondern vielmehr die gesetzliche Beschränkung der Datenverarbeitung rechtfertigungsbedürftig sei.[2095] Als eine Art vorrechtlichen und naturgegebenen Zustand beschreibt Druey die Informationsfreiheit. Die informationelle Selbstbestimmung sei quasi konträr zur Freiheit der Information.[2096]

1647 Eine gesetzliche Beschränkung der Datenverarbeitung mit einer Verbürgung des Rechts auf informationelle Selbstbestimmung für den privaten Bereich legitimiert Buchner unter Anwendung der *ökonomischen Analyse des Rechts*. Gemäss einer solchen ginge es darum, über das datenschutzrechtliche Regime eine *effiziente Informationsverteilung* hinsichtlich personenbezogener Angaben zu erreichen.[2097] Informationen, auch personenbezogene Angaben, sollen dorthin gelangen, wo sie am höchsten bewertet werden. Dies zu bewerkstelligen sei primäre Angelegenheit des *Marktes*. Dem Recht komme eine instrumentelle Funktion zu, indem es sich über die Zulässigkeit des Austausches von Ressourcen und Rechten äussere. Die kommerzielle Verwertung personenbezogener Angaben sei ein Faktum und das Recht habe darüber zu befinden, ob es dieser Realität einen angemessenen Rahmen zur Verfügung stellen wolle oder vielmehr die Kommerzialisierung verhindere resp. verbiete.[2098] Weil Daten resp. Rechte an Daten aufgrund von Markttransaktionen dorthin gelangen, wo ihnen die höchste Bewertung zugemessen würde, müsse das Datenschutzrecht Rahmenbedingungen schaffen. Diese sollen sich darauf konzentrieren, Hindernisse für einen reibungslosen Austausch von Informationsrechten abzubauen.[2099] Einzig und allein dann, wenn dem Einzelnen ein Recht an «seinen» Daten zugesprochen werde, sei es realistisch, dass ebendieses Recht im Folgenden durch Markttransaktionen dorthin gelange, wo es ggf. höher bewertet würde.[2100] Im Ergebnis plädiert Buchner für einen privatautonomen Interessenausgleich im Datenschutzrecht des privaten Sektors.

1648 Wenn nicht von einem Recht auf informationelle Selbstbestimmung, stattdessen von der Freiheit der Information zugunsten der Allgemeinheit ausgegangen würde, steigerten sich die Transaktionskosten für den Betroffenen drastisch. Es obliege dann dem Individuum, herauszufinden, wer welche Daten hat etc.[2101] Dagegen fielen die Transaktionskosten kaum ins Gewicht, sofern als Ausgangspunkt das

2095 Zech, 145 ff., insb. 147.
2096 Druey, 77 ff., insb. auch 92.
2097 Vgl. Buchner, 176.
2098 Ders., 202 ff., insb. 208 ff.
2099 Ders., 179.
2100 Ders., 180.
2101 Vgl. Ders., 177 ff.

Recht des Einzelnen an seinen Daten festgeschrieben würde. Prohibitiv hohe Transaktionskosten würden hier nicht verursacht.

Nachdem Buchner aufgrund einer ökonomischen Analyse des Rechts für die Anerkennung eines Rechts des Einzelnen an seinen Daten plädiert, befasst er sich mit den Einwänden, die gegen dieses ins Feld geführt werden können.[2102] 1649

Erstens reflektiert Buchner das Machtungleichgewicht zwischen Datenverarbeitenden und Datensubjekt.[2103] Für das Datensubjekt sei es, so lautet eine gängige Argumentation, nicht relevant, ob es der Staat oder ein privatwirtschaftliches Unternehmen sei, das Personendaten verarbeitet. Diese Machtasymmetrie führt dazu, dass eine Maxime des privatautonomen Interessenausgleichs im Datenschutz kritisch hinterfragt wird. Buchner führt die grundlegende und traditionsreiche Anerkennung von Differenzen zwischen dem öffentlichen und dem privaten Sektor ins Feld. Sie sei gerade im Rahmen der Grundrechtssituation relevant: Im privaten Verhältnis kommen die Grundrechte nicht direkt zur Anwendung. Immerhin haben sie von der zivilrechtlichen Gesetzgebung integriert zu werden. Hierbei seien die verschiedenen privatrechtlichen Akteure und ihre Positionen zu berücksichtigen. Es sei im privaten Sektor nicht nur das Interesse des Datensubjektes, sondern namentlich auch die Interessen auf Informations- sowie Wirtschaftsfreiheit vonseiten der Datenverarbeitenden, welche in die Rechtsgestaltung einzufliessen haben. Das Verhältnis zwischen Bürger und Staat sei anders geartet. Die Machtasymmetrie zwischen Staat und Bürgerinnen resp. Bürgern äussere sich insb. darin, dass der Staat seine Forderungen mittels *Zwangs* durchsetzen könne. Das gelte ebenso für die Personendatenverarbeitung. Ein solches Instrumentarium hätten private Datenverarbeitende dagegen nicht. 1650

Zweitens befasst er sich mit der Herausforderung, welche der Differenzierung der Normen für den privaten gegenüber dem öffentlichen Bereich entspringt. Sie besteht in der *Abgrenzung* der beiden Bereiche gegeneinander resp. in der Verhinderung oder Zulassung von Informationsflüssen *zwischen den beiden Bereichen*.[2104] An dieser Stelle werden die Relevanz der Bereichsdifferenzierung sowie eine Betrachtungsweise, die Datenströme und namentlich ihren Transfer zwischen verschiedenen Bereichen in den Blick nimmt, augenscheinlich. Dort, wo eine mildere Regulierung gilt, können umfassendere Datenbestände generiert werden. Entsprechend gibt es Zugriffsbegehrlichkeiten vonseiten der Personendatenverarbeitenden, die unter dem strengeren Datenschutzregime stehen. Buchner sieht in diesem Befund allerdings keinen Grund, von der Idee der Privat- 1651

2102 Buchner, 182 f.
2103 Ders., 103 ff.; kritisch zum Transfer einer Vorstellung, wonach das Machtungleichgewicht zwischen Bürger und Staat vergleichbar ist zu demjenigen zwischen Privaten und Privaten, Vesting, in: Ladeur (Hrsg.), 155 ff., 158 ff.
2104 Buchner, 72 ff.

autonomie für den privaten Bereich abzuweichen und diese einer «freiheitlicheren» Ordnung als dem öffentlichen Bereich zu unterstellen. Vielmehr fordert er die spezifische Adressierung der Mobilität personenbezogener Angaben *zwischen den beiden Sektoren*.[2105]

1652 Nach der Auseinandersetzung mit den Einwänden gegen sein Konzept lautet sein Plädoyer: Das Datenschutzrecht für den privaten Sektor soll dem Einzelnen *den immateriellen und materiellen Wert der preisgegebenen Informationen zuweisen*. Damit erlange das Datensubjekt die Chance, den Wert der sich auf die eigene Person beziehenden Daten abzuschätzen und damit als ernst zu nehmender Verhandlungspartner die informationelle Selbstbestimmung nicht unter Wert preisgeben zu müssen. Trotz des unbestritten vorhandenen Informations- und Machtungleichgewichts zwischen den privatrechtlichen Akteuren (das auch in anderen Privatrechtsgebieten bekannt sei) müsse es die Angelegenheit der Privatsubjekte bleiben, individuell und einzelfallbezogen darüber zu befinden, ob sie ihre personenbezogenen Angaben preisgeben oder nicht.[2106] Das Aufblähen gesetzlicher Ausnahmetatbestände, namentlich überwiegender Interessen, dränge dagegen die informationelle Selbstbestimmung an den Rand und münde in eine *Exklusion des Subjektes* sowohl im demokratischen (mitbestimmenden) als auch ökonomischen (Realisierung des pekuniären Wertes) Aspekt der Verarbeitung seiner personenbezogenen Angaben. Je schlanker die Ausnahmetatbestände, desto weniger laufe der Datenschutz am Willen des Einzelnen vorbei oder, anders gewendet, desto besser werde das *Datensubjekt in die Verarbeitungsprozesse integriert* – in demokratischer wie in wirtschaftlicher Hinsicht.[2107]

1653 Die Idee der Einbettung von Verwertungsbefugnissen in das Persönlichkeitsrecht wurde in der Schweiz namentlich von Büchler – allerdings nicht spezifisch für das Datenschutzrecht – dargestellt. Sie wies darauf hin, dass die Betonung des Autonomiegedankens als ein im Persönlichkeitsrecht angelegter Aspekt einen Ausweg präsentiere. Ein Ausweg aus der Aporie des Verwertungsrechts, in welchem ein ideell verhaftetes Persönlichkeitsrecht feststecke.[2108]

1654 Die Diskussionen im Zusammenhang mit einer ideellen Natur des Persönlichkeitsrechts interessiert in der Schrift Buchners eher am Rande. Ebenso die Frage, ob infolge der faktischen Kommerzialisierung personenbezogener Angaben eine Verlagerung auf ein (immaterielles) Eigentumsrecht geboten scheint. Buchner weist darauf hin, dass es Einwände gegen die Kommerzialisierung der informationellen Selbstbestimmung gebe, die in einer weiteren Debatte rund um die Kommerzialisierung von Persönlichkeitsgütern eine prominente Position in

2105 Buchner, 74 f.
2106 Ders., 106 ff.
2107 Ders., 202 ff.
2108 Hierzu Büchler, AcP 2006, 300 ff., 312 ff.

der persönlichkeitsrechtlichen Auseinandersetzung einnähmen. Die Diskussion um die Kommerzialisierung der Persönlichkeit, so Buchner, sei eine über das Verhältnis von Recht und Wirklichkeit.[2109]

In diesem Zusammenhang sei auf Flückiger hingewiesen. Er statuiert einige Jahre später für die Schweiz zum Verhältnis von (Datenschutz-)Recht, Technologie und Wirklichkeit: 1655

> «La technologie modifie inexorablement les habitudes sociologiques communicationelle. Le droit de la protection des données ne peut pas être un droit conservateur d'un passé nostalgique; c'est un droit dynamique condamné à évaluer avec son temps.»[2110]

Wirklichkeit in dem Sinne, wonach es um die Position(ierung) des Rechts zu faktischen Entwicklungen und Realitäten geht, nicht Wirklichkeit im Sinne einer quasi naturrechtlichem Denken verpflichteten Suche nach einer «Natur» des Persönlichkeitsrechts, genauer einer «ideellen Natur» des Persönlichkeitsrechts. 1656

Buchner richtet den Fokus nicht auf die dogmatischen Raffinessen des Diskurses zur Kommerzialisierung des Persönlichkeitsrechts. Vielmehr zielt der Autor mit seiner Analyse darauf ab, Antworten auf das datenschutzrechtliche Kernproblem – das faktische Vollzugsdefizit – zu formulieren.[2111] Hieran angekoppelt solle auch *der Exklusion des Datensubjektes* aus den Prozessen wirksam entgegengetreten werden.[2112] Dies werde erreicht über ein Regime, in welchem sich die *Rechtsposition des Subjektes nicht auf retrospektiv ausgerichtete Reaktionsinstrumente* wie das Auskunftsrecht, Löschungsbegehren oder die persönlichkeitsrechtlichen Klagen beschränke. Vielmehr sei die (pro)aktive Mitwirkung des Datensubjektes zu gewährleisten. Diese müsse von Anfang an für die Verarbeitungsprozesse gelten.[2113] Datenverarbeitungen basierend auf der Legitimation überwiegender Interessen, die ohne Integration des Datensubjektes stattfinden, sollen weitgehend ersetzt werden. Sie sollen einem System weichen, in welchem die Betroffenen resp. Datensubjekte als nicht ignorierbare Informations- und Kommunikationspartner auftreten würden.[2114] Dies bewerkstellige eine Datenschutzordnung, die den Betroffenen in ihr Zentrum oder an den Anfang stelle und gemäss der grundsätzlich das Einverständnis des Betroffenen notwendig sei: Mit einem Entscheidungsvorrecht des Datensubjektes, so Buchner, würden viele der Schwächen des Datenschutzes beseitigt. Denn ein Datenverarbeiter, der auf die Einwilligung des Subjektes angewiesen sei, werde viel dafür tun, das 1657

2109 Buchner, 185 ff.
2110 Flückiger, PJA 2013, 837 ff., 842.
2111 Vertiefend hierzu dritter Teil, VII. Kapitel, A.
2112 Keine Formulierung drücke das Problem symbolhafter aus, als dass es darum ginge zu verhindern, dass die Person, das Datensubjekt, zum Datenobjekt degradiert werde, vgl. Buchner, 130; für die Schweiz bereits BBl 1988 413 ff., 417.
2113 Buchner, 130.
2114 Ders., 131.

erforderliche Vertrauen zu generieren und somit faire und transparente Verarbeitungsprozesse zu implementieren.[2115]

1658 An dieser Stelle habe eine Infrastrukturverantwortung des Staates anzusetzen. Die Datenschutzgesetzgebung habe die Rahmenbedingungen für die faire und transparente Verarbeitung festzulegen. Buchner vertritt damit die Überzeugung, wonach es die Marktmechanismen seien, die im Falle eines *echten Entscheidungsvorrechts des Betroffenen* eine transparente, faire und korrekte Datenverarbeitung sicherstellen würden. An die Stelle staatlicher Regulierung trete die des Marktes, wobei den Ausgangspunkt ein Selbstbestimmungsrecht des Einzelnen darstellen solle. Das dem Einzelnen zukommende Recht an seinen Daten begründe dessen Einbindung und Mitbestimmung und verhindere seine Degradierung zum Datenverarbeitungsobjekt.[2116]

1659 Spezifisch datenschutzrechtlich verwirft Buchner mit seinem Modell der informationellen Selbstbestimmung für den privaten Sektor einen paternalistischen Ansatz. Es ginge in einem freiheitlichen Staatssystem nicht an, dass der Staat Datenverarbeitungen bevormundend reguliere.[2117] In einer pluralistischen Gesellschaft sei es (ähnlich wie im Familienrecht, *Anmerkung der Verfasserin*) nicht am Staat, Gesetze an einem Idealbild des «zurückhaltend-verantwortungsvollen» Einzelnen zu konstruieren und diesen dergestalt zu schützen oder aber auch im Umgang mit Personendaten zu beschneiden. Aufgabe des Rechts sei es, Rahmenbedingungen zu schaffen, bei denen sich der Betroffene weitestgehend in der Lage sieht, seine eigenen Interessen selbstbestimmt zur Geltung zu bringen. Dagegen ginge es nicht darum, dass der Staat festlege, was der Einzelne an Privatem preisgeben dürfe.[2118]

1660 Im Ergebnis plädiert Buchner für die *Ausdifferenzierung zwischen öffentlichem und privatem Sektor (Dualismus)*. Die Inklusion des Datensubjektes soll durch die Anerkennung eines Rechts auf informationelle Selbstbestimmung verbürgt werden. Dieses Recht auf informationelle Selbstbestimmung im privaten Bereich beinhaltet sowohl eine ideelle als auch wirtschaftliche Komponente. Im entwickelten Regime kommt der privatautonomen Ausgestaltung datenschutzrechtlicher Rechte und Pflichten zwischen Betroffenen und Datenverarbeitenden zentrale Bedeutung zu.[2119]

1661 Indem die informierte Einwilligung und informationelle Selbstbestimmung aufgewertet werden soll und damit die Abwägungstatbestände zurückgedrängt wer-

2115 Buchner, 132.
2116 Ders., 133.
2117 Ders., 106 ff.
2118 Ders., 113 ff.
2119 Ders., 114; vgl. zum Verhältnis von wirtschaftlichen und ideellen Komponenten im Persönlichkeitsrecht und Immaterialgüterrecht allgemeiner auch Ullmann, AfP 1999, 209 ff.

den, solle eine markant bessere Inklusion des Datensubjektes stattfinden. Die personendatenverarbeitenden Stellen sind mit der prinzipiellen Zuordnung von Entscheidungs- wie Verwertungskompetenzen bei den Datensubjekten im Zugzwang, deren Vertrauen zu gewinnen und datenschutzrechtskonform zu agieren. Eine Korrektur oder Ergänzung dieses für das allgemeine privatrechtliche Datenschutzregime geltenden Modells ist mittels hinreichend spezifischer bereichs- und spezialgesetzlicher Regelungen zu bewerkstelligen. Die Institutionalisierung von sog. Datentreuhändern, welche vergleichbar zu den Verwertungsgesellschaften im Immaterialgüterrecht in kollektiver Weise die datenschutzrechtlichen Interessen für die Datensubjekte ausüben, runden aus prozeduraler Sicht das Konzept eines privatautonomen Interessenausgleichs mit einem Recht auf informationelle Selbstbestimmung im Privatrecht ab.

1662 Buchner plädiert somit zunächst für eine Differenzierung des Datenschutzrechts für den privaten gegenüber dem öffentlichen Bereich und damit für ein dualistisches Modell.[2120] Eine weitere Ausdifferenzierung soll durch bereichsspezifische Normen erfolgen. Die DSGVO vollzieht dagegen den Übergang zu einem monistischen Regime. Aus einer subjektivrechtlichen Perspektive betrachtet löste Buchner das Datenschutzrecht für den privaten Bereich aus einer abwehrrechtlichen, defensivrechtlichen Konstruktion, indem er für ein im Persönlichkeitsrecht begründetes Recht auf informationelle Selbstbestimmung eintrat. Dieses Recht sollte zugleich auch eine Verwertungskomponente integrieren. Insofern tritt Buchner für ein Recht an eigenen Daten in einer monistischen Struktur ein, wobei diese Verbindung von persönlichkeitsrechtlichem und vermögensrechtlichem Gehalt Parallelen zum Urheberrecht aufweist.[2121] Die Studie von Buchner hat einen bedeutsamen Beitrag zur dogmatischen Durchdringung des Datenschutzrechts geleistet. Sie zielt darauf ab, ein Konzept zu entwickeln, welches dem Vollzugsdefizit wirksam entgegentreten soll.

1663 Seit dem Erscheinen von Buchners datenschutzrechtlichem Grundlagenwerk haben sich mehrere weitere rechtswissenschaftliche Studien *vertieft mit der informationellen Selbstbestimmung im Datenschutzrecht und damit den Konstruktionen informierter Einwilligung* befasst. Mit diesen Studien kann zugleich attestiert werden, dass das Datenschutzrecht wissenschaftlich sein Nischendasein verlässt. Specht analysiert die Konsequenzen der Ökonomisierung informatio-

2120 Dazu, dass in dualen Systemen eine krude Version eines systemischen Ansatzes zu lesen ist, Nissenbaum, 141, wobei die Autorin gegen ein hegemoniales Kontrollrecht des Datensubjektes eintritt, 2.

2121 Buchner, 202 ff.; vgl. zum Urheberrecht als einheitlichem Recht mit doppelter Funktion Wielsch, 12; vgl. auch Weichert, in: Bäumler (Hrsg.), 158 ff., 176 ff., insb. 182 ff.; vgl. zum Kontrollverlust an Informationen, der sich im Bereich des Datenschutzrechts wie des Urheberrechts als Bereiche des Themenfeldes Recht und Technik zeige, wobei ein Kontrollrecht resp. privacy als property ein Lösungsansatz sei, auch Lessig, Soc. Res. 2002, 247 ff., insb. 252 ff.; vgl. zu den Einwilligungskonstruktionen in Situationen, in denen über Personendaten als Gegenleistung verfügt wird, Kilian, in: Stiftung Datenschutz (Hrsg.), 191 ff., 198 ff.

neller Selbstbestimmung und vertritt, dass mit dem Recht auf informationelle Selbstbestimmung eine güterrechtliche Zuweisungsentscheidung erfolge.[2122] Liedke beschäftigt sich in seiner Doktorthesis aus dem Jahr 2012 mit der Rechtsnatur der datenschutzrechtlichen Einwilligung, ihren Gültigkeitsvoraussetzungen sowie dem Widerruf, wobei Letzterer spezifisch in seiner elektronischen Form betrachtet wird. Sodann setzt er einen ersten Schwerpunkt auf die Einwilligung im Kontext des Arbeitsverhältnisses sowie in der Werbung. Die Dissertation von Rogosch, erschienen 2013, analysiert die Voraussetzungen für die *gültige Einwilligung*. Insofern konstatiert sie die Uneinheitlichkeit der Gültigkeitsvoraussetzungen in Einwilligungsvorgaben im deutschen Recht und kritisiert die ungenügende Integration der europarechtlichen Vorgaben. Aus dem gleichen Jahr stammt die Doktorarbeit von Lindner, die sich ebenso mit den Wirksamkeitsvorgaben der datenschutzrechtlichen Einwilligung auseinandersetzt. Ein Schwerpunkt der Studie widmet sich den Informationen, die in AGB enthalten sein müssen, um die Voraussetzung der Informiertheit des Datensubjektes zu gewährleisten. Maisch widmet seine Doktorarbeit 2015 der informationellen Selbstbestimmung in Netzwerken. Konzeptionell in Frage gestellt wird die Einwilligung als datenschutzrechtliches Institut in Anbetracht der Realitäten, in der sie fungieren muss, durch Radlanski in seiner Dissertation aus dem Jahr 2016.[2123]

1664 Auch in der Schweiz widmen sich zwei Dissertationen dem Recht auf informationelle Selbstbestimmung und der datenschutzrechtlichen Einwilligung. Beide befassen sich in erster Linie mit grund-, verfassungs- und völkerrechtlichen Fragen. Waldmeier weist – neben einer praxisbezogenen Untersuchung für den Gesundheitsbereich – auf Defizite datenschutzrechtlicher Einwilligungskonstruktionen hin. Sie eruiert sodann Bedingungen und Voraussetzungen, um die Wirksamkeit der datenschutzrechtlichen Selbstbestimmung zu effektuieren.[2124] Zutreffend richtet sich ihre Kritik auf die unreflektierte Übertragung des Konzepts der informationellen Selbstbestimmung, wie es das Bundesverfassungsgericht geprägt hatte, auf die Schweiz.[2125] Die Autorin schlägt zur Bewältigung insb. den Ausbau des kollektiven Rechtsschutzes vor, die Herabsetzung der Prozessrisiken für Einzelpersonen, die Pflicht zur Herausgabe von unrechtmässig erlangten vermögenswerten Vorteilen.[2126] Die im Jahr 2017 erschienene Dissertation von Fasnacht setzt sich spezifisch mit der datenschutzrechtlichen Einwilligung auseinander. Der Autor beleuchtet die völker- und verfassungsrechtlichen Grundlagen im internationalen wie im nationalen Recht. Nicht genauer analysiert wird die Konstruk-

2122 Specht, 292, 40 ff. zur Einwilligungskonstruktion und 78 ff. zur Übertragbarkeit und Verwertbarkeit von Persönlichkeitsrechten resp. Personendaten als Gegenstand des Rechtsverkehrs.
2123 Radlanski, 8 ff.
2124 Waldmeier, 48, 128 ff.
2125 Dies., 44 ff.
2126 Dies., 130 ff.

tion für das Datenschutzrecht im Privatbereich. Fasnacht weist, wie bereits Waldmeier, für das Datenschutzrecht zunächst auf die Missverständlichkeit der Behauptung hin, wonach die Schweiz ein Recht auf informationelle Selbstbestimmung verbürge.[2127] Zudem betrachtet der Autor die völker- und verfassungsrechtlichen Vorgaben mit Blick auf die gültige datenschutzrechtliche Einwilligung im schweizerischen Recht.[2128] Weiter wird die Tauglichkeit von Einwilligungsvorgaben in spezifischen Konstellationen diskutiert.[2129] Eine Auseinandersetzung mit den Herausforderungen, denen die datenschutzrechtliche Einwilligung begegnet, leitet seine Schrift zu möglichen Lösungsansätzen über. Hierbei plädiert er für die *differenzierte Ausgestaltung und Positionierung der Einwilligung*, wozu auch das Einwilligungsverbot gehört, sowie für flankierende Massnahmen.[2130] In diesem Sinne lassen sich in der Schrift, weil sie eine bereichsspezifische Differenzierung mit Blick auf Einwilligungskonstruktionen fordert, Elemente feststellen, welche die Systembezogenheit und -relevanz des Datenschutzrechts anerkennen.

Offensichtlich werden mit den jüngeren datenschutzrechtlichen Studien die *informationelle Selbstbestimmung sowie Einwilligungskonstruktionen* in das Zentrum gestellt. Die Einschätzungen allerdings divergieren, wobei gerade in den jüngsten Studien Kritik am Selbstbestimmungsparadigma aufkommt: So finden sich ebenso kritische Beiträge in Bezug auf die Funktionstüchtigkeit von Einwilligungskonstruktionen im Datenschutzrecht. Diese Schriften bilden einen *Kontrapunkt*, welche die informationelle Selbstbestimmung und damit die informierte sowie freiwillige Einwilligung des Datensubjektes in Personendatenverarbeitungen als Dreh- und Angelpunkt datenschutzrechtlicher Lösungsansätze für das Datenschutzrecht auch im privaten Sektor präsentieren. Dass die informierte Einwilligung nicht pauschal als Rezept zur Beseitigung sämtlicher datenschutzrechtlicher Herausforderungen gelesen werden kann, wird von Nissenbaum und Barocas/Nissenbaum vertreten.[2131] 1665

Abrundend und zugleich überleitend zurück zu Buchner. Der Autor tritt in dezidierter Weise für ein Recht auf informationelle Selbstbestimmung und einen privatautonomen Interessenausgleich für das Datenschutzrecht des privaten Sektors ein. Sein Fokus liegt auf dem *Rechtssubjekt*, dem ein subjektives Recht an 1666

2127 Fasnacht, N 99 ff., insb. N 120 ff. mit Hinweis auch auf Belser und Gächter/Egli, Jusletter vom 6. September 2010.
2128 Fasnacht, N 214 ff.
2129 Ders., N 548 ff.
2130 Ders., N 419 ff. und N 548 ff.
2131 Nissenbaum dazu, dass ein Kontrollrecht an Personendaten durch Datensubjekte nicht als hegemoniales und pauschales Lösungsinstrument datenschutzrechtlicher Probleme gesehen werden kann, 2 und 231; Barocas/Nissenbaum, 1 ff., 4 ff.; dazu, dass Rechte auf Kontrolle an Personendaten resp. privacy als property Widerstand mit verschiedenen, guten Argumenten findet, m. w. H. Lessig, Soc. Res. 2002, 247 ff., 285 ff.

eigenen Daten zugestanden werden soll.[2132] Nach seiner Konstruktion hat dieses, trotz einer persönlichkeitsrechtlichen Anknüpfung, gleichzeitig demokratische wie ökonomische Aspekte zu inkludieren.

1667 Eine andere Herangehensweise und Perspektive wählt Zech, dessen Studie sich nicht auf Personendaten und das Datenschutzrecht beschränkt. Zechs Konzept wird sogleich vorgestellt. Sein Augenmerk gilt der Information als *Gut resp. Rechtsobjekt*. Die Betrachtung der Habilitationsschrift von Zech erfolgt – weil sie eine *Stufenordnung der Zuweisungsbefugnisse vorsieht* – nach der Auseinandersetzung mit dem Persönlichkeitsparadigma, aber vor derjenigen mit dem Eigentumsparadigma. Die hier gewählte Systematik ist damit keineswegs bloss Chronos geschuldet. Vielmehr ist der Einschub von Zechs Erkenntnissen zwischen die Titel zum persönlichkeitsrechtlichen und zum eigentumsrechtlichen Ansatz betreffend Personendaten ebenso sachlogisch motiviert: Das informationsrechtliche Grundlagenwerk vermittelt einbettende und erweiterte Erkenntnisse, die für das Verständnis des Eigentumsparadigmas produktiv sind. Zudem stellt Zech eine ausdifferenzierte Stufenordnung bezogen auf verschiedene Informationskategorien vor, womit ebenda persönlichkeits- wie eigentumsrechtliche Konstruktionen thematisiert werden.

3. Die Trias informationeller Güter mit Stufenordnung gemäss Zech

1668 Mit *Informationen als Gütern* und Zuordnungsfragen hat sich grundlegend sowie richtungsweisend Zech in seiner Habilitationsschrift mit dem Titel «Information als Schutzgegenstand» befasst.[2133] Es handelt sich dabei nicht um eine datenschutzrechtliche Untersuchung im engeren Sinne. Gleichwohl werden *Zuordnungsfragen* bezüglich Personendaten diskutiert. Der Autor präsentiert vorab eine Nomenklatur für Informationsgüter resp. einen juristischen Informationsbegriff.[2134] Basierend auf der Kategorisierung von *drei Informationsarten* beschreibt er, wie Informationen rechtlich durch absolute Rechte geschützt werden. Insofern zeigt er, dass ausschliessliche Zuweisungen nicht nur durch Rechte des geistigen Eigentums, sondern auch durch das Persönlichkeitsrecht resp. in anderen Rechtsgebieten erfolgen.[2135] Die Studie befasst sich in systematischer Weise mit etablierten Kategorien des Zivil- sowie Immaterialgüterrechts und korreliert sie mit den spezifischen Herausforderungen bezüglich Informationen

2132 Vgl. neuerdings zur digitalen Rechtssubjektivität neuer Aktanten, insb. mit Blick auf Verantwortungslücken, Teubner, AcP 2018, 155 ff.
2133 Später zu Verträgen über digitale Güter vgl. Grünberger, AcP 2018, 213 ff.
2134 Zech, 13 ff.; zu einem Informationsbegriff auch Roth, 5 ff., welcher neben der umgangssprachlichen auch die juristische Begriffsbildung darstellt; zur Heterogenität des Informationsbegriffs Gasser, 48 ff.
2135 Zech, 63 ff.

als Güter. Zech weist namentlich darauf hin, dass die für die analoge Welt und körperliche Sachen entwickelten Kategorien nicht *telle-quelle* analog in das Informationsrecht transportiert werden sollten.[2136] Hierauf basierend entwickelt Zech ein rechtliches Schutzregime für Informationen mit einer ausdifferenzierten Zuweisungsordnung. Eine *Tour d'Horizon* über seine Studie:

Zech beginnt mit der Reflexion des Güterbegriffs. Der *Güterbegriff* umfasse Er- 1669
scheinungen von Wirtschaftssystemen.[2137] *Drei Elemente* nennt er als konstitutiv, damit eine Entität als Gut zu qualifizieren sei: erstens die Nützlichkeit mit der Funktion der Interessenbefriedigung, die sich nicht auf ein wirtschaftliches Interesse beschränkt, zweitens die vorrechtliche Existenz und drittens die Existenz des Gutes ausserhalb der Person. Nach verbreiteter Ansicht gelten daher Persönlichkeitsgüter nicht als echte Güter.[2138] Zech spricht sich für die Beibehaltung des Erfordernisses der Abtrennbarkeit von der Person des Inhabers aus.

Gleichwohl zeige die Diskussion um die Kommerzialisierung von Persönlichkeits- 1670
rechten, dass gewisse Handlungen bezüglich einer Person «Gegenstände» betreffen, die zwar mit der Person verbunden seien, deren faktische Abtrennbarkeit indes bejaht werden könne. Als klassisches Beispiel wird das Abbild einer Person aufgeführt.[2139] Die Differenzierung zwischen nicht abtrennbaren und abtrennbaren Persönlichkeitsgütern spiele für die Behandlung von Informationsgütern eine wichtige Rolle. Hinzu trete der Begriff des wirtschaftlichen Wertes, der ein Indiz für die Knappheit eines Gutes sei und auch Relevanz für den Vermögensbegriff habe.[2140] Für die Beantwortung der Frage, wann Daten als Objekt oder Gegenstand bezeichnet werden können, sieht Zech die Anerkennung von Information als Gegenstand im Alltag als wesentlich an.[2141]

Nachdem er den Begriff des Gutes mit Bezug auf Information dargelegt hat, 1671
reflektiert er die *drei Gruppen von Informationen* hinsichtlich ihres Gütercharakters. Insofern macht sich der Autor linguistische Modelle zunutze, insb. die Erkenntnisse von De Saussure, zudem Morrison mit seinem semiotischen Dreieck. Die hierauf basierende und von Zech zur Bewältigung informationsrechtlicher Herausforderungen vorgeschlagene Kategorisierung hat breite Aner-

2136 Zech, 64, 91 ff.; vgl. zu den Informationsgütern mit den verschiedenen Narrativen zu den Rechten des geistigen Eigentums Mayer-Schönberger, Va. J.L. & Tech., 1 ff.
2137 Zech, 46.
2138 Ders., 48; zur Begrifflichkeit insb. von digitalen Gütern weiter Grünberger, AcP 2018, 213 ff., 223 ff.
2139 Zech, 46; zum Recht am eigenen Bild Bächli, *passim*; vertiefend zweiter Teil, VI. Kapitel, 6.2.
2140 Zech, 49.
2141 Ders., 36.

kennung und Rezeption gefunden.[2142] Unterschieden wird eine *Trias von Informationskategorien: syntaktische, semantische und strukturelle Informationen*.[2143]

1672 *Syntaktische Informationen* zeichnen sich dadurch aus, dass sie auf der Zeichenebene abgegrenzt werden. Die syntaktische Ebene meint die Codierung von den in Daten vorhandenen Informationen, und zwar in einer Formalsprache. Es geht mit anderen Worten um die Zeichenebene, die Buchstaben, Zeichen oder – in der digitalen Welt und mit Blick auf digitale Güter – den digitalen Binärcode (0101).[2144]

1673 Die Nützlichkeit von Daten allerdings manifestiere sich erst mit ihrer *semantischen Komponente*. Semantische Informationen weisen einen inhaltlichen Bedeutungsgehalt auf. Das Datenschutzrecht bezieht sich auf die semantische Dimension von Daten: Die Angaben resp. Daten haben stets einen Personenbezug; das DSG normiert den Umgang mit den sich auf bestimmte resp. bestimmbare Personen beziehenden Informationen. Personenbezogene Angaben stellen die kleinste Einheit von Aussagen über eine Person dar, die vom Datenschutzrecht adressiert werden. Personendaten haben somit eine semantische, persönlichkeitsrechtlich relevante Dimension. Umstritten sei, ob durch das Datenschutzrecht den persönlich Betroffenen eine vermögenswerte Rechtsposition eingeräumt werden solle. Faktisch aber handle es sich bei persönlichen Daten um ein Gut, das gehandelt wird.[2145] Dazu gehörten das Abbild, das gemäss § 22 KUG als Gut anerkannt wird, zudem Nachrichten über Prominente, Kreditauskünfte und weitere Informationen von Informationsbrokern, die zu Informationsgütern geworden sind.[2146] Exemplarisch für semantische Informationen sind darüber hinaus technische Lehren, Patente, Aussagen über ein Unternehmen und Unternehmensgeheimnisse.[2147] *Personendaten werden folglich unter den Begriff der semantischen Angaben* subsumiert, wobei das Datenschutzrecht insofern den Betroffenen, den Datensubjekten, Befugnisse zuweist. Allerdings erschöpft sich die privatrechtliche Wirkung des Datenschutzrechts als Persönlichkeitsrecht regelmässig in Abwehrrechten. Dies, obschon Personendaten in der Regel Gütercharakter zukomme.[2148]

2142 Vgl. z. B. durch Grünberger, AcP 2018, 213 ff., 227 ff.; Auer, ZfpW 2019, 130 ff.; Amstutz, AcP 2018, 438 ff.

2143 Zech, 37 ff.; hierzu ebenso m. w. H. bereits Hoeren, 9 ff.; zum Informationsbegriff und dessen Umsetzung im Recht sodann auch Roth, 5 ff. und 47 ff., der alsdann für ein «einheitliches Recht auf Information» in Gestalt eines Stammrechts eintritt, 182 ff.; das Konzept rezipierend Bijok, 28 ff.

2144 Zech, 54.

2145 Ders., a. a. O.

2146 Ders., 53 f.

2147 Ders., 52; zu sog. Wirtschaftsgeheimnissen und informationellen Zuordnungsfragen grundlegend bereits Hauck, 11 ff.

2148 Zech, 215 ff.

Diesem Befund entspringen auch Forderungen auf Anerkennung eines Rechts an eigenen Daten.[2149]

Die *dritte Kategorie von Informationsgütern* wird als *strukturelle Information* bezeichnet. Sie ist untrennbar mit der Verkörperung der in den Daten vorhandenen Information auf einem Datenträger verbunden. Es geht um die Information auf einem Träger, einem körperlichen Datenträger. Ein Beispiel bilden die auf einer Festplatte gespeicherten Informationen.[2150] Auch die CD oder DVD als Datenträger für digitale Informationen können genannt werden. Typisch für die Digitalisierung ist eine *Dematerialisierung*, das Verschwinden der körperlichen Komponente resp. des Datenträgers. Was bleibt, sind *zwei Schichten* – die syntaktische Ebene und die semantische Ebene. Beide Schichten sind immateriell. Somit lässt sich ein Stufenmodell nicht nur für Zuordnungsbefugnisse definieren. Ebenso lassen sich für die Informationsgüter verschiedene Schichten, vergleichbar mit einer Zwiebel, herausschälen.[2151] 1674

Die von Zech in den Rechtsdiskurs transportierte Trias von *Informationsbegriffen* – strukturelle, semantische und syntaktische Information – ermöglicht eine Abgrenzung unterschiedlicher Informationsgüter.[2152] Zech kommt zu dem Ergebnis, dass alle drei Informationskategorien als Güter in Erscheinung treten können. Der zweite und dritte Teil von Zechs Habilitationsschrift legt einen Boden anhand der rechtsdogmatischen Grundlagen unter den Titeln «Verdinglichung – Information als Gegenstand ausschliesslicher Rechte»[2153] sowie «Abstraktion – Umgang mit Information im Wandel».[2154] Diese Ausführungen werden einer differenzierenden Analyse von Zuordnungsfragen für jede der drei Kategorien von Informationsgütern vorangestellt.[2155] 1675

Insofern zeichnet der Autor ein detailliertes Panorama zu *Theorie(n) und Dogmatik subjektiver Rechte*. Er charakterisiert Ausschliesslichkeitsrechte anhand von *drei Merkmalen:*[2156] dem *subjektivrechtlichen* Charakter, der *Abwehrfunk-* 1676

2149 Zech, 215 ff.
2150 Ders., 57.
2151 Vgl. Grünberger, AcP 2018, 213 ff., 223 ff.; zum Bild der Zwiebel Pfaffinger, Digitale Güter: Knotenpunkte des Privat- und Zivilrechts, Vortrag vom 6. November 2019, HSG/Universität St. Gallen.
2152 Zech, 51, zusammenfassend zu den Abgrenzungen der drei Informationsbegriffe, 45.
2153 Ders., 63 ff.; zur Verdinglichung und der Idee von Informationen als Objekten Druey, in: Kramer/Nobel/Waldburger (Hrsg.), 589 ff., 600 f.; Ders., in: Brem/Druey/Kramer/Schwander (Hrsg.), unter Hinweis auf Wiener zu dem Konzept, Information als Tertium neben der Materie und der Energie zu betrachten, 379 ff., 379; hierzu auch Dreier, in: Bizer/Lutterbeck/Riess (Hrsg.), 65 ff., 68.
2154 Zech, 167 ff.
2155 Dazu, dass das Informationsrecht die Zuordnung resp. den freien Zugang zu Information gestaltet, Hoeren, 9 ff.
2156 Zech, m. w. H., 64 ff.; Ders., in: Leible/Lehmann/Zech (Hrsg.), 2 ff.; zur Güterzuordnung vgl. das Opus magnum von Peukert, *passim*; zum Charakter der Ausschliesslichkeitsrechte, das Recht

tion gegenüber jedermann sowie der positiven *Zuweisung von Zuständigkeitsbereichen* gegenüber jedermann.[2157]

1677 Die anhand dreier Charakteristika umschriebenen Ausschliesslichkeitsrechte können, müssen aber nicht zugleich Vermögensrechte sein. Es gibt absolute subjektive Rechte wie das Persönlichkeitsrecht, über die nicht oder nur beschränkt verfügt werden kann.[2158] Die Übertragbarkeit sei indes nicht das ausschlaggebende Kriterium, um ein Ausschliesslichkeitsrecht als Vermögensrecht zu qualifizieren. Zwar halte sich eine Überzeugung, wonach das Persönlichkeitsrecht ein Ausschliesslichkeitsrecht, nicht aber ein Vermögensrecht sei;[2159] ebenso wenig soll das Persönlichkeitsrecht übertragbar sein.[2160] Das bedeute indes nicht, dass es keine *Güter mit Persönlichkeitsbezug* gebe, die eigenständig bestünden und damit übertragen werden können. Exemplarisch für *Persönlichkeitsgüter*, die durch bestimmte Persönlichkeitsrechte geschützt werden, sei das Recht am eigenen Bild.[2161] Im Übrigen erkennt Zech in der faktischen Übertragung von Persönlichkeitsgütern ein starkes Indiz für die Notwendigkeit, die Anerkennung neuer Ausschliesslichkeitsrechte zu reflektieren. Seit Langem stehen in der Realität Kommerzialisierungspraktiken nicht nur von Informationsgütern, sondern auch von Körpersubstanzen und -teilen auf der Tagesordnung.[2162] Den stellvertretend genutzten schuldrechtlichen Rechtsgeschäften spricht Zech eine «Behelfsfunktion» zu.

1678 Nach der Präsentation einer Auslegeordnung kommt Zech zu dem Ergebnis, dass es eine *Stufenleiter der Güterzuordnung* gibt: Das stärkste Element stellt das Eigentum dar, weil es sämtliche Elemente in sich vereint. Das Spektrum endet mit sehr schwachen Ausschliesslichkeitsrechten.[2163] Zech beschreibt weitere Konzeptionen bezüglich der Ausschliesslichkeitsrechte. Hier finden sich Sichtweisen, welche Ausschliesslichkeitsrechte als Personen-Sachen-Beziehungen erfassen, und solche, die die Personen-Personen-Beziehungen fokussieren. Als Herrschaftsrecht gedacht rücke die eine Sichtweise auf das Ausschliesslichkeitsrecht das *Objekt* in das Zentrum, was im Englischen mit dem Terminus *ownership* artikuliert wird. Die andere Sichtweise wird mit dem Begriff *property rights* eingefangen. Sie beschreibe die Herrschaftsbefugnis als *Bündel von Befugnissen* im Umgang

auf informationelle Selbstbestimmung und Ausschliesslichkeitsrechte an Daten auch Specht/Rohmer, PinG 2016, 127 ff.

2157 Zech, 70 f.
2158 Ders., 77.
2159 Ders., 78.
2160 Ders., 83.
2161 Ders., 95; vertiefend zu diesem im Schweizer Recht Bächli, *passim*; vgl. weiterführend auch zweiter Teil, VI. Kapitel, 6.2.
2162 Ders., 83; hierzu und namentlich zu Kommerzialisierungsverboten auch Karavas, Körperverfassungsrecht, 177 ff.
2163 Ders., 85 ff.

mit dem Gegenstand, die dem Rechtsinhaber als Einzelkomponenten des Herrschaftsrechts ausschliesslich zugewiesen sind.[2164]

Um ein passgenaues Zuordnungsmodell für seine Informationskategorien entwickeln zu können, analysiert Zech in einem nächsten Schritt die Spezifika von Informationsgütern im Vergleich zu körperlichen Gütern.[2165] Insofern weist er *drei Differenzen* nach: erstens die Unkörperlichkeit und, daraus resultierend, zweitens die Rivalität[2166] sowie drittens die fehlende oder geringere Exklusivität.[2167] Bezüglich des Umgangs mit Informationen unterscheidet Zech zudem *drei Befugnisse:* erstens die Innehabung, zweitens die Nutzung und drittens die Veränderung. Während bei Sachen für die Nutzung, Fruchtziehung und Übertragung die Innehabung der Sache vorausgesetzt und damit die Körperlichkeit des Gegenstands zum Kristallisationspunkt der Befugniszuweisung wird, gilt dies so nicht für Informationsgüter.[2168] 1679

Besonderheit der Informationsgüter sei, dass die erste Befugnis, die Innehabung von Information, nicht zwingend die alleinige und ausschliessliche Nutzung bringe. Weil Informationen fast unbeschränkt vervielfältigt werden können, biete es sich an, an die Stelle einer Befugnis auf Innehabung von Information diejenige auf Zugang zu Information treten zu lassen. Der *Zugang* zu Information sei die einfachste Befugnis im Umgang mit Information.[2169] Die zweite Befugnis, diejenige zur Nutzung von Information, bildet die Hauptfunktion der Immaterialgüterrechte. Die dritte Befugnis ist diejenige, über die *Veränderung* zu entscheiden. Bekannt ist eine solche aufgrund des Integritätsschutzes gemäss Urheberrecht. An dieser Stelle erfolgt ein Bezug auf das Datenschutzrecht: Die Vorgabe der Richtigkeit sei nur bei semantischer Information relevant. Besondere Virulenz erlangt habe insofern die Verbreitung von Fehleinschätzungen zur Kreditwürdigkeit, wobei es wiederum die Persönlichkeitsrechte seien, die – potentiell und formell – Schutz gewährleisten sollen. 1680

Was aber bilden die Anknüpfungspunkte für die (rechtliche) Zuweisung von Informationen?[2170] Das Immaterialgüterrecht macht die *Schöpfung* der Informa- 1681

2164 Zech., 96 ff.; zu den verschiedenen Rechtskonstruktionen mit Blick auf Personendaten resp. privacy, insb. auch ein property right, vgl. m. w. H. Janger, Hastings L.J. 2003, 899 ff.; Litman, Stan. L. Rev. 2000, 1283 ff., 1288 ff.

2165 Vertiefend zur Zuordnung der Sache zu einer Person und zum Sachenrecht, insb. auch seine Prinzipien vertiefend, Füller, 47 und 112 ff.

2166 Keine Konkurrenz bei der Benutzung Zech, 118: Durch die Vervielfältigungsmöglichkeit besteht keine Rivalität. Geheimnis bedeutet, dass die Exklusivität einer Information gewährleistet wird, diese also nicht rivalisierend verwendet wird – *e contrario* heisst das, dass andere Informationen gerade nicht geheim und entsprechend rivalisierend sind; zugleich erfahren Informationsgüter in aller Regel durch ihre Nutzung keine Abnutzung; hierzu auch Wielsch, 13.

2167 Zech, 115.

2168 Ders., 116.

2169 Ders., 121 ff.; vertiefend auch Rifkin, Access, 9 ff.

2170 Zech, 130 ff.

tion zum massgeblichen Zuweisungselement. Als weitere Kriterien kommen Investitionsleistungen in Frage – in Abkehr vom Schöpferprinzip wird zusehends die wirtschaftliche Leistung resp. Investition berücksichtigt. Entsprechend wird Information demjenigen zugewiesen, der in diese investiert.[2171] Namentlich mit Blick auf semantische Informationen, wozu personenbezogene Angaben gehören, präsentiert sich das Subjekt resp. Objekt, auf das sich die Informationen beziehen, als potentieller Zuweisungsadressat. Zech hält hierzu fest:

> «Die Zuweisung von Aussagen über eine Person an diese Person wird von den Persönlichkeitsrechten vorgenommen. Diese erlauben teilweise eine Kontrolle von persönlichkeitsbezogenen Aussagen, insbesondere in Form einer Zuweisung der Befugnis zur Weiterverbreitung und zur Erzwingung ihrer Richtigkeit. Dabei handelt es sich jedoch in erster Linie um Abwehrrechte, insbesondere gegen die Offenbarung geheimer Sachverhalte und die Verbreitung falscher Aussagen. Die Kontrolle der Weiterverbreitung, wie zum Beispiel durch das Recht am eigenen Bild, stellt eine echte ausschliessliche Zuweisung dar. Zudem liegt in der Weiterverbreitung eine Form der Nutzung von Information. Dadurch kam es zu der Diskussion um die Kommerzialisierbarkeit von Persönlichkeitsrechten, insbesondere darum, ob bestimmte Bestandteile von Persönlichkeitsrechten übertragen werden können.»[2172]

1682 In Bezug auf Personendaten und das Datenschutzrecht zeigt sich damit das Persönlichkeitsrecht als Zuweisungsinstrument.[2173] Allerdings wurde im Zuge dieser Schrift sichtbar, wie unterschiedlich datenschutzrechtliche Modelle ausgestaltet werden, auch wenn sie auf dasselbe Quellrecht zurückgeführt werden. Weder die Ankoppelung des Datenschutzrechts an das Persönlichkeitsrecht noch die Qualifizierung des letzteren als Ausschliesslichkeitsrecht definiert resp. fixiert die Rechtsposition des Datensubjektes präzis.

1683 Die Anerkennung von Ausschliesslichkeitsrechten an Informationen führe zur Einschränkung der Handlungsfreiheit Dritter und bedürfe der Legitimierung.[2174] Informationen werden in aller Regel als frei, als frei fliessend charakterisiert.[2175] Informationsgüter werden von der Wirtschaft als öffentliche Güter wahrgenommen.[2176] Information und Kommunikation gilt für den Menschen – nicht zuletzt, weil er ein Beziehungswesen ist – als Regel, Restriktion als Ausnahme.[2177] Das

2171 Zech, 142 ff.; vgl. (auch kritisch) zur Propertisierung von Informationen Wielsch, 7 ff.; eine Übersicht auch zu kritischen Ansichten betr. die Anerkennung von property rights in Personendaten im US-amerikanischen Diskurs Schwartz, Harv. L. Rev. 2004, 2055 ff., 2076 ff.; zum geistigen Eigentum mit der Frage, ob es sich um eine Komplementärerscheinung zum Sacheigentum handle, Jänich, 3 ff.
2172 Zech, 133.
2173 Ders., 129.
2174 Ders., 145 ff.; Druey, 77 ff., insb. auch 92; zur Beschreibung eines Konfliktes zwischen Datenschutz und Informationsfreiheit Buchner, 80 ff.; zum Ausschliesslichkeitsrecht an Daten und zum Recht auf informationelle Selbstbestimmung auch Specht/Rohmer, PinG 2016, 127 ff., 128 ff.
2175 Druey, 84 ff.; Zech, 145 ff., insb. 147.
2176 Wielsch, 12 ff.
2177 Vgl. im Ergebnis auch Nissenbaum, 266 ff.

dürfte *a fortiori* für den Menschen der Informations- und Kommunikationsgesellschaft gelten. Im Rechtsstaat ist es das Recht, das mittels Anerkennung von Ausschliesslichkeitsrechten die Verknappung des Gutes, des Informationsgutes, realisiert.[2178]

Es gelte als anerkannt, dass Ausschliesslichkeitsrechte an Informationen der besonderen Rechtfertigung bedürfen. Ebendies wird nicht zuletzt anhand des Konzepts des *numerus clausus* der Immaterialgüterrechte zum Ausdruck gebracht.[2179] Für die Begründung der Ausschliesslichkeitsrechte, welche den Ausgangszustand der Gemeinfreiheit beschränken und deren Erforderlichkeit unbestritten ist, werden mehrere Ansätze resp. Theorien angeführt.[2180] Während *deontologische Ansätze* eine Zuweisung für gerecht halten, geht es in *utilitaristischen Ansätzen* um Nützlichkeitserwägungen. Kaum mehr vertreten werde die *Marktwerttheorie*, wonach alles, was Wert hat, mit Schutzrechten zu versehen ist. 1684

Im Rahmen eines *deontologischen Ansatzes* sind die *Eigentumstheorien* zu thematisieren. Hierzu gehört die Arbeitstheorie von Locke, welche die Okkupationstheorie (wonach gesellschaftlicher Konsens gebilligte Aneignung von Information begründet) ersetzt.[2181] Es sei die Verarbeitung, mit der es zu einer Verbindung zwischen Sache und Person kommt und die Sache durch Arbeit Teil der eigenen Persönlichkeit und damit zu Eigentum mache. Zwei Akzentuierungen sind denkbar: Man betont den Persönlichkeitsbezug als Begründungsstrategie und ist damit wieder beim semantischen Bezug zur Persönlichkeit des Schöpfers. Damit ist aber bereits der Übergang zu den Persönlichkeitsrechten erreicht. Wird dagegen der Vorgang der Bearbeitung in den Vordergrund gestellt, ist es die erbrachte Leistung, welche den Ausschliesslichkeitscharakter legitimiert. Die *Eigentumstheorien* integrieren gerade auch den Belohnungsaspekt (womit zugleich der Anreizgedanke adressiert wird). Die Einräumung (geistiger) Eigentumsrechte will einen gerechten Lohn für geleistete Arbeit erzielen. Zugleich soll die Nützlichkeit der Schaffung von Gütern anerkannt werden. Im Lichte der Eigentumstheorien hält Zech treffend fest, dass eine Begründung von Ausschliesslichkeitsrechten an Informationen, die nicht geschaffen wurden und selbst keine besondere Bedeutung haben, schwerfalle.[2182] 1685

2178 Zech, 147.

2179 Jänich, 237 ff.; vgl. auch Peukert, 7 ff.; zur Entstehung und Bedeutung des *numerus clausus* der dinglichen Rechte als zivilrechtliches Dogma vgl. Wiegand, in: Becker/Brauneder/Caroni u. a. (Hrsg.), 623 ff.

2180 Hierzu Zech, 149 ff.

2181 Vertiefend aus philosophischer Perspektive Held, 28 ff.

2182 Zech, 151 f.; zu den Eigentumstheorien im Zusammenhang mit Open Source Heller/Nuss, in: Gehring/Lutterbeck (Hrsg.), 385 ff., 392 ff.; allgemeiner aus rechtsphilosophischer Perspektive zum Verhältnis von Eigentum zur Person Haslbauer, 9 ff.; hierzu auch mit einer *Tour d'Horizon* von Bodin über Locke zu Hegel vgl. Rifkin, Traum, 155 ff.; zum Eigentum an Informationen mit Blick auf genetische Informationen und den Patentschutz grundlegend Godt, 1 ff.

1686 Anders die *utilitaristischen* Legitimierungen. Sie wollen mittels Anerkennung von Ausschliesslichkeitsrechten Ziele erreichen, die als erstrebenswert definiert werden. Dabei werden oft volkswirtschaftliche Zielsetzungen in den Vordergrund gerückt, die mittels ökonomischer Analyse des Rechts in das Rechtssystem integriert werden.[2183] Insofern lassen sich mehrere Begründungsmuster für die Anerkennung von Ausschliesslichkeitsrechten an Informationsgütern ausmachen.[2184] Die Theorie der *Verfügungsrechte* (property rights) geht davon aus, dass Privateigentum (Ausschliesslichkeitsrechte) die volkswirtschaftliche Effizienz resp. Wohlfahrt steigert, indem es positive und negative Folgen privaten Umgangs mit Gütern den Rechtsinhabern zuweist.

1687 Eine *informationsökonomische Analyse des Rechts*, eine Ökonomik der Informationsgüter, insb. des geistigen Eigentums, stellt in ihr Zentrum die Annahme, dass es sich bei Information um ein öffentliches Gut handelt, das sich durch Nichtausschliesslichkeit und Nichtrivalität auszeichnet.[2185] Es werden mehrere Ziele genannt, die mit der Einräumung von Verfügungsmacht an Informationen erreicht werden sollen. Als Anreiz für den Schöpfer zur Schaffung neuer Information, zur Sicherstellung der für die Gesellschaft nützlichen Verbreitung geschaffener Information sowie zwecks Respektierung allfälliger Persönlichkeitskomponenten. Gemäss Anreizparadigma stimulieren Ausschliesslichkeitsrechte die Schaffung von Information und Wissen, da sie die Internalisierung des Nutzens in Aussicht stellen und die Amortisation der Investitionskosten ermöglichen. Das *Paradigma der Allokationseffizienz* geht davon aus, dass Ausschliesslichkeitsrechte die Verteilung von Informationsgütern effektuieren, indem namentlich nicht allgemein zugänglich gemachte Information mittels Rechtsgeschäfts verteilt wird. Insofern ermöglichen Ausschliesslichkeitsrechte *dem Rechtsinhaber, die Nutzung vorhandener Information zu steuern*. Zudem wird die Nutzungseffizienz gewährleistet: Durch den Schutz von Betriebs- und Geschäftsgeheimnissen können die Kosten, die für einen faktischen Geheimnisschutz aufgebracht werden müssten, gesenkt werden. Ähnliches gilt für die Persönlichkeitsrechte, die so auch volkswirtschaftlich nützlich sind: Rechtlicher Schutz erlaubt es, weniger Geld für faktischen Schutz auszugeben.

1688 Ungeachtet der Theorien zur Legitimation von Ausschliesslichkeitsrechten gilt, was folgt: Für den Fall, dass der Gesetzgeber *Ausschliesslichkeitsrechte* an Informationen verbürgt, sieht er ein elaboriertes *Schrankensystem* vor. Es soll einen Ausgleich zum Ausschliesslichkeitsrecht leisten. Die Begründung liegt in der Er-

2183 Zech, 152 f.; in Erinnerung gerufen sei, dass Buchner sein Recht auf informationelle Selbstbestimmung im Privatrecht mit einer ökonomischen Analyse des Rechts mitbegründet, 176 ff.
2184 Zech, 153 ff.
2185 Zum Ganzen Ders., 153 ff.; vertiefend und allgemein zur ökonomischen Analyse des Rechts Posner, 3 ff.; in Bezug auf Personendaten Kilian, in: Garstka/Coy (Hrsg.), 195 ff., 201 ff.

kenntnis, dass Fortschritt nur auf vorhandenem Wissen aufbauen kann. Das Hervorbringen neuer Informationsgüter ist auf die Nutzung existenter Informationsgüter angewiesen.[2186] Besagte Funktion wollen Schrankenregeln gewährleisten: Aus den durch Ausschliesslichkeitsrechte etablierten *Verbotsrechten* werden punktuell Befugnisse herausgenommen und in die Gemeinfreiheit zurückgeführt. Als Schranken zu nennen sind *zeitliche Limitierungen,* wie sie das Patentrecht kennt, aber auch *inhaltliche* wie im Urheberrecht, wonach beispielsweise urheberrechtliche Werke zum privaten Gebrauch vervielfältigt werden dürfen.

1689 In einem letzten Abschnitt der dogmatischen Grundlegung befasst sich Zech mit der *Zuständigkeit zur Schaffung von Ausschliesslichkeitsrechten*.[2187] Unbestritten kommt die Kompetenz dem formellen Gesetzgeber zu. Kritisch beleuchtet wird die Schaffung neuer Ausschliesslichkeitsrechte qua Richterrecht. Während Zech die Anerkennung neuer Ausschliesslichkeitsrechte über Generalklauseln für denkbar hält, verwirft Peukert ein solches Prozedere.[2188] Allerdings würde manchmal in problematischer Weise aus Einzelentscheidungen, in denen beispielsweise ein Schadenersatz zugesprochen wurde, mittels Abstraktion auf die Anerkennung eines allgemeinen Rechts geschlossen.

1690 Hinsichtlich der Etablierung neuer Ausschliesslichkeitsrechte werden zwei Schrittmacher benannt: Neben dem erwähnten Vertragsrecht kommt dem lauterkeitsrechtlichen Leistungsschutz eine richtungsweisende Rolle zu. Er führt dazu, dass neue Güter, die durch den technischen und wirtschaftlichen Fortschritt hervorgebracht werden, rechtlich in den Blick genommen werden.[2189]

1691 Allerdings ist es nicht nur die *Schaffung neuer Güter*, die als faktischer Befund das Recht herausfordert. Als weiteren Entwicklungstrend benennt Zech die *Abstraktion und Verdinglichung von Information*.[2190]

1692 Zech zeichnet in der Folge auch aus einer historischen Perspektive die Reaktionsweise des Zivilrechts auf die entsprechende Herausforderung der Abstraktion nach. An deren Anfang steht die Anerkennung *geistiger Eigentumsrechte*. Ihre Ableitung aus einem Persönlichkeitsrecht ist unübersehbar: Durch das Recht des geistigen Eigentums, insb. des Urheberrechts, wurden Regelungen geschaffen, die eine Antwort auf die Abstraktion vom Informationsträger geben konnten. Ebendies erreichte man, indem auf den Konnex zur Persönlichkeit des Schöpfers und später auf die Schöpfung selbst abgestellt wurde, bis selbst der Schöpferbezug im Zuge neuer Datenverarbeitungstechnologien erodiert wurde. Auf die fort-

2186 Hierzu auch Wielsch, 1 ff.
2187 Zech, 158 ff.; grundlegend zur Frage ob, in welchem Umfang und wem neu entstehende Güter zugeordnet werden sollen; Peukert, 1, 32 ff.
2188 Zech, 159; Peukert, 10, 880 ff.
2189 Zech, 161.
2190 Ders., 181 ff.

schreitende Abstraktion hat das Zivilrecht, so Zech, noch keine angemessenen Antworten gefunden. Namentlich die *Existenz abstrakter Informationsgüter hat noch keine eigenständige Regelung* nach sich gezogen.

1693 Zech präsentiert basierend auf dem von ihm entwickelten juristischen Informations(güter)begriff eine *informationsrechtliche Zuweisungsordnung*. Sie referiert differenzierend auf die drei von ihm präsentierten Informationsbegriffe – semantische, strukturelle und syntaktische Informationen. Die geschützte Rechtsposition soll unter Berücksichtigung der Informationsart sowie der Interessenlage definiert werden. Vorgeschlagen wird eine gestufte Zuweisung an die Schöpferin, den Speichernden oder die Codierende. Es wird dafür plädiert, dass die Rechtsposition des Codierenden ausgebaut wird und eine verstärkte Ausrichtung am Skripturakt stattfindet.[2191]

1694 Zech beschäftigt sich wiederholt mit den Rechten *an personenbezogenen Angaben*, die er als *Prototyp semantischer Informationen* beschreibt.[2192] Er spricht sich allerdings *gegen ein allgemeines Recht auf informationelle Selbstbestimmung in Gestalt und mit Gehalt eines Rechts an den eigenen Daten* aus.[2193] Damit verwirft er eine Position, wie sie von Buchner vertreten wird. Wie dargelegt plädierte Buchner für ein einheitliches Recht auf informationelle Selbstbestimmung im Privatrecht. Dieses sollte persönlichkeits- und vermögensrechtliche Ingredienzen in sich vereinen und dem Subjekt aktive Verwertungsbefugnisse einräumen. Eine solche Weiterentwicklung beurteilt Zech im Hinblick auf den Schutzzweck des Datenschutzrechts als problematisch. Ein so gestaltetes Recht auf informationelle Selbstbestimmung für das Privatrecht sei weder im geltenden (deutschen) Datenschutzrecht für den privaten Sektor verwirklicht noch sollte es *de lege ferenda* eingeführt werden. Personenbezogene Angaben werden und sollen einen Integritätsschutz erfahren, nicht aber mittels ausschliesslicher Nutzungsrechte zugewiesen werden, so Zech.

1695 Anzufügen bleibt: Die rechtlichen Positionen an den jeweiligen Informationsgütern resp. -kategorien variieren resp. überlagern sich.[2194] Zur Veranschaulichung: Beim Erwerb einer CD wird eine Sache im Sinne von Art. 641 ff. ZGB erworben, was sich als erste Schicht in Anlehnung an das Zwiebelmodell beschreiben liesse. Die CD ist gleichzeitig das verkörperte Werk des Schöpfers. Die zweite Schicht ist das «Werk», das immaterielle Gut, die Lieder. Diese sind die semantische Ebene oder Bedeutungsebene. Auf der semantischen Ebene digitaler Güter bestehen regelmässig Immaterialgüterrechte, insb. Urheberrechte. Die dritte Schicht ist die syntaktische Ebene: 0101, der digitale Binärcode.

2191 Zech, 421 ff.; hierzu auch Hoeren, MMR 1998, Beilage, 6 ff., 9.
2192 Zech, 215.
2193 Ders., 227 ff.
2194 Vgl. auch Schmid/Schmidt/Zech, sic! 2018, 627 ff., 630 ff.

Ein auch datenschutzrechtlich relevantes Beispiel findet sich in Bezug auf genetische Daten.[2195] Es geht um sog. Lifestyle-Gentests. Die Unternehmen, die solche Gentests anbieten, haben nicht nur Verträge mit Kundinnen und Kunden, sondern auch mit Pharmakonzernen und Forschungsinstitutionen. Personendaten und sog. semantische Informationen sind einzig im Verhältnis zwischen Gentestunternehmen und den Kunden betroffen. Hier greifen die datenschutzrechtlichen Vorgaben. Anders handelt es sich bei den Daten, die den Forschungseinrichtungen oder Pharmakonzernen zur Verfügung gestellt werden, um syntaktische und strukturelle Informationen. Die Forschungseinrichtungen und Pharmakonzerne interessieren sich primär für den Zugang zu den biologischen Proben sowie zu den syntaktischen Informationen, wie diese in den Datenbanken der Gentestunternehmen erfasst und gespeichert worden sind. Gegen solche Nutzungsweisen kann nur bei Anwendbarkeit der datenschutzrechtlichen Vorgaben vorgegangen werden, wobei infolge einer Anonymisierung der Angaben dies gerade nicht mehr möglich ist. Der Personenbezug, der für die Anwendbarkeit des Datenschutzrechts relevant ist, wurde gekappt. Die Zuweisungsfrage wird mit anderen Worten nicht vom Datenschutzrecht beantwortet, wenn es um syntaktische oder strukturelle Informationen geht. Sie weisen keine semantische und folglich ebensowenig eine persönlichkeitsrechtlich relevante Dimension auf.[2196] 1696

Faktisch scheint es so, dass syntaktische und strukturelle Informationen im Eigentum der diese Informationen verarbeitenden Unternehmen stehen, die sich quasi herrenlose Objekte im Sinne eines originären Besitz- und Eigentumserwerbs aneignen.[2197] Gemäss dem Geschäftsmodell erscheinen in der Realität als Eigentümer syntaktischer und struktureller Informationen die Gentestunternehmen. Eine solche Auffassung wird indes kritisiert.[2198] Mit ethischen, ökonomischen sowie juristischen Argumenten wird dafür plädiert, ein neues Eigentumsrecht an Daten anzuerkennen.[2199] Ein solches soll auf den Skripturakt abstellen.[2200] Eine andere Begründung, aber dieselbe Folgerung findet sich bei Amstutz, der die Rechte an Daten ebenso dem Skribenten zuweisen möchte.[2201] 1697

Damit ist die Brücke zum *Eigentumsparadigma* geschlagen. Neue Eigentumsrechte werden keineswegs bloss in Bezug auf die strukturelle und syntaktische Di- 1698

2195 Karavas/Burri/Gruber, TA-SWISS 2020, 251 ff., 298 ff., wobei sich anschliessend unter 7., 303 ff., Schlüsse und Empfehlungen sämtlicher Autorinnen und Autoren der Studie finden.
2196 Dies., 251 ff., 297.
2197 Dies., 251 ff., a. a. O.
2198 So durch Schmid/Schmidt/Zech, sic! 2018, 627 ff., 633 ff.
2199 Vgl. Dies., a. a. O., 627 ff., 631 f.
2200 Vgl. Hürlimann/Zech, sui-generis 2016, 89 ff., 94; Hoeren, MMR 2013, 486 ff., 487; als Skribent und damit als originär Berechtigte an den Daten gilt die Person, die durch die Verwendung eines Digitalgeräts die Daten erstellt. Im Rahmen der hier interessierenden Gentests gilt als Skribent diejenige Person, die einen Gentest durchführen lässt, m. w. H. Karavas/Burri/Gruber, TA-SWISS 2020, 251 ff., 298 f.
2201 Vgl. den Gouvernementalitätsansatz bei Amstutz, AcP 2018, 438 ff., 517 ff.

mension von Informationen diskutiert, sondern auch für Personenangaben und somit für semantische Informationen.

4. Zum Eigentumsparadigma

1699 Die Frage nach der Anerkennung eines Eigentums an Daten, auch an Personendaten, hat viel Aufmerksamkeit auf sich gezogen.[2202] Zur Hochkonjunktur von *sachenrechtlichen Ansätzen mit Figuren der res digitalis*[2203] und einem *Eigentum an (Personen-)Daten* führt eine spezifische Kognition: Es geht um die Abspaltung von Personendaten von der Person und um die Transformation von (Personen-)Daten in Wirtschaftsgüter. Der ideell-defensivrechtliche Persönlichkeitsschutz stösst bei der Bewältigung dieser faktischen Entwicklungen an Grenzen. Vorgeschlagen wurden(persönlichkeitsrechtliche) Ansätze eines Rechts an eigenen Daten nach dem Vorbild des Urheberrechts, das persönlichkeits- wie vermögensrechtliche Komponenten beinhaltet.

1700 In den Diskussionen zur Frage, ob stattdessen ein Eigentum an Personendaten anzuerkennen sei, zeigt sich eine Objektfokussierung. Die juristischen Interpretationen bleiben trotz der Digitalisierung mit ihrer Dematerialisierung und im Bereich des Informationsrechts, das in erster Linie unkörperliche Phänomene adressiert, bis heute an den Kategorien der analogen Welt sowie der körperlichen Sache ausgerichtet.[2204] Was mit der Verhaftung am Materiellen, Körperlichen

2202 Vgl. Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 26, m. w. H. auch zu einer eigenen kritischen Einschätzung; Meister, DuD 1983, 163 ff.; Hoeren, MMR 2013, 486 ff.; Beurskens, in: Domej/Dörr/Hoffmann-Nowotny u. a. (Hrsg.), 443 ff.; m. w. H. Weber/Thouvenin, ZSR 2018, 43, ff., 44; Specht, CR 2016, 288 ff., 290, mit weiteren Verweisen; vgl. sodann Amstutz, AcP 2018, 438 ff. und NZZ vom 5. September 2018, 10; Flückiger, PJA 2013, 837 ff.; Hess-Odoni, Jusletter vom 17. Mai 2003; Schunck, digma 2013, 66 ff.; Fröhlich-Bleuler, Jusletter vom 6. März 2017; Benhamou/Tran, sic 2016, 571 ff.; Briner, Jusletter IT vom 21. Mai 2015; Thouvenin, SJZ 2017, 21 ff.; Thouvenin/Weber, ZSR 2018, 43 ff., Thouvenin/Früh/Lombard, SZW 2017, 25 ff.; Hürlimann/Zech, sui-generis 2016, 98 ff.; Murphy, Geo. L.J. 1996, 2381 ff.; Reichman/Samuelson, Vand. L. Rev. 1997, 52 ff.; Rule/Hunter, in: Bennet/Grant (ed.), 168 ff.; Lessig, Soc. Res. 2002, 247 ff.; Bergelson, UC Davis L. Rev. 2003, 379 ff.; vgl. auch Basho, Calif. L. Rev. 2000, 1507 ff., 1526 ff., der für die Anerkennung eines wirtschaftlichen Verwertungsrechts eintritt; mit kritischen Hinweisen zu einer Konzeptionierung von privacy als property m. w. H. Schwartz, Wis. L. Rev. 2000, 743 ff., 763 ff. unter Diskussion der Problematik von Preisdiskriminierungen mit dem Risiko des Marktversagens; vgl. zur wirtschaftlichen Dimension von Personendaten, allerdings aus der Perspektive der vertraglichen Gegenleistung und nicht in Bezug auf ein Eigentumsrecht an Personendaten Kilian, Stiftung Datenschutz (Hrsg.), 191 ff., 195 ff.; kritisch jüngst mit der Forderung eines kommerzialisierungsfesten Datenschutzes, auch mit einer Analyse des «Dateneigentums», Bijok, 367 ff.

2203 So Eckert, SJZ 2016, 245 ff., 245.

2204 Vgl. in diesem Zusammenhang die Worte von Wielsch, 1: «Die Wirtschaft des Bürgerlichen Gesetzbuches ist eine Wirtschaft der körperlichen Gegenstände. Die Wirtschaft der Gegenwart ist in wachsendem Masse eine Wirtschaft der immateriellen Güter, deren Gegenstand Vereinbarungen über die Nutzung von Wissen bilden»; zu den unkörperlichen Gütern aus diversen Betrachtungsweisen vgl. die verschiedenen Beiträge in Leible/Lehmann/Zech (Hrsg.); mit Blick auf das Zivil- und Privatrecht und den rechtlichen Umgang mit digitalen Gütern unlängst Pfaffinger, Digitale Güter:

gemeint ist, klingt in der Debatte um die Anerkennung eines Eigentumsrechts an Daten in den kritischen Worten von Zech/Hürlimann an:

> «Man mag es kaum mehr hören: Daten sind das Öl des 21. Jahrhunderts. Der Vergleich mag in Bezug auf die wirtschaftliche Relevanz eine gewisse Gültigkeit haben. Gleichzeitig ist er aber in verschiedener Hinsicht unsinnig: Öl kann man nutzen und dann ist es in der Regel weg. Öl kann man kaufen und dann gehört es niemand anderem. Öl kann man aus einer bestimmten Quelle fördern und damit verhindern, dass es jemand anderes tut. Demgegenüber kann man Daten nutzen, ohne dass sie danach weg wären. Man kann Daten kaufen, ohne dass damit ausgeschlossen wäre, dass ein anderer diese Daten auch kauft. Und man kann Daten sammeln, ohne damit zu verhindern, dass sonst jemand die gleichen Daten auch sammelt. Kurz (oder ökonomisch gesprochen): Öl ist rivalisierend, Daten sind es nicht. Nicht rivalisierende Güter können von mehreren Personen gleichzeitig verwendet werden, ohne dass eine Verwendung die andere beeinträchtigt. Öl ist darüber hinaus auch ausschliessbar, der Eigentümer kann also kontrollieren, wer den Rohstoff nutzt und wer nicht. Die Frage der Ausschliessbarkeit ist bei Daten weniger eindeutig: Kann die Verwendung von Daten durch Dritte ausgeschlossen werden? Falls ja, auf welche Rechtsgrundlage könnte sich der Ausschluss stützen?»[2205]

Die Erfassung informationeller und digitaler Güter stellt die etablierten Kategorien des geltenden Rechts, das ein Recht der analogen Welt ist, auf die Probe. 1701

Die Beiträge, die den *sachenrechtlichen Ansatz für den Umgang mit Daten* analysieren, lassen sich grob in *zwei Gruppen* einteilen: Einige Aufsätze widmen sich der Debatte um eine sachenrechtliche Erfassung personenbezogener Angaben, andere exkludieren diese explizit und wollen sich auf sog. Sachdaten konzentrieren.[2206] 1702

Auf sog. Sachdaten und damit strukturelle sowie syntaktische fokussieren sich theoretisch Eckert und wenig später Fröhlich-Bleuler.[2207] Eckert befasst sich mit «digitalen Daten» und schlägt eine Beurteilung digitaler Daten als Sachen und deren Zuweisung durch Besitz- und Eigentumsrecht vor. Eckert anerkennt, dass personenbezogene Daten auch in Gestalt «digitaler Daten» erscheinen. Insofern weist er auf das «eigenständige» Regime des Datenschutzrechts hin.[2208] Mit anderen Worten werden Personendaten – wegen ihrer semantischen Dimension – in das Regime des persönlichkeitsrechtlichen Datenschutzes verwiesen, während die eigentumsrechtlichen Ansätze sich auf Daten in ihrer syntaktischen und strukturellen Information beziehen. Nicht erörtert wird, wie die Abgrenzung von digitalen Daten mit resp. ohne Personenbezug im Lichte der Realitäten bewerkstelligt werden soll. Dass dies Schwierigkeiten bereitet, wird 1703

Knotenpunkte des Privat- und Zivilrechts, Vortrag vom 6. November 2019, HSG/Universität St. Gallen.

2205 Hürlimann/Zech, sui-generis 2016, 98 ff., 98.

2206 Zur Notwendigkeit dieser Einteilung Früh, digma 2019, 172 ff.

2207 Eckert, SJZ 2016, 245 ff., 247; Fröhlich-Bleuler, Jusletter vom 6. März 2017, N 1 ff.

2208 Eckert, SJZ 2016, 245 ff., 247; ebenso Fröhlich-Bleuler, Jusletter vom 6. März 2017, N 1 ff.

zumindest anerkannt.[2209] Ob die Abgrenzung von digitalen Daten mit semantischer Dimension (z. B. dem Personenbezug) oder ohne semantische Dimension (ebenso als Sachdaten bezeichnet von Thouvenin[2210]) und eine anknüpfende Unterscheidung des anwendbaren Rechts sinnhaft möglich ist, erscheint zweifelhaft. Eine trennscharfe Abgrenzung der verschiedenen Informationsdimensionen – semantische, strukturelle und syntaktische – ist kaum möglich. Mittlerweile ist die Schwierigkeit, Sachdaten und Personendaten voneinander abzugrenzen, unbestritten.[2211]

1704 Eckert legt einen Qualifikationsansatz vor, der auf Daten ohne Personenbezug fokussiert. Er befasst sich für seine Analyse zum Eigentum an Daten mit dem *Sachbegriff* der Schweizer Zivilrechtsordnung.[2212] Für diesen haben sich in der herrschenden Lehre vier Elemente etabliert: Abgegrenztheit, Beherrschbarkeit, Körperlichkeit und Unpersönlichkeit.[2213] Vertieft betrachtet werden die Elemente Beherrschbarkeit und Körperlichkeit. Insofern bezieht sich der Autor auf Lehrmeinungen, die den Sachbegriff nicht ausschliesslich «naturgegeben», sondern funktional definieren. Ebendies erfolgt über die Integration teleologischer Erwägungen, womit der Sachbegriff dynamisch bleibt.[2214] Unter Anwendung eines «funktionalen» Sachbegriffs plädiert Eckert für die Qualifikation von digitalen Daten als *Sache,* als *res* und – genauer – als *res digitalis*. Auf dieser Qualifikation aufbauend überprüft der Autor die Tauglichkeit der sachenrechtlichen Normen, genauer des Besitzes- und Eigentumsrechts für die *res digitalis*. Als Besitzer bezeichnet er die Person, welche in technischer Hinsicht die Herrschaft über digitale Daten hat. Ihr wird das Eigentum zugewiesen, womit sie für die unbeschränkte Verkehrsfähigkeit durch die vollständige Übertragbarkeit eintritt.[2215]

1705 Wie aber wird ein *Eigentum an Personendaten* diskutiert? Politisch wurde wiederholt für die Fortentwicklung des defensivrechtlich angelegten Datenschutzgesetzes hin zu einem eigentumsrechtlich orientierten Datenschutz eingetreten.[2216] Die Vorstösse blieben ohne Erfolg und die Totalrevision des DSG verfolgt, wie gezeigt, weiterhin ein persönlichkeitsrechtlich basiertes und damit defensivrechtliches Konzept. Die subjektivrechtliche Anknüpfung des DSG im Persönlichkeitsrecht wird nicht abgelöst durch einen eigentumsrechtlichen Ansatz. Charakte-

2209 Vgl. Früh, digma 2019, 172 ff., 172 f.
2210 Thouvenin, SJZ 2017, 21 ff., 22.
2211 Vgl. Cichocki, Jusletter IT vom 21. Mai 2015, N 13 ff., insb. N 20 ff., der für ein sog. Datenbearbeitungsrecht eintritt; zur Abgrenzungsschwierigkeit auch Thouvenin, SJZ 2017, 21 ff., 22.
2212 Eckert, SJZ 2016, 245 ff., 246 f.; zum Sachbegriff im schweizerischen ZGB vertiefend Kälin, 1 ff.; gegen die Anerkennung eines Dateneigentums und die Notwendigkeit des Datenschutzrechts in diese Richtung Schmidt, digma 2019, 181 ff.
2213 Hierzu m. w. H. Kälin, 12 ff.
2214 Zum funktionalen Sachbegriff vgl. Rey, N 68 und 106 ff.; dieser funktionale Sachbegriff wurde indes kritisch beurteilt durch Kälin, 131 f.
2215 Eckert, SJZ 2016, 245 ff., 249 f.
2216 M. w. H. Schmid/Schmidt/Zech, sic! 2018, 627 ff., 635.

ristisch für die Totalrevision ist, dass der rechtliche Subjektschutz in Gestalt des Persönlichkeitsschutz durch Ansätze und Instrumente ergänzt wird, für die nicht die subjektivrechtliche Prägung entscheidend ist (Stichworte «Compliance-Ansatz» und «Risiko-Ansatz»).

Wissenschaftlich findet sich gleichwohl eine Auseinandersetzung mit der Sinnhaftigkeit der Anerkennung eines Personendateneigentums *de lege ferenda*. 1706

In die Richtung eines *Eigentums sui generis* an personenbezogenen Angaben möchte Flückiger ein Recht auf Selbstbestimmung weiterentwickeln. Der Autor stellt zutreffend dar, dass der Schutz vor Missbrauch das Schweizer System *de lege lata* terminologisch aussagekräftig abbilde. Es sei noch immer stark im Sphärenkonzept verhaftet.[2217] Dem Autor geht es darum, den Datensubjekten eine veritable Entscheidungsbefugnis über ihre Personendaten einzuräumen. Flückiger liefert die verfassungsrechtliche Begründungsarbeit und setzt sich kritisch mit den Einwänden gegen das Recht auf Selbstbestimmung auseinander. Als Ausgangspunkt dient ihm die Gewährleistung des Selbstbestimmungsrechts: 1707

> «Le droit à l'autodétermination est gravé dans le bronze de la Constitution est un signal fort.»[2218]

Der Autor weist unter Reflexion der Eigentumstheorien, namentlich derjenigen von Locke und Westin, auf die Assimilierung der Selbstbestimmung zum Eigentum hin. Sie zeige sich besonders deutlich anhand des Rechts am eigenen Bild.[2219] Es folgt eine vertiefte, auch historisch ausgerichtete Beschäftigung mit den verschiedenen Ideen zum Privaten, so in Gestalt einer defensiv gedachten Sphärenkonstruktion oder einer Vorstellung der Kontrolle von Personenangaben durch das Subjekt.[2220] Nach einer Reflexion der den Ansätzen entgegengebrachten Einwänden tritt Flückiger im Ergebnis für eine *Stärkung der informationellen Selbstbestimmung* ein. Insofern spielt die Anknüpfung in der Menschenwürdegarantie eine Hauptrolle.[2221] Dessen ungeachtet führt er das vorgeschlagene Recht auf informationelle Selbstbestimmung nicht auf das Persönlichkeitsrecht zurück. Vielmehr will er dieses im Recht des (geistigen) Eigentums anknüpfen. 1708

Welche Konsequenzen der Datenschutzgesetzgeber für den privaten Sektor ziehen müsste, evaluiert Flückiger, der für die Stärkung der informationellen Selbstbestimmung in Gestalt eines Eigentumsrechts eintritt, nicht. Er sieht die informationelle Selbstbestimmung als eine logische Folgerung eines freiheitlichen 1709

2217 Flückiger, PJA 2013, 837 ff., 847.
2218 Ders., a. a. O., 837 ff., 837.
2219 Ders., a. a. O., 837 ff., 895 ff.; vgl. zum Lockeschen Eigentumstheorem auch Bergelson, UC Davis L. Rev. 2003, 379 ff., 420 ff., wobei dieses nur *prima vista* für ein Eigentum an Daten der Datensammelnden und Verarbeitenden spricht.
2220 Flückiger, PJA 2013, 837 ff., 843.
2221 Ders., a. a. O., 837 ff., 837 und 839; vgl. hierzu auch Kang/Buchner, Harv. J.L. & Tech. 2004, 229 ff., 231 f., 234 ff.

Staatswesens, das die individuelle Freiheit verbürgen, auf Paternalismus dagegen verzichten soll. Ausser Frage steht für den Autor, dass punktuelle Beschränkungen des Rechts auf informationelle Selbstbestimmung unverzichtbar sind.[2222] Diese Schranken liessen sich, so Flückiger, anlehnend an die Eigentumstheorie und Wirtschaftsfreiheit begründen. Flückiger plädiert für die Stärkung informationeller Selbstbestimmung mit *eigentumsrechtlicher Basierung – für ein Eigentum sui generis*.[2223] Auf einen Detailvorschlag zur Gestaltung seines Eigentumsansatzes an Personendaten verzichtet er.

1710 Ebenso mit einem Eigentum an *personenbezogenen Daten natürlicher Personen* befasst sich Thouvenin. Seiner Ansicht nach sei «allgemein anerkannt», dass die Bundesverfassung ein Grundrecht auf informationelle Selbstbestimmung verbürge.[2224] Zutreffend weist er darauf hin, dass ein Eigentumsrecht der Datensubjekte an «ihren» Personendaten keineswegs selbstredend sei. Personendaten seien in aller Regel eher ein Nebenprodukt des Verhaltens der (Daten-)Subjekte. Der isolierte Wert von Personendaten als Quasi-Rohstoff sei – auch wenn eine Bewertung nicht leicht falle – doch eher gering.[2225]

1711 An dieser Stelle ist eine Rückblende auf Zech angezeigt: Die Besonderheit der Informationsverarbeitung liege auch darin, dass durch die Kombination vieler vorhandener Aussagen neue Aussagen erzeugt werden können. Ein Befund, der ebenso für den Umgang mit Personendaten und damit für das Datenschutzrecht relevant ist. Aus zahlreichen geringfügigen (semantischen) Informationen können mittels technologischer Prozesse neue Aussagen über Personen generiert werden (Data Mining).[2226] Dem hieraus resultierenden Gefährdungspotential soll durch die gesetzlichen Regelungen zum Datenschutz Rechnung getragen werden.[2227] Der wirkliche Wert personenbezogener Angaben wird bei Lichte betrachtet vonseiten der Unternehmen generiert, indem sie nicht nur unzählige Angaben sammeln. Der Wert von Personenangaben konstituiert sich nicht an der schieren Menge gesammelter Personendaten. Vielmehr verwirklicht er sich durch komplexe sowie teure Analyseverfahren mittels neuer Informationstechnologien. Damit erstaunt nicht, dass die verarbeitenden Unternehmen den datenschutzrechtlichen Ansprüchen oft das Unternehmensgeheimnis entgegenhalten.[2228] Das Arbeits-

2222 Flückiger, PJA 2013, 837 ff., 855.
2223 Ders., a. a. O., 837 ff., 837 und 864.
2224 Thouvenin, SJZ 2017, 21 ff., 22 f.; zur Frage, wem Personendaten gehören, insb. bereits Weichert, in: Bäumler (Hrsg.), 158 ff., 176 ff.; Ders., in: Taeger/Wiebe (Hrsg.), 281 ff.; vgl. die Beiträge in Büllesbach/Dreier (Hrsg.), insb. auch von Kuhlen, 1 ff.
2225 Beachte allerdings auch Karg, digma 2011, 146 ff. mit dem Hinweis, dass Personendaten keineswegs bloss ökonomischen Wert haben.
2226 Vgl. die zahlreichen Beiträge zu Data Mining und Erkenntnisgenerierung anhand von Big Data Chu (ed.).
2227 Zech, 38.
2228 Hierzu vgl. Bull, ZRP 2008, 233 ff., 235.

und Wertschöpfungstheorem – eines der Fundamente der Eigentumstheorien – würde sein Gewicht in die Schale der Legitimation zugunsten des *Eigentumsrechts der Verarbeitenden* legen.[2229] Das Datensubjekt habe lediglich einen isoliert dastehenden Rohstoff geliefert.

1712 Zurück zu Thouvenin – er wirft trotz Art. 1 (n)DSG die Frage auf, ob das geltende (Datenschutz-)Recht *de lege lata* dem Datensubjekt eine Position einräume, die als Eigentum an Personendaten qualifiziert werden könne.[2230] Zur Beantwortung legt er vorab die Charakteristika des Sacheigentums wie des geistigen Eigentums dar. Das Datenschutzgesetz räume dem Datensubjekt kein «Herrschaftsrecht» ein, das der positiven Seite des Eigentums entsprechen würde. Vielmehr vermittle es dem Datensubjekt angesichts des Rechts auf informationelle Selbstbestimmung die Befugnis, die Verarbeitung seiner Personendaten zu erlauben oder zu verbieten.[2231] Der *de lege lata* fehlende Zuweisungsgehalt kollidiere allerdings mit dem Faktum, wonach personenbezogene Angaben Wirtschaftsgüter seien.[2232] Anders als die positive Seite sieht Thouvenin die negative Seite des Eigentumsrechts im Datenschutzgesetz weitgehend verwirklicht. Es gehe hierbei insb. um die Abwehrbefugnis gemäss Art. 641 Abs. 2 ZGB. Zutreffend weist der Autor darauf hin, dass die Auffassung, wonach eine Personendatenverarbeitung nach DSG grundsätzlich nur zulässig sei, wenn eine Einwilligung des Datensubjektes vorliege, falsch sei.[2233] Thouvenin beurteilt den Eingriff in das «Datenrecht» der Datensubjekte basierend auf überwiegenden Interessen als kompatibel mit der Struktur von (geistigen) Eigentumsrechten. Ein solcher Eingriff erfolge zwar bei den Immaterialgüterrechten nicht im Einzelfall. Vielmehr werde er in Gestalt der Schranken gesetzlich definiert.[2234] Hieraus leitet Thouvenin ab, dass in einer abstrakten Evaluierung einschlägiger Interessen durch den Gesetzgeber, wie man sie im Immaterialgüterrecht fände, ein zukunftsweisendes Gestaltungselement für ein neues Datenschutzrecht gefunden werden könne.

1713 Der Vorschlag erscheint vielversprechend: Er setzt an einer Schwachstelle des aktuellen Rechtskonzepts an, derjenigen der ungenügenden Strukturierungswirkung durch den Gesetzgeber. Die ungenügende Strukturierungswirkung, die das Regelungsregime basierend auf Generalklauseln und Interessenabwägungen für den Einzelfall bringt, würde überwunden. Es wäre der Gesetzgeber, der in abstrakter Weise divergierende Interessen im Zusammenhang mit Personendatenverarbei-

2229 Vgl. m. w. H. die differenzierende Reflexion bei Specht/Rohmer, PinG 2016, 127 ff., 129 ff.
2230 Thouvenin, SJZ 2017, 21 ff., 25 f.; auch kritisch zur Propertisierung von Informationen Wielsch, 7 ff.
2231 Thouvenin, SJZ 2017, 21 ff., 26 f.
2232 Ders., a. a. O., 21 ff., 24 ff.
2233 Ders., a. a. O., 21 ff., 27.
2234 Ders., a. a. O., 21 ff., 27; zum Verhältnis des geistigen Eigentumsrechts zum Sacheigentum vertiefend Jänich, 185 ff.

tungen gewichtet. Auf diesem Weg könnte ebenso die systemische Dimension des Datenschutzrechts integriert werden. Ein Schutzziel, dessen elementare Bedeutung in dieser Schrift herausgearbeitet wurde und im anschliessenden letzten Kapitel verfestigt wird.

1714 Thouvenin vertieft neben der präzisierenden Charakterisierung des geltenden Datenschutzrechts, einer Stellungnahme zur Frage der Verwirklichung eigentumsrechtlicher Positionen sowie der Präsentation eines Vorschlags *de lege ferenda* die Frage nach der Sinnhaftigkeit eines erweiterten «Eigentumsbegriffs resp. Eigentumsrechts». Die Anerkennung eines Eigentums an Personendaten, das gerade auch der positiven Seite Nachachtung verschaffen soll, skizziert er anhand *zweier Modelle*. Als Gestaltungsvariablen dienen Thouvenin Gegenstand, Zuweisung resp. Inhaberschaft sowie die Wirkungen des Eigentums an Daten.

1715 In einer *ersten Variante* soll, in Anlehnung an die eigentumsrechtlich geprägte Schöpferdoktrin, den Datensubjekten ein geistiges Eigentum an ihren Daten als immateriellen Gütern zukommen (die diese nach Ansicht von Thouvenin «geschöpft» haben). Den Unternehmen soll ein «Recht an der Festlegung der Daten», die sie gesammelt haben, zugewiesen werden. Der Autor beschreibt sogleich die Problematik der Kollision zwischen den beiden Eigentumsrechten und namentlich diejenige, wonach die Unternehmen Eigentum an den Daten der Subjekte erlangen und damit das Datensubjekt selbst exkludieren können. Folglich bilanziert er sein erstes Modell als nicht sinnvoll.[2235]

1716 Sein *zweites Modell* ist ein kollektives Eigentum, genauer ein Miteigentum. Eine Konsequenz wäre, dass die Veräusserung der Festlegung der Daten nur bei Vorliegen der Zustimmung aller Eigentümer möglich wäre.[2236] Doch auch für diese Konstruktion attestiert Thouvenin Schwierigkeiten, wie sie bereits für andere Felder des Miteigentums festgestellt wurden. Als Ausweg diskutiert er die Möglichkeit eines «kumulativen Eigentums», dessen Funktionstüchtigkeit indes erst zu prüfen wäre.[2237]

1717 In Bezug auf die Nutzungsbefugnisse beschreibt er *drei Ausgestaltungsmöglichkeiten*. Erstens die Nutzungsbefugnis infolge einer Zustimmung aller Berechtigter, zweitens die Nutzung durch beide – und zwar ungeachtet einer Zustimmung durch die andere berechtigte Person – sowie drittens der Nutzungsvorrang des Datensubjektes, das den anderen «Eigentümern» die Nutzung mittels Zustimmung einräumen kann. Die letztere Variante steht nach Auffassung des Autors im Einklang mit dem Recht auf informationelle Selbstbestimmung, indem das Datensubjekt selbst darüber entscheidet, ob es die Nutzung «seiner Daten» ande-

2235 Thouvenin, SJZ 2017, 21 ff., 28 f.
2236 Ders., a. a. O., 21 ff., 29.
2237 Ders., a. a. O., 21 ff., 29 ff.

ren erlauben will, unter Umständen auch gegen ein Entgelt. Sodann untersucht Thouvenin, wie dieses Recht mit dem bestehenden Datenschutzrecht harmonisiert werden könnte. Auch insofern stellt er drei Varianten zur Debatte: Das On-Top-Szenario, das Anstelle-Szenario oder das Alternativ-Szenario.[2238] Eine Koexistenz, nach der das Datensubjekt nicht nur seine Rechte – wie das Auskunftsrecht gemäss DSG –, sondern zugleich eine Eigentümerposition hätte, lehnt er ab.[2239]

1718 Einer genaueren Evaluierung unterziehen will Thouvenin eine (mindestens weitreichende) Substitution des aktuellen Datenschutzrechts für den privaten Sektor durch ein Eigentumsrecht. Hierfür spreche, dass das geltende Recht in seiner Lesart bereits den Aspekt der informationellen Selbstbestimmung transportiere. Damit würde in seinen Augen kein Paradigmenwechsel im eigentlichen Sinne vollzogen.[2240] Eine Alternative, die bereits von der Rechtsprechung mit BGE 136 III 401 vorgezeichnet sei, verortet Thouvenin im vertraglichen Weg. So sollen bindende Verträge über personenbezogene Angaben und damit der Verzicht auf die Widerruflichkeit der Einwilligung möglich sein.[2241] Allerdings hinterfragt Thouvenin zu Recht kritisch, ob tatsächlich über sämtliche Felder hinweg – ungeachtet der Frage, ob es sich um Personendaten zur Gesundheit, zum Konsumverhalten beim Grossisten, um Versicherungsangaben oder um Angaben im Arbeitsrechtskontext handelt – die Einwilligung des Datensubjektes als massgebliches Element des Datenschutzrechts definiert werden könne. Eine generelle und unwiderrufliche Übertragung von Daten wird problematisiert. Der Autor kommt zu dem Schluss, dass die Einführung eines Dateneigentums und dessen Verhältnis zum Datenschutzgesetz vertiefter Studien bedürfte.

1719 Dass ein Eigentumsrecht der Datensubjekte das Risiko in sich trage, zum Nachteil der Datensubjekte und deren Schutz zu wirken, wurde jüngst trefflich von Weber/Thouvenin konstatiert.[2242] Die beiden Autoren äussern sich skeptisch zum Eigentum an Personendaten.

1720 Ebenso kritisch Stellung bezieht Schunck in seinem Aufsatz zur Propertisierung von Personendaten.[2243] Er gibt ein differenziertes Panorama über das geltende Recht wie auch über Stärken und Schwächen eines sachenrechtlichen gegenüber einem persönlichkeitsrechtlichen Ansatz. Überzeugend beschreibt er die Verhaftung des Datenschutzrechts in der Dogmatik des zivilrechtlichen Persönlichkeits-

2238 Thouvenin, SJZ 2017, 21 ff., 30 f.; vgl. kritisch die Einwände mit Blick auf ein property right an Personendaten Litman, Stan. L. Rev. 2000, 1283 ff., 1294 ff.
2239 Thouvenin, SJZ 2017, 21 ff., 30.
2240 Ders., a. a. O., 21 ff., 31.
2241 Ders., a. a. O., 21 ff., 32.
2242 Vgl. Weber/Thouvenin, ZSR 2018, 60 ff., 64.
2243 Schunck, digma 2013, 66 ff.; m. w. H. zu den kritischen Stellungnahmen im US-amerikanischen Diskurs betr. property rights an Personendaten Schwartz, Harv. L. Rev. 2004, 2055 ff., 2076 ff.

rechts, wobei er die Mechanik sowie die Defizite des DSG darlegt. In der Folge analysiert er eine «Propertisierung» an personenbezogenen Angaben, welche der auch in der Schweiz gesetzlich gestützten Exklusion des Datensubjektes entgegenwirken solle.[2244] Vier Argumente resp. Elemente führt er bezüglich der Anerkennung einer eigentumsrechtlichen Position des Datensubjektes an: erstens die Inklusion des Subjektes, dessen Einwilligung primäres Verarbeitungselement wird; zweitens die Möglichkeit der Monetarisierung, der das ideell gedachte Persönlichkeitsrecht bis heute mit Widerstand begegnet; im Sinne der Erwägungen der ökonomischen Analyse des Rechts führt Schunck drittens den Effekt der Verteuerung von Personendaten an; und viertens sei die Steigerung der Effizienz relevant – das Rechts- resp. Geschäftsverhältnis werde stärker aus dem Einflussbereich der staatlichen Verantwortlichkeit gelöst und in den Privatbereich verlagert: Es seien der Datenkollektor und das Subjekt, die sich über die Austauschbedingungen zu einigen haben.[2245] Auch Schunck setzt sich mit den Einwänden auseinander, die einem Dateneigentum entgegengehalten werden. Dazu gehören die Monopolisierung des Wissens sowie die Illusion der Egalität der Vertragspartner.[2246] Er weist richtig darauf hin, dass die (datenschutzrechtlichen) Probleme bei einer eigentumsrechtlichen Konzeption des Datenschutzes im Grunde genommen bestehen bleiben.[2247] Damit lautet, nach einer Analyse auch der Gegenargumente, sein Plädoyer, die *Kontinuität der Anknüpfung im Persönlichkeitsrecht zu bewahren*, zumal das Persönlichkeitsrecht der Einwilligung und dem Willen des Subjektes eine eigentumsähnliche Position einräumen könne.[2248]

1721 Einen Beitrag zur Klärung der Frage, ob ein Datenrecht im Sinne eines Rechts an eigenen Personendaten anzuerkennen sei, leisten zudem Hürlimann/Zech. Die Autoren weisen zutreffend darauf hin, dass im Schweizer Recht in singulärer Weise über weite Strecken hinweg keine Rechte an Daten im Sinne von zuweisenden Herrschaftsbefugnissen anerkannt sind. Damit entkräften sie Behauptungen, wonach das schweizerische Regime ein Recht auf informationelle Selbstbestimmung verbürge. Hürlimann/Zech sprechen sich für die Stärkung der Rechtsposition des Datensubjektes aus, begegnen indes einer Strategie, welche dies durch die Einführung eines Eigentums an Daten erreichen will, mit Skepsis. Eine solche Lösung beurteilen die Autoren als Hemmschuh für die Schweizer Wirtschaft.[2249]

2244 Schunck, digma 2013, 66 ff., 66 ff.; die Exklusionsproblematik wurde bereits beschrieben durch Samuelson, Stan. L. Rev. 2000, 1125 ff., 1132 ff.; Bergelson, UC Davis L. Rev. 2003, 379 ff., 419; Buchner, 276 ff.
2245 Vgl. m. w. H. Schunck, digma 2013, 66 ff., 66 f.
2246 Ders., a. a. O., 66 ff., 68 f.
2247 Ders., a. a. O., 66 ff., 70.
2248 Ders., a. a. O., 66 ff., 71 f.
2249 Hürlimann/Zech, sui-generis 2016, 89 ff., 93.

Zusammenfassend lässt sich feststellen, dass das Eigentumsparadigma bezüglich Personendaten in den letzten Jahren eine für die Disziplin des Datenschutzrechts beachtliche wissenschaftliche Aufmerksamkeit auf sich gezogen hat. Mit dem Eigentumsparadigma ist die Hoffnung verbunden, datenschutzrechtliche Herausforderungen wirksam zu adressieren. Dass die datenschutzrechtliche Diskussion sich vom subjektiven Recht der Persönlichkeit zum subjektiven Recht des Eigentums verlagert, ist teilweise typologisch für die Herangehensweise von zivil- und privatrechtlichen Expertinnen und Experten. Für diese datenschutzrechtliche Forschung ist zu attestieren, dass sie in den Anfängen steht und rudimentär bleibt. Bislang wird der eigentumsrechtliche Ansatz in der Schweiz eher kritisch beurteilt, wobei vertiefende, auch interdisziplinäre sowie empirische Studien gefordert werden.[2250] Fest steht, dass ein Eigentum an Personendaten, das den Datensubjekten zugewiesen wird, von einer prinzipiellen Kontrolle resp. einem Herrschaftsrecht der Datensubjekte ausgeht. Mit der Anerkennung eines Eigentumsrechts der Datensubjekte an ihren Daten würde auch die vermögensrechtliche Komponente anerkannt. 1722

Einbettend ist anzufügen: Personendateneigentum und persönlichkeitsrechtlich begründetes Recht an eigenen Daten (nach dem Vorbild von Buchner), das neben der ideell-persönlichkeitsrechtlichen auch die vermögensrechtliche Komponente anerkennt, nähern sich einander an: Beide Konstruktionen würden die Zuordnungsfrage zugunsten des Datensubjektes entscheiden. Beide Rechtskonstruktionen müssten an ihren Anfang die *Entscheidungskompetenz des Individuums stellen*.[2251] In beiden Ausschliesslichkeits- resp. Kontrollrechten der Datensubjekte an ihren Personendaten wäre auch ein Property-Gehalt angelegt: Das Datensubjekt und Individuum wäre grundsätzlich in der Position, darüber zu befinden, unter welchen Bedingungen seine Personendaten anderen zugänglich gemacht werden und durch diese verarbeitet werden können.[2252] Damit kommt zwingend den *Einwilligungskonstruktionen* resp. dem *informed consent* prioritäre Bedeutung zu.[2253] 1723

Die *Totalrevision* des DSG für den privaten Bereich schafft seine ursprünglich konstruierte und tragende Säule des Persönlichkeitsschutzes nicht ab: Es gilt weiterhin eine datenschutzrechtliche Missbrauchs- oder Integritätsgesetzgebung, in deren Regime die Datensubjekte in erster Linie Abwehrbefugnisse haben. Die Regelung entscheidet im Zuordnungskonflikt zugunsten des Verarbeitenden. Das DSG für den privaten Bereich bedürfte, um ein Recht an eigenen Daten anzuer- 1724

2250 So Thouvenin, SJZ 2017, 21 ff., 23; Hürlimann/Zech, sui-generis 2016, 89 ff., 94.
2251 Vgl. Bergelson, UC Davis L. Rev. 2003, 379 ff., 402.
2252 Dies., UC Davis L. Rev. 2003, 379 ff., a. a. O., wobei die Autorin auf die duale Natur des privacy right und die Ähnlichkeit zum Copyright hinweist.
2253 Vgl. auch Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 44.

kennen, einer Anpassung und Neupositionierung der *Einwilligung des Datensubjektes*. Die Diskussion ist lanciert, viele Fragen sind offen. Doch obschon die informierte Einwilligung resp. Anerkennung der informationellen Selbstbestimmung resp. die Forderung nach einem Personendateneigentum Hochkonjunktur erlangt hat, findet das Rezept bereits heute konzeptionelle und damit grundlegende Kritik.

1725 Solchen kritischen Analysen widmen sich die anschliessenden Ausführungen, nicht ohne festzuhalten: Die jüngsten Entwicklungen vonseiten der Gesetzgeber wählen, wie gezeigt, *andere Strategien und Ansätze*. Für die rechtlichen Neuerungen ist nicht das «Umschwenken» von einem zivil- und privatrechtlichen subjektiven Recht, dem Persönlichkeitsrecht, zu einem anderen subjektiven Recht, dem Eigentumsrecht, charakteristisch. Vielmehr werden dem weiterhin persönlichkeitsrechtlich begründeten Datenschutzrecht neue Ansätze zugefügt, namentlich der Governance- und Risiko-Ansatz. Zugleich deutet sich über die DSGVO, weniger explizit über das totalrevidierte DSG an, dass datenschutzrechtliche Schutzziele plural sind. Die jüngsten Rechtsentwicklungen gehen damit über die zivil- und privatrechtlichen Kategorien hinaus. Sie integrieren den Datenschutz in eine erweiterte Landschaft. Eine solche Strategie wird im letzten Kapitel dieser Schrift nutzbar gemacht, um einen neuen Ansatz – das Recht auf informationellen Systemschutz – zu verdichten. Er leitet sich u. a. aus Untersuchungen ab, welche den informationellen Subjektschutz und seinen Ausbau skeptisch sehen.

5. Weitere Ansätze

5.1. Kartografie der Konstruktionen, De- und Rekonstruktionen

1726 Die vorangehende Darstellung ausgewählter Beiträge zeigte, dass bezüglich Personendaten *Zuordnungsfragen* im Zentrum der wissenschaftlichen Aufmerksamkeit stehen. Die datenschutzrechtliche Debatte bleibt von einer Subjekt-Objekt-Wahrnehmung geprägt, die ihren Ursprung im Recht der analogen Welt hat. Zudem wird die Diskussion von der Kategorie der subjektiven Rechte geprägt. Der traditionelle Ansatz eines abwehrrechtlich konstruierten, im Persönlichkeitsrecht verankerten Datenschutzrechts wird rechtswissenschaftlich nicht nur gutgeheissen. Neuerdings wird *de lege ferenda* ein Herrschaftsrecht der Datensubjekte an Personendaten diskutiert und gefordert. Für ein Recht an «eigenen Personendaten» werden beide der etablierten subjektiven Rechte des Zivilrechts vorgeschlagen: Nicht nur das persönlichkeitsrechtlich angeknüpfte Selbstbestimmungsrecht, das eine Verwertungskomponente aufweisen kann, sondern auch ein Eigentumsrecht wird analysiert. Die Debatten bewegen sich im Rahmen dualer Konzepte von Subjekt versus Objekt sowie Persönlichkeitsrecht versus Eigentumsrecht.

Dort, wo für ein Recht des Datensubjektes an den eigenen Daten eingetreten wird, gewinnt die *informierte Einwilligung* – m. E. ungeachtet eines persönlichkeitsrechtlichen oder eigentumsrechtlichen Ansatzes – prioritäre Bedeutung. Das Konzept der informierten Einwilligung hat sich zu einer Hauptlösungsstrategie verdichtet, um die datenschutzrechtlichen Herausforderungen zu adressieren. 1727

Eine Betrachtung, wonach das Datenschutzrecht Datenflüsse in ihrer Einbettung in Kontexte zu regulieren hat, findet sich in der rechtswissenschaftlichen Diskussion Kontinentaleuropas nur ansatzweise.[2254] Damit wird eine neue Perspektive in das Thema des Datenschutzes und seines Rechts eingespeist, das sich bislang auf die Kategorien des Datensubjektes und des Personendatums als Quasi-Objekt fokussierte. Früh wurde die Relevanz des Verarbeitungszusammenhangs im Datenschutzrecht resp. die Problematik des Kontextverlustes in Anbetracht automatisierter Verarbeitungen insb. von Simitis betont.[2255] Dem Aspekt kommt zentrale Bedeutung im Rahmen der bundesverfassungsgerichtlichen Anerkennung eines Rechts auf informationelle Selbstbestimmung zu.[2256] 1728

Simitis war es auch, der eine Konzeptionierung des Datenschutzrechts als Unterfall des Persönlichkeitsrechts – sei es in Gestalt der Abwehr von Penetrationen in eine individuelle Rechtsposition resp. die Persönlichkeitssphäre, sei es in Gestalt eines Rechts an eigenen Daten oder eines Dateneigentums – bald schon kritisch beurteilte. Mit diesen Diskussionen würde über den sinnvollen Ausgleich zwischen Herrschaftssphären diskutiert. Damit allerdings blieben strukturelle Aspekte im Hintergrund.[2257] 1729

Schunck bezeichnet es als Illusion zu meinen, dass ein eigentumsrechtlicher Ansatz sämtliche datenschutzrechtlichen Probleme zu beseitigen vermöge.[2258] Dem Autor ist beizupflichten. Die jüngsten rechtlichen Entwicklungen mit ihren Neuerungen reden ihm das Wort. 1730

Der folgende Abriss schält heraus, weshalb sich das Nachdenken über die *Weiterentwicklung des Datenschutzrechts* – selbst nach den jüngsten Rechtsentwicklungen – *nicht auf die Debatte rund um zwei Hauptkategorien der subjektiven Rechte zurückziehen kann*. Die Suche nach dem Schlüssel zum datenschutzrechtlichen Erfolg kann nicht allein im Lichtpegel der subjektiven Rechte und in einem Herrschaftsrecht an eigenen Datenerfolgen. Ungeachtet eines persönlich- 1731

2254 Vgl. Gächter/Egli, 6, 12, 15, 30, 55; Waldmeier, 1, 145 ff.; Helfrich, 29 ff.; vgl. allgemeiner Druey, 86 f., 134, 400; Passadelis, in: Passadelis/Rosenthal/Thür (Hrsg.), § 6 N 6.1, leitet seinen Beitrag mit der Wendung der «Internationalisierung von Datenströmen» ein; richtungsweisend dazu, dass die Betrachtung von Personendatenflüssen den Gesetzgeber anleiten sollen, Nissenbaum, *passim*.

2255 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 10, 18, 20.

2256 Vgl. zweiter Teil, V. Kapitel und weiterentwickelt zum Systemschutz, dritter Teil, IX. Kapitel.

2257 Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 26.

2258 Schunck, digma 2013, 66 ff., 72.

keitsrechtlichen oder eigentumsrechtlichen Gewandes spielt *in beiden Konstruktionen die informierte Einwilligung des Datensubjektes eine initiale Rolle*. Die kritischen Befunde zu ihrer Funktionstüchtigkeit und -weise erhellen den Weg zu einem Lösungsansatz, der ein Recht auf informationellen Systemschutz begründet. Im Zuge dieser Schrift wurde an mehreren Stellen freigelegt, dass im Datenschutzrecht seit jeher Aspekte des Systemschutzes angelegt sind – auch wenn das DSG in seinem Art. 1 (n)DSG den persönlichkeitsrechtlichen Subjektschutz konstant an die erste Stelle stellt.

1732 Mehrere jüngere Untersuchungen befassen sich mit der Funktionstüchtigkeit eines Kontrollrechts des Datensubjektes resp. eines Rechts an eigenen Daten – ungeachtet seiner dogmatischen Konstruktion – und damit der informierten Einwilligung im Datenschutzrecht. Sie stellen die *Tauglichkeit der Konstruktion in Frage, namentlich in Anbetracht der Realitäten*.[2259] Eine solche Analyse findet sich insb. bei Radlanski, dessen Untersuchung sich an spezifischen Verarbeitungszusammenhängen mit entsprechenden Kontexten orientiert.[2260]

1733 Besagte Studien beschränken sich nicht darauf, die Sinnhaftigkeit datenschutzrechtlicher Einwilligungskonstruktionen zu dekonstruieren. Vielmehr werden Vorschläge zur Konstruktion einer kommenden Generation von Datenschutzrechten abgeleitet. Von besonderem Interesse ist die Forderung nach *Differenzierung:* Demnach solle die informierte Einwilligung nicht als Pauschalrezept zur Bewältigung datenschutzrechtlicher Herausforderungen gesehen werden. Vielmehr dränge sich ein selektiver Einsatz auf.[2261] Aus dergestaltigen Forderungen lässt sich ein *Plädoyer für ein bereichsspezifisch ausdifferenziertes Datenschutzrechtsregime ableiten*.

1734 Bevor eine Auseinandersetzung mit diesen ergänzenden Perspektiven stattfindet, soll eine weitere, ebenso prominent positionierte Lösungsstrategie des Datenschutzrechts nicht unerwähnt bleiben. Es handelt sich gewissermassen um die *Gegenstrategie der informierten Einwilligung* – sie erfolgt durch die *Anonymisierung*. Während die informierte Einwilligung das Band zwischen Personendaten als Quasi-Objekten und dem Datensubjekt stärkt, vollzieht die Anonymisierung die Gegenbewegung: Das Band zwischen den Angaben resp. Daten und der Person resp. dem Datensubjekt wird gekappt, die semantische Ebene quasi eli-

2259 Vgl. insb. Radlanski, 11 ff. und zur Analyse anhand von Referenzgebieten 124 ff.; kritisch auch Heuberger, N 285 ff.; m. w. H. Barocas/Nissenbaum, 4 f.; Dies., Communications of the ACM 2014, S. 31 ff., 32; Nissenbaum, 1 f. und 231 führt hierzu aus, dass sie die herrschende Vorstellung, wonach der Schutz von privacy eine strikte Limitierung des Zugangs zu Personendaten oder ein Recht auf Kontrolle von Personendaten durch die Datensubjekte meine, ablehne; vielmehr ginge es um die angemessene Regelung von Personendatenflüssen.

2260 Vgl. Radlanski, 124 ff., 124 ff. zur Analyse anhand von Referenzgebieten.

2261 Nissenbaum, 145 ff., insb. 147 f., wobei die Einwilligung eines von vielen Transmissionsprinzipien ist zur Gestaltung von kontext-adäquaten Datenflüssen; Radlanski, 192 ff.

miniert.[2262] Auch die *Anonymisierung* wird als Patentrezept gegen disruptive Effekte, die Datenverarbeitungstechnologien bringen, bezeichnet.[2263] Der Ansatz wird inklusive der an ihm geübten Kritik ebenso erwähnt werden. Auch hieraus werden Erkenntnisse für die Gestaltung des Datenschutzrechts der Zukunft generiert. Folglich sind die nachfolgenden Ausführungen als Brücke in das IX. und letzte Kapitel dieser Studie zu lesen.

5.2. Grenzen eines subjektiven Rechts an eigenen Daten

5.2.1. Vorbemerkungen

Die Idee eines Rechts an eigenen Daten resp. der informationellen Selbstbestimmung geht Hand in Hand mit der Idee einer Herrschaftsbefugnis des Datensubjektes an den sich auf sie beziehenden Personendaten einher. Eine solche Konzeptionierung wurde im Recht und im rechtswissenschaftlichen Diskurs prioritär behandelt.[2264] In Erinnerung gerufen seien insofern die Worte des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung als Recht des Einzelnen, «grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Angaben zu bestimmen».[2265] 1735

Charakteristisch für ein solches subjektives Recht ist, dass die *Zuordnungsfrage* bezüglich Personenangaben dem Grundsatz nach zugunsten des Datensubjektes entschieden wird. Der informierten Einwilligung kommt damit eine vorgeschaltete Rolle zu. Gleichwohl ist unbestritten, dass ein solches subjektives Recht – ungeachtet seiner Gestaltung im Detail – weder absolute Vorrangstellung beanspruchen noch schrankenlos gelten kann. 1736

Die vorgeschlagenen Rechtskonstruktionen werden, wie gezeigt, nicht nur inhaltlich unterschiedlich gestaltet. Auch die Bewertungen fallen unterschiedlich aus. So finden sich Stimmen, die ein subjektives Recht an eigenen Daten als *das* Rezept zur Emanzipation des Individuums gegenüber Degradierungs- und Einverleibungseffekten vonseiten der Informationsverarbeitungstechnologien beschreiben. Ein Recht an eigenen Daten soll das Datensubjekt gegen Ausbeutungen durch die Technologiekonzerne mit ihrem Gewinnstreben und den hierbei eingesetzten Geschäftspraktiken schützen. Den Datensubjekten soll ein Recht an eigenen Daten in Gestalt eines Kontrollrechts verliehen werden. Anders dagegen Beiträge, die in 1737

2262 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 49.
2263 Vgl. Dies., a. a. O., 44 ff., 45 ff.; m. w. H. Heuberger, N 77 ff.
2264 Vgl. Nissenbaum, 70, mit Hinweis auf eine Definierung der privacy durch Westin, die Parallelen zum Diktum des Bundesverfassungsgerichts aufweist: «the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others».
2265 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983.

einem Konzept des Rechts an eigenen Daten einen Datenegoismus der Individuen verorten. Das sei mit Interessen der an den Informationen Interessierten und der Allgemeinheit nicht zu vereinbaren. In den verschiedenen Diskussionsbeiträgen finden sich oft frappante Anleihen an die traditionellen Debatten zum Sacheigentum der analogen und körperlichen Welt.[2266] Noch weiter geht das Verdikt, wonach der Terminus einer informationellen Selbstbestimmung eine *contradictio in adiecto* sei – eine Selbstbestimmung bezüglich Informationen sei bereits aus kategorischen Gründen nicht möglich.[2267]

1738 Die *Dekonstruktion des datenschutzrechtlichen Selbstbestimmungs-, Autonomie- oder Eigentumsparadigma* genauer zu beleuchten, ist produktiv, um die Rekonzeptionalisierung des Datenschutzrechts der Zukunft möglich zu machen. Richtungsweisend sind gerade auch die Vorbehalte, die gegenüber den datenschutzrechtlichen Einwilligungskonstruktionen angebracht werden. Sie lassen sich grob in zwei Gruppen kategorisieren: Zum einen geht es um die *ungenügende Funktionstüchtigkeit in Anbetracht der Realitäten*, zum anderen um eine *konzeptionelle und theoretische Problematisierung*. Der Lösungsansatz gilt als nicht kompatibel mit dem notwendig erweiterten Schutzverständnis datenschutzrechtlicher Regelungen.

1739 Innerhalb der *ersten Gruppe* von Vorbehalten wird thematisiert, dass die Erfüllung der *Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung* in der Realität oft an Grenzen stösst. Mit anderen Worten wird die Realisierung und Realisierbarkeit einer *sinnhaften Einwilligung* bezweifelt. Gesprochen wird von einer Fiktion, in welcher Einwilligungen zu einem reinen Formalismus verkommen.[2268] Eine rein schematisch-formelle Einwilligung (im Sinne eines Abnickens) vermag auch im Kontext des Datenschutzrechts den rechtlichen Anforderungen nicht zu genügen. Spezifisch sind damit die Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung angesprochen: Die *Informiertheit* wie

2266 Vgl. m. w. H. Flückiger, PJA 2013, 837 ff.

2267 Nassehi, 295; eindrücklich sichtbar wird die Inkompatibilität bei Cavoukian, digma 2009, 20 ff., 20, welche von der Herausforderung spricht, freie Datenflüsse sowie das Kontrollrecht resp. das Recht auf informationelle Selbstbestimmung der Subjekte zu gewährleisten; dazu, dass sich für den Bereich der Biodatenbanken ein Konsens in der biomedizinrechtlichen Literatur durchsetzt, wonach ein individualistisches Schutzkonzept des informed consent nicht funktioniert, m. w. H. Fateh-Moghadam, BJM 2018, 205 ff., 220 ff.; nach Bull, Vision, 46 ist eine umfassende informationelle Selbstbestimmung illusionär; von einem Aushebeln des Datenschutzes durch die Einwilligung spricht Schaar, 226; Schermer/Custers/van der Hof, Ethics Inf. Technol., 117 ff., auch mit Hinweis auf die Vorschläge, die zur Beseitigung der faktischen Schwächen des informed consent im Datenschutzrecht diskutiert werden.

2268 Buchner/Kühling, Beck-Komm.-DSGVO, Art. 7 N 10; Radlanski, 18; kritisch zur Einwilligung auch Rosenthal, Jusletter vom 27. November 2017, N 35; zur Verbesserung der Wirksamkeitsvoraussetzungen Rogosch, 190 ff.; Kamp/Rost, DuD 2013, 80 ff.; dazu, dass Datenschutz oft mit informationeller Selbstbestimmung gleichgesetzt wird und damit die Einwilligung prioritäre Bedeutung erlangt, was allerdings mit den Realitäten des 21. Jahrhunderts nicht kompatibel ist, vgl. Koops, Tilburg Law School Legal Studies Research Paper Series 2015, 1 ff., 3 f.; allgemeiner zur Fiktion eines umfassenden Rechts auf informationelle Selbstbestimmung Bull, Vision, 46.

die *Freiwilligkeit* der Einwilligung werden – in der Realität überprüft – auf eine harte Probe gestellt.

Die *zweite Gruppe* von Einwänden ist *konzeptionell-theoretischen Charakters*. Problematisiert wird, *dass die informierte Einwilligung dem Datenschutz und der Gewährleistung seiner Schutzaufträge* selbst abträglich sein könne. Anders gewendet: Die Konstruktion gefährde die Garantie des Privatheitsschutzes, anstatt diesen zu gewährleisten. Damit werden Herrschaftsrechte der Datensubjekte unter bestimmten Umständen als datenschutzrechtlich kontraproduktiv identifiziert. Kritisch beurteilt wird namentlich, dass der Umgang mit Personendaten weitgehend individuell und privatautonom verhandelbar wird.[2269] 1740

5.2.2. Die datenschutzrechtliche Einwilligung im Reality Check

Mehrere Untersuchungen aus jüngerer Zeit reflektieren die datenschutzrechtliche Einwilligung im Lichte der Realitäten. Sie kommen zu dem Ergebnis, dass der Lösungsansatz zwar theoretisch tauglich sein möge, in der Praxis umgesetzt allerdings mehrere Schwachstellen aufweise. Die Einwände, welche gegen die informierte Einwilligung resp. ein Recht an eigenen Daten und das Recht auf informationelle Selbstbestimmung aufgeführt werden, sind grundlegend und konzeptioneller Natur. Ebendies erstaunt in Anbetracht der Tatsache, dass die Stärkung informationeller Selbstbestimmung, für welche das Einwilligungserfordernis als paradigmatisch gelten kann, im Zentrum der wissenschaftlich diskutierten Lösungsansätze steht.[2270] 1741

Eindringlich die Worte von Barocas/Nissenbaum: Sie sprechen vom Ersticken einer Resthoffnung mit Blick auf Notice-and-Consent-Verfahren angesichts von Big Data.[2271] Die Wissenschaftlerin und der Wissenschaftler weisen darauf hin, dass die Preisgabe vieler Angaben durch einige wenige Personen Auswertungsmöglichkeiten ergeben, deren Konsequenzen unzählige Menschen tangieren. Besagte Informationen betreffen auch Personen, die ihre eigenen Angaben gerade nicht preisgeben (wollten). Wenn Analysten aus Angaben von wenigen Menschen Regeln und Annahmen für alle Menschen entwickeln, dann spiele der Consent der einzelnen Person keine Rolle mehr.[2272] 1742

Eine weitere Kernkritik am System und Recht auf informationelle Selbstbestimmung wird mit futuristischen Begrifflichkeiten umschrieben: Sie wird als *fiktiv* 1743

2269 Vgl. den Hinweis bei Bergelson, UC Davis L. Rev. 2003, 379 ff., 401 f.; Weber/Thouvenin, ZSR 2018, 60 ff., 64; vgl. zu weiteren Kritikpunkten m. w. H. Schunck, digma 2013, 66 ff., 68 f.
2270 Vgl. Barocas/Nissenbaum 1 ff., 4; Dies., in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 44.
2271 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff.
2272 Dies., a. a. O., 44 ff., 61 f.

oder *utopisch* taxiert.[2273] Anders gewendet: Die datenschutzrechtliche Einwilligung funktioniert in der Realität oftmals nicht sinnhaft.[2274] Innerhalb dieses Problemfeldes werden mehrere Aspekte thematisiert.

1744 Zunächst ist betreffend die Einwilligung als Instrument des Datenschutzes und zur Gewährleistung der Selbstbestimmung des Datensubjektes auf ein Phänomen hinzuweisen, das zunächst als *Paradoxon* erscheint. Mehrere Studien belegen, dass Menschen tiefe Zweifel und Vorbehalte gegenüber den modernen Verarbeitungstechnologien äussern. Es ist empirisch belegt, dass bis heute der grösste Teil der Menschen – auch die jüngeren Generationen – den eindringlichen Wunsch nach wirksamem Schutz ihrer Privatheit äussern.[2275] Geht es allerdings faktisch um die Umsetzung, handeln Menschen in aller Regel in einer dem Datenschutz entgegenlaufenden Weise. Sie nutzen Dienste wie WhatsApp oder Facebook intensiv, selbst wenn sie diesen aus datenschutzrechtlicher Perspektive mit Skepsis begegnen. Es gibt kaum Personen hierzulande, die auf sämtliche Dienste wie diejenigen von Amazon, WhatsApp, Google, Skype oder Ähnliches aus Erwägungen des Datenschutzrechts gänzlich verzichten. Datenschutzerklärungen werden – so der empirisch bestätigte, ernüchternde Befund – weder gelesen noch verstanden.[2276]

1745 Hinsichtlich formularmässiger Einwilligungserklärungen wurde sodann festgestellt, dass sich ein substanzieller Teil der Menschen *passiv verhält*.[2277] Beim opt-in im engeren Sinne muss das Datensubjekt selbst aktiv werden, um seine Einwilligung zu erteilen (explizite Ja-Erklärung). Dies erfolgt z. B., indem in eine leere Checkbox ein Häkchen gesetzt wird.[2278] Anders beim opt-out, wo die Einwilligung quasi angenommen wird. Das Datensubjekt muss für sein «Nein» aktiv werden. Dies geschieht z. B., indem man ein Häkchen setzt. Tut man dies nicht, wird von einer Einwilligung ausgegangen. Die beiden Systeme führen, so die empirischen Untersuchungen, zu signifikanten Unterschieden: Wird die aktive und explizite Einwilligung verlangt, stimmen nur 20 Prozent der Nutzenden zu. Wird die Einwilligung angenommen und ist es die Verweigerung, die aktiv erfolgen muss, waren es wiederum nur 20 Prozent der Nutzenden, die dies taten.[2279]

2273 Vgl. statt vieler Flückiger, PJA 2013, 837 ff., 838, 856 f.; Buchner/Kühling, Beck-Komm.-DSGVO, Art. 7 N 10; Radlanski, 18.
2274 Hierzu namentlich Radlanski, *passim*.
2275 Vgl. Martin/Nissenbaum, Abstract; Bergelson, UC Davis L. Rev. 2003, 379 ff., 427; Bolliger/Féraud/Epiney/Hänni, II; vgl. auch Nissenbaum, 186 ff.; BR, Schlussbericht Evaluation 2011–1952, 335 ff., 342.
2276 «Over the course of roughly a decade and a half, privacy policies have remained the linchpin of privacy protection online, despite overwhelming evidence that most of us neither read nor understand them», Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 57; Passadelis, NZZ vom 7. November 2019 sowie NZZ-Verlagsbeilage, 3.
2277 Buchner, DuD 2010, 30 ff., 32; Rogosch, 117; vgl. Lindner, 128.
2278 Vgl. m. w. H. Radlanski, 19; vgl. auch Hoeren, LMK 2008, 65 f.
2279 Radlanski, 20.

Online-Bestellungen wollen in aller Regel ohne Exegese der privacy policy getätigt werden. Entsprechend werden sie auch ohne entsprechende Lektüre erledigt. Warum? Wenn eine Person ein Buch online erwerben möchte, dann möchte sie ein Buch bestellen und nicht Datenschutzerklärungen studieren müssen. Wenn eine Person surfen möchte, möchte sie surfen und keine privacy policies studieren. Das Gut, Interesse oder Ziel des Privaten kollidiert mit anderen Gütern, Zielen und Interessen wie Informationen recherchieren, Zeitung lesen, online Kontakte pflegen, «gamen», (digital) einkaufen oder Rabatte resp. Geschenke im Austausch gegen Personendaten erhalten.[2280] Wenn die Chance besteht, durch die Nutzung von Treueprogrammen Rabatte und Sonderangebote zu erhalten, werden datenschutzrechtliche Bedenken beiseitegeschoben. Eine Lektüre, die im Ergebnis dazu führt, nur zu verstehen, wie extensiv Personendaten verarbeitet werden, erscheint als reine Zeitverschwendung. 1746

Man mag geneigt sein zu schlussfolgern, dass der Privatheits- und Datenschutz den Individuen trotz abstrakter Behauptungen eben doch nicht wichtig sei. Oder dass sie ihre Autonomie ausüben, indem sie, um das andere Gut zu erlangen, auf die Privatheit verzichten. Allerdings scheint ein anderer Schluss angezeigt: Die Kontroll- und Einwilligungskonstruktionen stossen in der Realität an Grenzen. Sie vermögen Ziele des Datenschutzrechts nicht angemessen umzusetzen. Das *in abstracto* deklarierte Interesse der Menschen, wonach diese dem Datenschutz zumindest theoretisch-abstrakt hohe Bedeutung zumessen, *kollidiert mit anderen Interessen.* Folglich wird vertreten, dass das Instrument von «notice and consent» im Kontext des Datenschutzes in weiten Feldern nicht das richtige sei, um Anliegen des Datenschutzes zu bewerkstelligen.[2281] 1747

Weniger weit gehen Beiträge, welche Defizite des Instruments zwar anerkennen, an diesem als Hauptlösungsansatz datenschutzrechtlicher Herausforderungen gleichwohl festhalten wollen. Vorgeschlagen werden *Modifikationen*, die den Befund, wonach sich das Gros der Datensubjekte passiv verhält, adressieren. Daran anknüpfende Ansätze fordern das aktive Tätigwerden des Datensubjektes durch ein opt-in im engeren Sinne, zudem die Erhöhung von Transparenzvorgaben durch Separierung von privacy policies und Einwilligungserklärungen von anderen Vertragsinhalten usf. 1748

Einwände struktureller Natur gegenüber der datenschutzrechtlichen Einwilligung als (Haupt-)Instrument eines zeitgemässen und effektiven Datenschutzrechts sind damit nicht ausgeräumt. Insofern werden Defizite benannt, die auch, aber nicht nur die Realisierung *sinnhafter*, sprich nicht rein formeller Zustimmungen («meaningful consent») betreffen.[2282] 1749

2280 Hierzu Martin/Nissenbaum, Measuring Privacy, Abstract.
2281 Nissenbaum, 105.
2282 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 58 ff.

1750 *Zwei Praktiken* sind in diesem Zusammenhang vorausschickend zu erwähnen. Beide Praktiken sind kritisch und finden sich sowohl im Rahmen eines Regimes, wie es das schweizerische DSG für den privaten Bereich kennt, als auch unter einem Regime, wie es die DSGVO implementiert.

1751 In der *ersten Konstellation* wird die datenschutzrechtliche Einwilligung entgegen den gesetzlichen Vorgaben *nicht* eingeholt. Obschon eine informierte Einwilligung einzuholen wäre, geschieht dies nicht. Es handelt sich um einen Verstoss gegen datenschutzgesetzliche Vorgaben. Werden rechtlich gebotene Einwilligungen nicht eingeholt, ist dies ein Element des in dieser Arbeit präsentierten Vollzugsdefizits.

1752 In der *zweiten Konstellation* werden datenschutzrechtliche Einwilligungen, obschon rechtlich nicht verlangt, quasi zur Sicherheit eingeholt. Eine Praxis, wonach die Einwilligung der Datensubjekte pro forma und zur Reserve eingeholt wird, obschon es dieser gar nicht bedürfte, suggeriert dem Datensubjekt eine Selbstbestimmung, die ihm von Gesetzes wegen gerade nicht eingeräumt wird. Ist eine Personendatenverarbeitung ohne Einwilligung zulässig, ist das Einholen der Einwilligung ebenso problematisch. Eine juristische Beurteilung des Vorgangs fällt gleichwohl nicht leicht: Das Vorgehen könnte als Verstoss gegen den Verarbeitungsgrundsatz von Treu und Glauben sowie die Transparenzvorgaben beurteilt werden. Offensichtlich datenschutzrechtlich unrechtmässig ist die in der Realität ebenso anzutreffende umgekehrte Problematik, erwähnt als erste Konstellation.

1753 Weitere Schwachstellen der datenschutzrechtlichen Einwilligung werden mit Blick auf die *Gültigkeitsvoraussetzungen* der Einwilligung und damit der Informiertheit sowie Freiwilligkeit beschrieben. Radlanski geht davon aus, dass ein grosser Teil der erteilten Einwilligungserklärungen ungültig sei, weil die Informiertheit oder die Freiwilligkeit nicht gewährleistet seien. Beide Gültigkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung – die Freiwilligkeit und die Informiertheit – geraten, je nach Verarbeitungszusammenhang und Verarbeitungsmethoden, stark unter Druck.[2283]

1754 Die *Freiwilligkeit als erste Voraussetzung* für eine wirksame Einwilligung verlangt auch im Datenschutzkontext – grob und negativ definiert – die Abwesen-

2283 Radlanski, 11 ff. und 192 ff.; vgl. auch Simitis, NomosKomm-BDSG, § 4a N 3 ff.; zu den datenschutzrechtlichen Einwilligungsvoraussetzungen weiter Liedke, 25 ff.; Rogosch, 69 ff.; kritisch zur Einwilligungskonstruktion nach Totalrevision des DSG Rosenthal, Jusletter vom 27. November 2017, N 35 ff.; zur Freiwilligkeit und Ausdrücklichkeit der datenschutzrechtlichen Einwilligung sodann vertiefend Vasella, Jusletter vom 16. November 2015; früh und grundlegend zur störenden Wirkung von Machtasymmetrien auf die informationelle Selbstbestimmung Mallmann, 28; zu Theorien der Macht Luhmann, Macht, 13 ff.

heit von Zwang.[2284] Unter dem Begriff des Zwanges werden mehrere Tatbestände eingefangen, von Gewalt über Drohung, Gefährdung qua Machtungleichgewicht, Abhängigkeit und übermässigen Anreizen bis hin zu sozialem Druck.[2285] Wann diese Einflüsse ein Mass an Intensität erreicht haben, damit sie rechtlich relevant werden und die Freiwilligkeit der Einwilligung untergraben, ist und bleibt nicht exakt fixiert und fixierbar.

Unter dem Titel der Freiwilligkeit ist zudem der Befund zu berücksichtigen, wonach personenbezogenen Angaben ein *monetärer Wert* zugewiesen wird.[2286] Manch ein Datensubjekt will diesen Wert für sich nutzbar machen. Unklar bleibt allerdings: Wann ist eine Einwilligung zur Preisgabe personenbezogener Angaben gegen Rabattpunkte oder die kostenlose Nutzung eines Dienstes Ausdruck von Selbstbestimmung? Wann dagegen ist sie Ausdruck der Korrumpierung resp. Manipulation des Willens des Datensubjektes durch ökonomische Anreize? Und weiter gefragt: Wann ist die datenschutzrechtliche Einwilligung Ausdruck der ungenügenden Ausweichmöglichkeiten infolge einer Monopolstellung der Dienstanbieter?[2287] 1755

Hinzu kommt, dass namentlich bei sog. Treueprogrammen mittels elektronischer Kundenkarten den Nutzenden oft gar nicht bewusst ist, dass diese weniger ihre Einkaufstreue honorieren als vielmehr eine Gegenleistung für die gelieferten Personendaten sind. Der Befund beschlägt sowohl die Gültigkeitsvoraussetzung der Informiertheit als auch der Freiwilligkeit. Dasselbe gilt für die vermeintlich unentgeltliche Nutzung von Internet-Diensten, hinter denen in aller Regel eine Tauschsituation steht. Vor diesem Hintergrund ist verständlich, weshalb die Migros ihr Treueprogramm in ihrem Slogan nicht mehr als «Belohnprogramm für Treue» beschreibt. 1756

Radlanski analysiert konkrete Beispiele und Situationen, in denen die Freiwilligkeit der datenschutzrechtlichen Einwilligung an ihre Grenzen kommt. So sei die Einwilligung einer Person zur Verarbeitung ihrer Personenangaben, die auf *Stellensuche* sei, kaum je eine wirklich freiwillige. Eine Person, die sich *medizinisch behandeln* lassen wolle und müsse, werde in Anbetracht dieses für sie höchstrangigen Zieles und Interesses kaum die Einwilligung in eine Datenverarbeitung durch einen Rechnungssteller verweigern, der die Ärztin unterstützt. 1757

2284 Vgl. BGE 138 I 331, E 7.4.1.; BVGer A-3548, Urteil vom 19. März 2019, E 4.7.; mit Fallgruppen und nicht spezifisch datenschutzrechtlich Hass, N 731 ff.; Maurer-Lambrou/Steiner, BSK-DSG, Art. 4 N 16 f.; Rampini, BSK-DSG, Art. 13 N 6 m. w. H.; Rosenthal, HK-DSG, Art. 4 N 95, nach dem eine freie Entscheidung selbst mangels Handlungsalternativen oder trotz Abhängigkeitsverhältnissen angenommen werden könne, sofern eine Einwilligung im subjektiven Interesse der betroffenen Person liege.

2285 Radlanski, 14 ff.

2286 Buchner, 183 ff.; Radlanski, 21.

2287 Vgl. EFD, Bericht 2018, 82 f.

1758 Die Freiwilligkeit der Einwilligung gerät somit in *spezifischen Kontexten unter Druck*, so gerade im Gesundheitsbereich sowie im Arbeitskontext und hier insb. in der Anstellungsphase.[2288]

1759 Spezifisch für das *Beschäftigungsverhältnis* und damit den Anstellungs- resp. Arbeitskontext hat sich eine Debatte rund um die Freiwilligkeit der datenschutzrechtlichen Einwilligung entspannt – die Bewertungen und geforderten Konsequenzen allerdings weisen in divergierende Richtungen: Die Freiwilligkeit wird im *Arbeitsbereich* infolge der *strukturellen Machtungleichheit* zwischen den Akteuren nicht nur von Radlanski als prekär beurteilt.[2289] Die Problematik akzentuiert sich in der Bewerbungssituation.[2290] Werden bestimmte Angaben auf Nachfrage hin verweigert, führt dies regelmässig zu einer Negativinterpretation mit Auswirkungen auf den Erfolg der Stellensuche. Dennoch wird vertreten, dass der äussere Druck in der Beschäftigungssituation resp. im Abhängigkeitsverhältnis rechtlich irrelevant sein soll in Bezug auf die Wirksamkeit der datenschutzrechtlichen Einwilligung.[2291] Einer anderen Ansicht nach sollen die von Gerichten im Arbeitskontext formulierten erhöhten Anforderungen an die Einwilligung auch für die datenschutzrechtliche Einwilligung gelten.[2292] Ein Ansatz, der die Machtasymmetrie als rechtlich einschlägig beurteilt, will nur das Erfragen von Angaben zulassen, die im Zusammenhang mit dem Beschäftigungsverhältnis notwendig seien.[2293]

1760 Letztere Forderung überzeugt. Sie bestätigt eine in dieser Schrift eingeschlagene Entwicklungsrichtung. Entscheidend ist die Frage, wie Flüsse von Personendaten zu gestalten und rechtlich zu strukturieren sind, damit die jeweiligen Ziele und Zwecke verschiedener Kontexte möglichst angemessen erreicht werden können. Damit findet eine enge Anbindung von Verarbeitungsprozessen an die Verarbeitungszwecke sowie die Verhältnismässigkeit im Sinne einer Mittel-Zweck-Relation statt. Ein solches Konzept soll im Zusammenhang mit einer datenschutzrechtlichen Einwilligung berücksichtigt werden. In der intensiv geführten Debatte im sog. Beschäftigtendatenschutz zeigt sich die hohe Relevanz, kontextbezogene Realitäten in die datenschutzrechtlichen Erwägungen zu integrieren. Für den Ar-

2288 Radlanski, 14, 38, 54, 125, 129, 162, 206, 219; zu Rekrutierungsentscheidungen mittels Automatisierungen, sog. Robot Recruiting vgl. Glatthaar, SZW 2020, 43 ff., insb. 48, wo er die Einwilligung in diesem Zusammenhang als dornenreich beschreibt.

2289 M. w. H. Radlanski, 125 ff.

2290 Ders., 4, 22 f.

2291 So Liedke, 38.

2292 Vgl. Radlanski, 126; vgl. den Leitfaden des EDÖB zur Datenbearbeitung im Arbeitsbereich, <https://www.kdsb.ch/documents/Leitfaden_Datenschutz_im_Arbeitsbereich.pdf> (zuletzt besucht am 30. April 2021); vgl. zum Datenschutz im Personalwesen Papa/Pietruszak, in: Passadelis/Rosenthal/Thür (Hrsg.), § 17; Pärli, in: Riemer-Kafka (Hrsg.), 55 ff.

2293 Radlanski, 127; dass die informationelle Selbstbestimmung nur Bestand haben kann in Verhältnissen, in denen die Parteien weitgehend gleichgewichtig sind, früh und allgemein schon Mallmann, 28.

beitskontext zeigt sich die Verdichtung eines bereichsspezifischen Datenschutzrechts, vgl. Art. 328b OR.

Die Einschlägigkeit des Verarbeitungszusammenhanges und des Kontextes für das Datenschutzrecht zeigt sich zudem dergestalt, dass die informierte Einwilligung mit Blick auf den Umgang mit Personendaten vorab bezüglich der im *Gesundheitsbereich und Behandlungskontext* erhobenen Informationen einschlägig ist.[2294] Die im Rahmen einer medizinischen Behandlung erhobenen Informationen werden – zum Schutz des Vertrauensverhältnisses zwischen Ärztin und Patient, das seinerseits die Integrität des Gesundheitsbereichs schützen soll – vom Arztgeheimnis geschützt.[2295] Gleichwohl finden Transfers von ebenda erhobenen Angaben in weitere Bereiche statt, z. B. in den Versicherungsbereich, den Forschungskontext, zum Arbeitgeber und damit in den Beschäftigungskontext, ggf. zu Unternehmen, welche die Fakturierung übernehmen. Eine besondere Rolle zur Bewältigung dieser Informationsflüsse zwischen verschiedenen Kontexten spielen Spezialgesetze wie z. B. das Humanforschungsgesetz. Hier findet sich ein elaboriertes Regime mit einem ausdifferenzierten Einsatz verschiedener Transmissionsprinzipien, wozu auch die informierte Einwilligung gehört.[2296] 1761

Mit der empirisch belegten bescheidenen Funktionstüchtigkeit der informierten Einwilligung als Ausdruck der *Selbstbestimmung* und Autonomie, mit der sie gemeinhin assoziiert wird, befasste sich für das (Bio-)Medizinrecht namentlich Karavas. Der Autor legt weitere Funktionen des auch im Biomedizinrecht bedeutsamen Instruments frei, das nicht nur als Governance-Instrument, sondern zudem als *Kompatibilisierungsinstrument* charakterisiert wird.[2297] 1762

Für diese Arbeit mit ihrer Intention, datenschutzrechtlich – jeglichen jüngsten gesetzgeberischen Neuerungen zum Trotz – eine Neukonzeptionierung für das Datenschutzrecht der Zukunft zu entwickeln, ist an dieser Stelle ein schlichter Befund relevant: Die Auseinandersetzung mit kritischen Thematisierungen der Freiwilligkeit auch datenschutzrechtlicher Einwilligungen ermöglicht es, den Datenschutz und das Datenschutzrecht kontextuell zu lesen: Datenschutz ist nicht isoliert als «Querschnittsthematik» zu sehen. Die Tauglichkeit der Einwilligung mit Fokus auf das Freiwilligkeitserfordernis beurteilt sich *je nach Verarbeitungszusammenhang* unterschiedlich. Weiterführend zeigt sich anhand der informier- 1763

2294 Vgl. Karavas, Körperverfassungsrecht, 227 ff.; Nissenbaum, 171 ff.
2295 Nissenbaum, 171 ff.
2296 Vgl. zum Begriff des Transmissionsprinzips Dies., 145 ff., 192 f., 201 f. und zum Gesundheitskontext 159 f., 171 ff., 187; Karavas, Körperverfassungsrecht, 151 ff.; vgl. zur Transferthematik auch Pärli, in: Riemer-Kafka (Hrsg.), 55 ff., 56 ff.; zum Datenaustausch zwischen Arbeitgeber und Versicherung, den hier erforderlichen Harmonisierungsaufgaben und einschlägigen (Spezial-)Gesetzen vgl. vertiefend ebenso Pärli, 1 ff.
2297 Vgl. Karavas, Körperverfassungsrecht, 193 ff., 222 ff.; vgl. weiter Fateh-Moghadam, BJM 2018, 205 ff.

ten und freiwilligen Einwilligung als eines von mehreren Koordinationsinstrumenten von Datenflüssen in verschiedenen Verarbeitungszusammenhängen neben der kontextuellen resp. akzessorischen Dimension die dynamische Dimension des Datenschutzes und seines Rechts.[2298]

1764 Auch die Gültigkeitsvoraussetzung der *Informiertheit datenschutzrechtlicher Einwilligungen* wird problematisiert. Erneut bezieht sich die Skepsis auf die Voraussetzung in Anbetracht der datenschutzrechtlichen Realitäten. Theoretisch muss die einwilligende Person über sämtliche für die Zustimmung relevanten Informationen verfügen. Radlanski bemerkt hierzu humoristisch:

> «Sollte man diese Voraussetzung wörtlich verstehen, würde dies darauf hinauslaufen, den Betroffenen für manche Einwilligungserklärung speziell ausbilden zu müssen […].»[2299]

1765 Die Informiertheit als Element einer datenschutzrechtlichen Einwilligung wird im Zusammenspiel mit Big Data und OBA von Barocas/Nissenbaum problematisiert. Sie attestieren, dass die Datenverarbeitungsprozesse selbst für die implementierenden Expertinnen und Experten nicht mehr durchschaubar seien. Die Vertrags- und Datennetzwerke seien dermassen verästelt, dass sie nicht mehr nachvollziehbar seien. Zudem würden privacy policies in hoher zeitlicher Frequenz angepasst.[2300] Das Studium von Datenschutzerklärungen würde zum Lebensinhalt und wäre doch nie von Erfolg gekrönt.[2301] Barocas/Nissenbaum führen insofern das «Transparenz-Paradoxon» ein: Sind privacy policies hinreichend detailliert, dokumentieren sie ansatzweise den Datenverarbeitungsprozess. Für die meisten Menschen werden sie damit unverständlich.[2302] Diesem Befund Rechnung tragend, bleiben viele Dokumente, um nachvollziehbar zu bleiben, unpräzise. Damit bilden sie keine Basis für eine informierte Einwilligung. Umgekehrt werden detailreiche und seitenlange privacy policies kaum gelesen. Insofern spielt die Kollision zwischen verschiedenen Interessen eine Rolle: Wer online ein Hotel buchen will, möchte ein Hotel buchen und nicht Minuten oder Stunden damit zubringen, Datenschutzdokumente zu studieren und Datenschutzerklärungen anzuklicken.

1766 Auch in diesem Zusammenhang wird versucht, Lösungen zu entwickeln: Insofern sind der sog. layered consent zu erwähnen oder auch grafische Darstellungen resp. Visualisierungen von Verarbeitungsprozessen.[2303] Gleichwohl bleibt die

2298 Zur Ausarbeitung eines Rechts auf informationellen Systemschutz dritter Teil, IX. Kapitel.
2299 Radlanski, 16.
2300 Zu Änderungen der AGB von sozialen Plattformen im Internet vgl. auch Baeriswyl, digma 2010, 56 ff., 57 f.
2301 Zum Ganzen im Zusammenhang mit Big Data Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 45, 49, 56 ff., insb. 59 f.; im Zusammenhang mit OBA Dies., 1 ff., 4 f.
2302 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 58 f.
2303 Vgl. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/> (zuletzt besucht am 30. April 2021).

Informiertheit der Einwilligenden in Anbetracht der Komplexität heutiger Datenverarbeitungsprozesse gerade im Internet über weite Strecken unerreichbar.

Die informierte Einwilligung, die als Ausdruck von Autonomie resp. Selbstbestimmung oder als ein Recht an eigenen Daten sowie als Hauptstrategie zur Bewältigung datenschutzrechtlicher Probleme taxiert wird, weist somit in der Realität erhebliche Schwächen auf.[2304] Die kritischen Erkenntnisse zum informed consent als datenschutzrechtliche Lösungsstrategie sind für die Diskussionen in der Schweiz von hohem Interesse. Auch hierzulande rückt das Recht an eigenen Daten in das Zentrum der Aufmerksamkeit. Der Erfolg dieses Instruments scheint indes primär theoretischer Natur. Damit kann sich ein Datenschutzrecht, das faktische Wirksamkeit erzielen will und keine reine Existenz auf dem Papier fristen will, nicht begnügen. 1767

Wenn die rechtliche Stärkung des Bandes zwischen Datensubjekt und Personendaten zur Lösung datenschutzrechtlicher Probleme faktisch nicht die gewünschten Effekte bringt, liegt eine *Gegenstrategie* nahe: die *Anonymisierung*. Wie die informierte Einwilligung nimmt die Anonymisierung eine prominente Rolle im Rahmen datenschutzrechtlicher Lösungsinstrumente ein: 1768

> «Anonymity and informed consent emerged as panaceas because they presented ways to 'have it all'; they would open the data floodgates while ensuring that no one was unexpectedly swept up or away by the deluge. Now, as then, conscientious industry practitioners, policymakers, advocates, and researchers across the disciplines look to anonymity and informed consent as counters to the worrisome aspects of emerging applications of big data. We can see why anonymity and consent are attractive: anonymization seems to take data outside the scope of privacy, as it n longer maps onto identifiable subjects, while allowing information subject to give or withhold consent maps onto the dominant conception of privacy as control over information about oneself. In practice, however, anonymity and consent have proven elusive, as time and again critics have revealed fundamental problems in implementing both.»[2305]

5.3. Das Anonymisierungsparadigma als Gegenstrategie

Bei der Anonymisierung wird quasi der für das Datenschutzrecht charakteristische Personenbezug der Angabe aufgelöst resp. die Identifizierbarkeit aufgehoben.[2306] Oft ist eine Verarbeitung von Informationen auch ohne die semantische Dimension und damit ohne Bewahrung des Personenbezuges der Angaben sinn- 1769

2304 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 56 ff.; zu den Herausforderungen des Lösungsansatzes in Anbetracht der datenschutzrechtlichen Realitäten Radlanski, 1 ff.; m. w. H. auch Heuberger, N 285, N 320, N 345.

2305 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 45.

2306 Dies., a. a. O., 4; vgl. auch Isler, Jusletter vom 4. Dezember 2017, N 3; zu den Begriffen der Personendaten, der Identifizierbarkeit, aber auch der Anonymisierung z. B. Probst, AJP 2013, 1423 ff. mit Analyse zweier Beispiele, der Sozialversicherungsnummer sowie IP-Adressen.

voll möglich. Um die Anwendbarkeit des Datenschutzrechts zu exkludieren, erfolgt eine Anonymisierung.[2307] Die Anonymisierung, die regelmässig unter Einsatz entsprechender Technologien bewerkstelligt wird, zielt darauf ab, die Identifizierung einer Person zu verunmöglichen oder so zu erschweren, dass eine Re-Identifikation nicht mehr oder nur mit unverhältnismässig hohem Aufwand denkbar ist.[2308]

1770 In der DSGVO wird das Instrument weder explizit verlangt noch legaldefiniert. Gleichwohl kann die Anonymisierung der Gewährleistung datenschutzrechtlicher Grundsätze Rechnung tragen – so dem Verhältnismässigkeitsgrundsatz. Thematisiert wird die Anonymisierung insb. in ErwG 26. Art. 6 Abs. 4 nDSG verlangt, dass Personendaten vernichtet oder anonymisiert werden, sobald sie zum Zweck ihrer Verarbeitung nicht mehr erforderlich sind.[2309] Auch Art. 31 Abs. 2 lit. e nDSG sieht das Instrument vor.

1771 Weil die Anonymisierung oft mittels spezifischer Technologien bewerkstelligt wird, ist sie ein gutes Beispiel für die Gewährleistung des Rechts durch die Technologie selbst. Technologien sind mit anderen Worten zugleich beides: eine Bedrohung und eine Garantie für den Datenschutz. Das mag auf den ersten Blick paradox klingen. Das Phänomen ist im Medizinkontext und hier insb. in der Homöopathie aber bekannt. Es lautet: Gleiches mit Gleichem behandeln. Und dieses Prinzip kann sich das Datenschutzrecht zunutze machen, indem es die mannigfaltigen Bedrohungen, welche aus den Informationstechnologien resultieren, mittels Informationstechnologien adressiert und zu bewältigen sucht. Anonymisierungstechnologien sind in diesem Zusammenhang relevant.

1772 Von wissenschaftlicher und politischer Seite her wird indes ebenso dieses Instrument zusehends kritisch betrachtet. Problematisiert wird vorab, dass die Anonymisierung kaum je so robust erfolge, dass diese «absolut» sei. Eine Re-Identifizierung bleibe trotz des technologischen Fortschrittes oft möglich.[2310] Der Kritikpunkt bezieht sich damit erneut auf Defizite der (ungenügenden) Wirksamkeit eines zugleich rechtlichen sowie technologischen Instruments im Lichte der Realitäten und der Potenzen von Informationsverarbeitungstechnologien.

2307 Vgl. Ziebarth m. w. H., NomosKomm-DSGVO, Art. 4 Nr. 1 N 24 ff.; Klar, BeckKomm-DSGVO, Art. 4 Nr. 1 N 31 ff.

2308 M. w. H. Heuberger, N 119 ff. und N 393 ff.

2309 Zur Anonymisierung auch Botschaft zur Teilrevision des DSG BBl 2017–1084, 17.059, 6941 ff., 7019; WP 29, Anonymisation; Blechta, BSK-DSG, Art. 3 N 13; vgl. Waidner/Karjoth, digma 2004, 18 ff.

2310 Vgl. Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 50; vgl. zur Re-Identifikation auch Heuberger, N 128 ff.; vgl. Waidner/Karjoth, digma 2004, 18 ff.; zur Frage, ob und wann überhaupt ein Personenbezug besteht, zur Anonymisierung sowie hohen Wahrscheinlichkeit der Re-Identifizierung bei Big Data vgl. auch Cichocki, Jusletter IT vom 21. Mai 2015, N 13 ff.

Die Anonymisierung wird sodann als ungeeignetes Instrument im Zusammenhang mit Big Data und/oder dem (Online-)Tracking und Targeting taxiert: Anonymisierung verstanden als «Namenlosigkeit» greife zu kurz, um gerade auch *ethischen Bedenken* bezüglich Big Data wirkungsvoll zu berücksichtigen.[2311] Im Zentrum der Kritik steht der Begriff der *Reachability*, der Erreichbarkeit: Eine Person kann keineswegs bloss aufgrund ihres Namens und ihrer Adresse «identifiziert» werden. Vielmehr gibt es gerade im Online-Bereich Möglichkeiten, gewisse Angaben und Verhaltensweisen jemandem zuzuordnen, ohne zwingend den Namen und die Adresse kennen zu müssen. Der Name mag das klassische Beispiel für einen Identifikator sein, er ist aber heute keineswegs der einzige. Er ist nicht zwingend notwendig, um eine Person adressieren oder angehen zu können. Es gibt Identifikatoren, anhand derer auf konkrete Personen «zugegriffen» werden kann. Eine «bestimmte» Person kann resp. muss weiterhin mit Konsequenzen resp. mehr oder minder attraktiven Angeboten usf. rechnen, weil sie ebenso anderweitig angesprochen werden kann. Ihr Verhalten bleibt weder unbeobachtet noch folgenlos. Der Wert resp. das Ziel der Anonymisierung wird unterminiert.[2312] Selbst anonym erfolgende Datenverarbeitungen können zu diskriminierenden oder manipulierenden Effekten führen, was spezifisch für das Profiling beschrieben wird.[2313] Gerade eine rein «formelle» Anonymisierung im Sinne eines «Pixelns» des Namens vermag die «materielle» Anonymisierung in Zeiten von Big Data, wo Datenbestände beliebig abgeglichen werden können, nicht zu gewährleisten. Zudem können aufgrund von Big Data Rückschlüsse auf und für Individuen gezogen werden, ohne dass über diese identifizierende Angaben vorliegen.[2314] 1773

Damit sind gleichermassen für die Strategie der Anonymisierung Schwachpunkte anerkannt. Sie beschränken sich nicht auf die Funktionstüchtigkeit in Anbetracht der Potenzen der Informationstechnologien. Sie sind konzeptioneller Natur. 1774

6. Resümee

Während in diesem VIII. Kapitel unter dem Titel der aktuellen Lösungsansätze unter A. die *datenschutzrechtlichen Entwicklungstrends in den jüngsten Gesetzesneuerungen* beschrieben wurden, folgten unter B. die vonseiten der *Rechtswissenschaften diskutierten Lösungsansätze*. Die wichtigsten der rechtswissenschaftlich verhandelten Lösungskonzepte wurden anhand von *Paradigmen* beschrieben. 1775

2311 Nissenbaum, 51.
2312 Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff., 49 ff., insb. 51.
2313 Vgl. die Beiträge von Barocas/Nissenbaum; m. w. H. Heuberger, N 135 auch mit Hinweis auf den sog. Mosaikeffekt N 6 ff. und N 130 ff.
2314 Nissenbaum, 55.

1776 In den (privat-)rechtswissenschaftlichen Beiträgen, die sich mit den Herausforderungen der Informationstechnologien und dem Datenschutz befassen, steht das *subjektive Recht als Anknüpfungspunkt im Zentrum*. In Einklang mit dem aktuellen Zivilrecht – wie es für die analoge Welt geschaffen wurde – nehmen die datenschutzrechtlichen Diskussionen das Persönlichkeitsrecht einerseits, das Eigentumsrecht andererseits zu ihrem Bezugspunkt.

1777 Dogmatisch wird ein weites Spektrum diskutiert: Den Ausgangspunkt bildet weiterhin das *Persönlichkeitsparadigma* in Gestalt eines *abwehrrechtlich gedachten Missbrauchs- resp. Integritätskonzepts*.[2315] Allerdings wird zusehends ein *Herrschaftsrecht* von Datensubjekten an Personendaten verhandelt, was dem steigenden ökonomischen Wert von Informationen, Daten und damit auch Personendaten geschuldet ist. Rechtswissenschaftlich werden *zwei Hauptkonstruktionen* präsentiert: zum einen das *persönlichkeitsrechtlich basierte, duale Selbstbestimmungsrecht*, das zugleich eine *vermögensrechtliche Komponente aufweist* und sich damit dem Vorbild des Urheberrechts annähert, und zum anderen ein *Eigentum an Personendaten* durch das Datensubjekt.

1778 Gezeigt wurde, inwiefern in der rechtswissenschaftlichen Debatte *Zuordnungsfragen* von Daten und Personendaten an Bedeutung gewonnen haben. Während mit Sachdaten Angaben in ihrer syntaktischen und strukturellen Dimension angesprochen werden, geht es bei Personendaten um Daten in ihrer semantischen Dimension. Mit der intensivierten Diskussion rund um die Zuordnungsfragen verbunden steht eine Abkehr von einer deliktsrechtlichen, abwehrrechtlichen Konzeptionierung des Datenschutzrechts zur Debatte. Während ein Missbrauchs- resp. Integritätskonzept den informationellen Konflikt prinzipiell zugunsten der Verarbeitenden entscheidet, gilt etwas anderes für die diskutierten Rechte an eigenen Daten.

1779 Sobald mit einer (wie auch immer gearteten) Position dem Datensubjekt die Kontrolle resp. Herrschaftsbefugnisse an seinen Personendaten verbürgt werden sollen, gelangen *Einwilligungskonstruktionen* von der Peripherie in das Zentrum der datenschutzrechtlichen Thematisierung.

1780 Die *informierte Einwilligung*, die untrennbar mit einem Recht an eigenen Daten resp. einem Kontrollrecht des Subjektes assoziiert wird (sei es in Gestalt eines

2315 Die Habilitationsschrift von Aebi-Müller blieb mit Fokus auf den Umgang mit Personendaten im privaten Bereich lange Monografie im wahrsten Sinne des Wortes. Die Autorin richtete ihre Analyse allerdings auf den Umgang mit Personendaten im System des zivilrechtlichen Persönlichkeitsschutzes und damit Art. 28 ff. ZGB aus, wohingegen das DSG eher am Rande zur Sprache kommt. Die Autorin ging insofern davon aus, dass ein Recht auf informationelle Selbstbestimmung, wie es das DSG anerkenne, zu weit gehe. Das von ihr vorgeschlagene Konzept des Schutzes einer informationellen Privatheit, welches auf die Studien der Philosophin Rössler referiert, bleibt stark dem defensivrechtlichen Charakter und einer ideellen Natur mit seiner Ausrichtung an Art. 28 ZGB verpflichtet.

persönlichkeitsrechtlich oder eigentumsrechtlich angeknüpften Rechts), ist im Bereich des Technologierechts resp. Technikrechts zu einem zentralen Lösungselement avanciert.[2316]

Solche Ansätze wollen gerade auch Wirksamkeitsdefizite eines abwehrrechtlich gedachten Privatsphärenschutzes beseitigen sowie die Autonomie und Selbstbestimmung des Menschen gewährleisten. Damit wird symbolhaft dem Bild, wonach die neuen Technologien den Menschen, das Subjekt, zum Objekt degradieren, etwas entgegengesetzt. Kognitiv sind Herrschaftsrechte an Daten – in Analogie zu Konzepten des Zivilrechts der analogen Welt – geprägt von Kategorien des Subjekts und des Objekts, wobei dem Datensubjekt (resp. den Verarbeitenden) Personendaten als Quasi-Objekte zugewiesen werden. 1781

Für ein *Recht an eigenen Personendaten* und die Anerkennung eines Rechts auf informationelle Selbstbestimmung im Privatrecht hat *de lege ferenda* namentlich Buchner plädiert. Er fordert ein persönlichkeitsrechtlich basiertes Recht der informationellen Selbstbestimmung für den privaten Bereich. Trotz einer *persönlichkeitsrechtlichen Anknüpfung* integriert sein Konzept die ideelle wie ökonomische Komponente, womit es sich dem Urheberrecht annähert. Seine Forderung zielt auf eine konsequente Ausrichtung des Datenschutzrechts für den privaten Bereich an einem privatautonomen Ausgleich. 1782

Im Anschluss an die Betrachtung zweier Hauptkonzepte innerhalb des Persönlichkeitsparadigmas – deliktsrechtliches Abwehrkonzept in Gestalt eines Schutzes informationeller Privatheit, informationelle Selbstbestimmung in Gestalt eines Rechts an eigenen Daten – wurde die *Nomenklatur für einen juristischen Informationsbegriff mit der Trias von syntaktischen, semantischen und strukturellen Informationen* gemäss Zech vorgestellt. Der Autor präsentiert ein an diese Kategorisierung anknüpfendes, ausdifferenziertes Zuweisungsregime. Ein allgemeines Recht auf informationelle Selbstbestimmung in Gestalt und mit Gehalt eines Rechts an eigenen Personendaten (semantische Dimension) hält Zech für nicht angezeigt.[2317] Vielmehr plädiert er bezüglich Personendaten für einen Integritätsschutz. 1783

Die Diskussion von *Herrschaftsbefugnissen des Datensubjekts an seinen Daten de lege ferenda* hat jüngst auch die Privatrechtswissenschaft der Schweiz erreicht, wobei die Diskussion oft unter dem Titel eines *Eigentums an Personendaten* geführt wird. In diesen neueren Beiträgen erfolgt eine Klarstellung zum geltenden Recht: Die Qualifizierung des Regimes gemäss DSG für den privaten Bereich als 1784

2316 Nissenbaum, 70, mit Hinweis auf eine Definition der privacy durch Westin: «the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information about them is communicated to others».

2317 Zech, 227 ff.

eines der informationellen Selbstbestimmung vermöge nicht zu überzeugen.[2318] Für eine Anerkennung eines Rechts an eigenen Daten resp. eines Rechts auf informationelle Selbstbestimmung oder eines Eigentums an Personendaten, so der herrschende Tenor, sei es zu früh. Notwendig seien vertiefende Studien.

1785 Nachgewiesen wurden somit neben der defensiv- und abwehrrechtlichen Konstruktion eines im Persönlichkeitsrecht basierenden Datenschutzrechts ein im Persönlichkeitsrecht verankertes Recht auf informationelle Selbstbestimmung mit oder ohne Integration von Verwertungsbefugnissen hin zu eigentumsrechtlichen Ansätzen. *Alle Lösungsansätze* kreisen um die Frage der *Stärkung der Rechtsposition der Datensubjekte*.

1786 Die Vorschläge zur Neugestaltung des Datenschutzrechts liessen sich mit dem Fokus auf die Rechtsposition des Datensubjektes anhand eines *abgestuften Systems* beschreiben. Die stärkste Rechtsposition hätte das Datensubjekt in einem Konzept, das ein Recht an eigenen Daten anerkennt, das persönlichkeitsrechtliche wie wirtschaftliche Komponenten integriert. Hier hätte das Datensubjekt ein eigentliches Vorentscheidungsrecht. Je nachdem, wie die Schranken gestaltet werden, würde dieses mehr oder minder stark beschnitten werden. Namentlich der Verzicht auf generalklauselartige überwiegende Interessen würde ein so gestaltetes Recht an eigenen Daten effektuieren. Die schwächste Position kommt dem Datensubjekt in einem abwehrrechtlich konzipierten Integritätsschutz resp. einer Missbrauchsgesetzgebung zu. Die schweizerische Rechtslehre bewertet die Konzepte unterschiedlich.

1787 Obschon zur gebotenen Anerkennung eines Rechts an eigenen Personendaten – sei es persönlichkeitsrechtlich, sei es eigentumsrechtlich begründet – Unschlüssigkeit herrscht, zeigt sich: Es sind die Einräumung von Herrschaftsbefugnissen des Datensubjektes an Personendaten und damit die Einwilligungskonstruktionen, die den grossen Teil der rechtswissenschaftlichen Aufmerksamkeit absorbieren. Das Recht an eigenen Daten wird damit auch in der Schweiz als Hauptstrategie zur Lösung datenschutzrechtlicher Herausforderungen debattiert.[2319]

1788 Folglich drängte sich eine Betrachtung der jüngst zusehends kritischen Reflexionen bezüglich einer pauschalen Stärkung der informationellen Selbstbestimmung resp. eines Rechts an eigenen Daten mit der damit verbundenen Aufwertung von Transparenz- und Zustimmungserfordernissen auf. Der Kurzabriss leistete einen

2318 Als *appellation trompeuse* bezeichnet von Flückiger, PJA 2013, 837 ff., 856 f.; Belser, in: Epiney/Fasnacht/Blaser (Hrsg.), 19 ff.; auf Missverständlichkeiten hinweisend Meier, N 15 ff.; kritisch sodann Gächter/Egli, Jusletter vom 6. September 2010, N 19 ff.; vgl. jüngst auch zu den Diskussionen *de lege ferenda* zur Abkehr vom Missbrauchsschutz und hin zur Verbürgung eines Rechts auf informationelle Selbstbestimmung Schmid/Schmidt/Zech, sic! 2018, 627 ff., 637 ff.

2319 Dies entspricht den Tendenzen in den USA, vgl. Solove, Stan. L. Rev. 2001, 1393 ff., 1445 ff., allerdings kritisch zu diesem Paradigma.

Beitrag dazu, die für die Schweiz attestierten Erkenntnislücken zu verringern. Weil entsprechende Analysen nicht bloss dekonstruierend sind, stattdessen Impulse für die Weiterentwicklung datenschutzrechtlicher Konzepte liefern, wurde mit ihrer Betrachtung gleichzeitig eine Brücke zum neunten und letzten Kapitel dieser Schrift konstruiert. Gezeigt wurde, dass die *datenschutzrechtliche Einwilligung* zunächst in Bezug auf ihre Tauglichkeit innerhalb der datenschutzrechtlichen Realitäten kritisch beleuchtet wird. Zugleich gibt es theoretisch-konzeptionelle Bedenken.

Die Aufmerksamkeit richtete sich auf den *ersten Kritikpunkt:* Demgemäss wird 1789
das Konzept der informierten Einwilligung in der Realität von erheblichen *Informations- wie Freiwilligkeitsdefiziten* belastet.[2320] Weil die Informiertheit und die Freiwilligkeit der datenschutzrechtlichen Einwilligung *faktisch* oft nicht erfüllt werden (können), wird von einer *Utopie der freien und informierten Einwilligung oder der kühnsten Zustimmungsfiktion* gesprochen. In kafkaesker Manier würde gerade im Online-Bereich und den ebenda beschriebenen netzwerkartigen Geschäftsstrukturen sowie Technologien das Studium einschlägiger und ständig variierender privacy policies zum Lebensinhalt der meisten Menschen, ohne dass sie diese jemals verstehen könnten. Weiter wurden Verarbeitungssituationen beschrieben, in denen nicht von der Freiwilligkeit der Einwilligung ausgegangen werden kann. Das Datensubjekt findet sich nicht selten in dilemmatischen oder aussichtslosen Situationen wieder: Es möchte ein bestimmtes Ziel erreichen oder ein bestimmtes Interesse verfolgen, beispielsweise eine Stelle erhalten, online Waren bestellen oder digital Beziehungen pflegen, Zeitung lesen etc. Besagte Interessen kollidieren regelmässig mit dem Datenschutz resp. den Vorgaben in Konstruktionen der informierten Einwilligung. Zur Bewältigung des Konfliktes erteilt das Datensubjekt meist eine «Pseudo-Einwilligung» in die Datenverarbeitung, um das, was es *primär* wollte, realisieren zu können. Die Einwilligungserklärung verkommt damit zu einer rein formalistischen Legitimation und entbehrt im Kern der Sinnhaftigkeit. Der *zweite Kritikpunkt an den Einwilligungskonstruktionen* verdichtet sich zu der These, wonach ein pauschales Recht an eigenen Daten dem Datenschutz nicht zu-, stattdessen abträglich ist. Die Überlegungen insofern wurden in diesem Kapitel kurz gehalten, zumal im letzten Kapitel mit dem dort gemachten Rekonzeptionalisierungsvorschlag eine integrative Auseinandersetzung mit dieser Thematik stattfindet. Es wird von Interesse sein, dass benannte Defizite an einem Recht an eigenen Daten, der informationellen Selbstbestimmung und damit der datenschutzrechtlichen informierten Einwilligung nicht per se zu ihrer Ablehnung als datenschutzrechtlicher Strategie führen. Das

2320 Der Tragfähigkeit der informierten und freiwilligen Einwilligung widmet Radlanski seine Studie; sodann wird diese vertieft beleuchtet z. B. von Barocas/Nissenbaum, in: Lane/Stodden/Bender/Nissenbaum (ed.), 44 ff.

Instrument wird einzig als hegemonialer Lösungsansatz verworfen. Im Gegenzug wird vorgeschlagen, die informierte Einwilligung – neben anderen Instrumenten – *differenziert* einzusetzen. Die Gestaltung eines ausdifferenzierten Regimes soll dabei stets von den jeweils einschlägigen Lebens- und Rechtsbereichen abhängig gemacht werden.[2321]

1790 Abgerundet wurde der Überblick über die wissenschaftlichen Diskussionen mit dem *Anonymisierungsparadigma*. Es wird ebenso als effizientes Rezept zur Linderung datenschutzrechtlicher Probleme gesehen und lässt sich als Gegenstrategie oder Antithese zur informierten Einwilligung beschreiben: Bei der ersten rechtswissenschaftlich intensiv diskutierten Lösungsstrategie – dem Recht an eigenen Daten (sei es in Gestalt des Persönlichkeitsrechts, sei es in Gestalt des Eigentumsrechts) mit Einwilligungskonstruktion – geht es um die *Stärkung des Bandes zwischen Datensubjekt und Personendaten*. In die entgegengesetzte Richtung weist die *Anonymisierung als zweiter Bewältigungsansatz*, wobei es um die *Auflösung des Bandes zwischen Daten und Person geht*. Der Personenbezug soll in robuster Weise gekappt werden. Um dies zu bewerkstelligen, werden technologische Prozesse und Kapazitäten genutzt, namentlich Anonymisierungstechniken. Zwar gilt der *Anonymisierungsansatz* als vielversprechend, doch auch er sieht sich *kritischen Einschätzungen* ausgesetzt. Die Einwände lassen sich – parallel zur Kategorisierung der Einwände gegenüber dem Ansatz der informierten Einwilligung – in *faktizitätsbezogene einerseits, theoretische Einwände andererseits* einteilen. In der Realität betrachtet zeigt sich, dass die Anonymisierung kaum je so robust ist, dass sie nicht rückgängig gemacht werden könnte. In theoretischer Hinsicht wird attestiert, dass trotz Anonymisierung negative Effekte bestehen bleiben. Die Aufhebung des Personenbezuges eliminiert weder die Identifizierbarkeit resp. die Adressbarkeit noch nachteilige Effekte für die Datensubjekte.

1791 Die Auseinandersetzung mit den rechtswissenschaftlichen Lösungsansätzen drängte die Frage in den Vordergrund, ob der Schlüssel zur Lösung der datenschutzrechtlichen Herausforderungen nicht in einer zivilrechtsdogmatischen Debatte bezüglich der Anerkennung eines persönlichkeits- oder eigentumsrechtlich geprägten subjektiven Rechts an eigenen Daten liegt.

1792 Dass die vorliegende Studie sich darauf beschränkte, in grober Weise zwei Basiskonstruktionen in Analogie zum Recht der subjektiven Rechte des ZGB und damit dem Persönlichkeitsrecht und dem Eigentumsrecht vorzustellen, auf eine

2321 Grundlegend Nissenbaum, *passim*; Radlanski, 209 ff., plädiert dafür, ein Gleichrangigkeitsverhältnis der Legitimationsgründe aufzubrechen. Die Einwilligung könne keine Grundregel des allgemeinen Datenschutzrechts sein; vielmehr bedürfe es anderer Grundregeln, die gesetzlich verankert werden, und nur wenn diese nicht greifen, soll die Einwilligung greifen. Umgekehrt seien Bereiche abzustecken, in denen nur die Einwilligung den Datenumgang legitimieren könne; zu einem Recht auf informationellen Systemschutz sogleich dritter Teil, IX. Kapitel.

Darstellung der unzähligen dogmatischen Raffinessen und Ausdifferenzierungen dagegen verzichtet wurde, ist nunmehr, da in das letzte Kapitel übergeleitet wird, nachvollziehbar: Diese Schrift plädiert dafür, den Schlüssel für ein in Zukunft wirksames Datenschutzrecht nicht im Lichtkegel der subjektiven Rechte zu suchen, sondern stattdessen den Blick zu weiten.

1793 Die jüngsten datenschutzrechtlichen Entwicklungen zeigen, dass Lösungen nicht isoliert in einer Umlagerung von individualrechtlichen Positionen verortet werden. Vielmehr werden neue Ansätze wie der Compliance- und Risiko-Ansatz eingefügt. Sie ergänzen die tragende Säule des Subjektschutzes um zusätzliche tragende Säulen. Sodann haben die jüngsten wissenschaftlichen Erkenntnisse kritische Einschätzungen zu aktuellen Lösungsansätzen – namentlich dem informed consent – angebracht. Die Strategie, wonach das Datenschutzrecht seine Probleme durch das Patentrezept eines Rechts an eigenen Daten des Datensubjektes lösen kann, gilt als nur beschränkt tragfähig.

1794 Ein Denken «out of the box» ist gefragt, gerade für ein Rechtsgebiet, das sich mit neuen Technologien zu befassen hat. Die traditionellen Konzepte des Zivilrechts der analogen Welt vermögen isoliert, im Alleingang und ohne Anpassung an die neuen Realitäten gerade auch in Anbetracht der Digitalisierung keine überzeugenden Lösungsansätze zu generieren. Dass die Suche nach Lösungskonzepten ausserhalb vertrauter Kategorien oder naheliegender Felder produktiv sein kann, bestätigen zwei für die Rechtswissenschaft inspirierende Beispiele aus der Geologie sowie der Geophysik: Jüngere Untersuchungen zur Stranderosion, die mit dem Klimawandel einhergeht, deuten darauf hin, dass die naheliegenden und etablierten Massnahmen – die Schutzbauwerke – eher schädlich zu sein scheinen. Auch im Bereich der Wasser-Retentionsmassnahmen werden neue Konzepte entwickelt. So kann z. B. durch die Nutzung anderer Bewirtschaftungsformen von Feldern Regenwasser besser vom Boden absorbiert und dann langsam abgegeben werden.[2322] Die Beispiele sind nicht zufällig gewählt – denn die Bilder von Flüssen und Feldern, von Schutzwällen, von Übertritten und Erosion, von Fokuswechsel und Neukonstruktion sind prädestiniert, um in das letzte Kapitel dieser Studie überzuleiten.

1795 Im nun folgenden IX. und letzten Kapitel geht es darum, für den Datenschutz und das Datenschutzrecht einen *Perspektivenwechsel* zu vollziehen. Denn subjektive Rechte an Daten, ein Recht an eigenen Personendaten – ungeachtet der Frage, ob in Gestalt eines Eigentumsrechts oder eines Rechts auf informationelle

2322 Vgl. Rubin, Causes and Effects on Beach Erosion, abrufbar unter: <https://www.soest.hawaii.edu/GG/ASK/beacherosion.html> (zuletzt besucht am 30. April 2021); Natural water retention measures – Environment – vgl. European Commission zu natural water retention measures, abrufbar unter: <https://ec.europa.eu/environment/water/adaptation/ecosystemstorage.htm> (zuletzt besucht am 30. April 2021).

Selbstbestimmung mit Kommerzialisierungserlaubnis – sowie Anonymisierungsbestrebungen greifen zu kurz. Allem voran kann eine Umlagerung des Datenschutzrechts von einem subjektiven Recht, dem Persönlichkeitsrecht (selbst in seiner Emanzipation von einem Abwehrrecht zu einem Selbstbestimmungsrecht), zu einem anderen subjektiven Recht, dem Eigentumsrecht, die facettenreichen und komplexen Probleme des zeitaktuellen Datenschutzrechts nicht lösen. Vielmehr drängt sich eine neue Sichtweise und Anknüpfung auf.

IX. Kapitel: Das Recht auf informationellen Systemschutz

> «Context is crucial to privacy, not only as a passive backdrop against which the interests of affected parties are measured, balanced, and traded off; rather, it contributes independent, substantive landmarks for how to take these interests and values into account. It makes the integrity of the contexts themselves the arbiter of privacy practices – vibrant marketplace, effective healthcare, sound education, truly democratic governance, and strong, trusting families and friendships.»[2323]

A. Impulse für eine erweiterte Perspektive

Schon früh wurde von wissenschaftlicher Seite davor gewarnt, die Relevanz der sozialen Konflikte hinter einer verengten Fokussierung auf den Computer als Sündenbock resp. das Persönlichkeitsrecht als Bezugspunkt des Datenschutzrechts zu übersehen.[2324] Ein Recht auf informationellen Systemschutz ist kein *Deus ex machina*. Systemrelative Aspekte sind seit jeher in verschiedenen Textquellen – ebenso im geltenden Recht – angelegt, wie an zahlreichen Stellen dieser Studie sichtbar gemacht wurde. 1796

Der zweite Teil dieser Arbeit zeigte, dass das schweizerische DSG auf drei Strukturmerkmalen beruht: Dualismus, generalklauselartiges Regime und persönlichkeitsrechtliche Anknüpfung. An diesen hält die Totalrevision fest. Allerdings fügt sie diesen drei Strukturmerkmalen weitere Ansätze hinzu, womit erstere neu eingebettet werden. Die Totalrevision begnügt sich folglich nicht damit, die individualrechtliche Anknüpfung und Rechtsposition der Betroffenen auszubauen. Vielmehr verleihen insb. der Governance-Ansatz, der Ansatz der faktischen Verwirklichung und der Risiko-Ansatz dem Datenschutzrecht neue Charakterzüge, ohne dass die früh angelegten Charakteristika aufgegeben werden. Für dieses letzte Kapitel liefern die drei von Anfang an angelegten Strukturmerkmale Referenzpunkte. *Pro memoria:* 1797

Der im IV. Kapitel des zweiten Teils analysierte *Dualismus* implementiert eine *pointierte Ausdifferenzierung* der datenschutzrechtlichen Vorgaben für den *privaten gegenüber dem öffentlichen Bereich*. Hierbei ist der entgegengesetzte Ausgangspunkt – prinzipielles Verarbeitungsverbot mit Erlaubnistatbeständen für den öffentlichen Bereich, grundsätzliche Verarbeitungsfreiheit mit Schranken für den privaten Bereich – richtungsweisend. Für die Ordnung des privaten Bereiches, die mangels Widerspruchs oder Weitergabe von besonders schutzwürdigen 1798

2323 Nissenbaum, Sci. Eng. Ethics 2018, 831 ff., 849.

2324 Fiedler, in: Podlech/Steinmüller (Hrsg.), 179 ff., 193, auch zum Antagonismus zwischen Technologie und Persönlichkeitsrecht Simitis, NomosKomm-BDSG, Einleitung: Geschichte – Ziele – Prinzipien, N 2 und N 26.

Angaben oder Persönlichkeitsprofilen an Dritte greift, wurde die Qualifizierung als *Integritätsschutz* vorgeschlagen. Anders das monistische Modell der DSGVO, das für die Personendatenverarbeitung durch private wie öffentliche Verantwortliche das generelle Verarbeitungsverbot mit Erlaubnistatbeständen vorsieht und auch ansonsten einheitliche Vorgaben an die Personendatenverarbeitung durch die Akteure formuliert. Indem die Schweiz die Differenzierungswürdigkeit der datenschutzrechtlichen Vorgaben für den öffentlichen und den privaten Bereich umsetzt, anerkennt sie – in grober Weise – einen *systemischen Ansatz*. In diesem Ansatz wird die Situation von Personendatenverarbeitungen je nach Akteur und Kontext – öffentlich versus privat – als datenschutzrechtlich einschlägig anerkannt.

1799 Es folgte im V. Kapitel des zweiten Teils ein Blick auf die *generalklauselartigen Bearbeitungsgrundsätze*, die in jene beiden divergierenden Ansätze eingebettet sind. Sie bilden bis heute das materiellrechtliche Kernstück des Datenschutzes. Es wurden die wichtigsten Entwicklungen nachgezeichnet sowie Konturierungsvorschläge präsentiert. Von zentraler Bedeutung zeigte sich die Analyse zum *Zweckbindungsgrundsatz*, der auch in der Argumentation des Volkszählungsurteils des Bundesverfassungsgerichts eine bedeutsame Rolle einnimmt. Ebenda wurde herausgearbeitet, dass datenschutzrechtliche Vorgaben keineswegs nur das Individuum und ein Recht auf informationelle Selbstbestimmung schützen. Vielmehr sollen sie die Funktionstüchtigkeit der statistischen Erhebung selbst gewährleisten. Kein Verarbeitungsgrundsatz macht die Relevanz *systemischer Erwägungen* für das Datenschutzrecht so deutlich wie der Zweckbindungsgrundsatz. Im Volkszählungsurteil wird auf die Bedeutung des Statistikgeheimnisses und die Notwendigkeit, dass zum Zweck der Volkszählung erhobene Angaben nicht zu anderen Massnahmen des Verwaltungsvollzuges eingesetzt werden dürfen, hingewiesen. Ein Kernargument lautet, dass die korrekte Beantwortung der Fragen durch die Bürgerinnen und Bürger nur durch das Vertrauen, dass die erteilten Personenangaben nicht in anderen Verarbeitungszusammenhängen des Verwaltungsvollzuges (Migration, Steuern usf.) verwendet würden, gewährleistet werde. Besagter Schutzgedanke soll nicht nur durch ein materiellrechtliches Statistikgeheimnis, sondern darüber hinaus durch organisatorische und prozedurale Massnahmen gewährleistet werden. Diese Stossrichtung – der Ausbau von organisatorischen und prozeduralen Instrumenten wie der Einführung der Pflicht zu einem Verarbeitungsverzeichnis, einer Datenschutz-Folgenabschätzung usf., die das Datenschutzrecht faktisch griffig machen sollen – wird von den jüngsten rechtlichen Neuerungswellen, wie sie die DSGVO und das totalrevidierte DSG bringen, fortgesetzt.

1800 Das VI. Kapitel des zweiten Teils zeigte, dass das DSG für den privaten Bereich seine Normierungen am *individualrechtlichen Persönlichkeitsschutz* defensiv-

abwehrrechtlich ausrichtet. Ebendies wird durch den Zweckartikel des DSG an erster Stelle festgehalten. Da im privaten Bereich dem Grundsatz nach nur eine *qualifizierte Personendatenverarbeitung* und nicht jeder Umgang mit Personendaten als persönlichkeitsverletzend gilt, wurde das Regime als eines des *Integritätsschutzes* bezeichnet. Die Betrachtung des Regimes des DSG für den privaten Bereich wurde ergänzt um einen Blick auf datenschutzrechtliche Bestimmungen in Spezialerlassen, wodurch die in dieser Arbeit vorgeschlagene Qualifizierung des Regimes des DSG erhärtet wurde. Zugleich wurde gezeigt, dass das Datenschutzrecht der Schweiz ein bereichsspezifisch ausdifferenziertes Rechtsgebiet ist. Somit liess sich auch hier die Anerkennung kontextueller Erwägungen freilegen und zeigen, dass das Datenschutzrecht kontextrelatives Recht ist. Datenschutzrecht umfasst nicht nur das DSG, vielmehr finden sich zahlreiche Spezialerlasse und -normen, so im Humanforschungsbereich, Arbeitsbereich und Gesundheitsbereich, wobei diese sowie die Geheimhaltungspflichten in Bezug auf Personenangaben die Anerkennung bereichsspezifischer Datenschutznormierungen belegen.

1801 Im dritten Teil wurden im VII. Kapitel Bedeutungszuweisungen hinsichtlich des Datenschutzrechts und namentlich des DSG beleuchtet, wobei insb. auf das *faktische Vollzugsdefizit* des DSG eingegangen wurde. Hier wurde gezeigt, dass die «Aufbürdung» der Einhaltung des Datenschutzrechts auf das Individuum problematisch ist und weitgehend ins Leere läuft. Sichtbar wurde, dass es in erster Linie die Interventionen des EDÖB infolge sog. Systemfehler sind, welche dem DSG eine gewisse Griffigkeit verleihen. Allerdings handelt es sich dabei, in Anbetracht des Ausmasses von Personendatenverarbeitungen in der heutigen Zeit, um punktuelle Interventionen.

1802 In der Realität und Praxis hat das DSG vor seiner Totalrevision nur marginale Bedeutung erlangt. Anhand eines Blickes auf die *mediale Landschaft* sowie die *politische Debatte* wurde nachgewiesen, dass Anliegen des Datenschutzes hoch auf der Agenda stehen, wobei erneut der Facettenreichtum der Thematik sichtbar wurde. Insofern liess sich feststellen, dass die allgemeine gesellschaftliche Reflexion die erweiterte Landschaft, in welche datenschutzrechtliche Anliegen eingebettet sind, besser abzubilden vermag als ein verengter Fokus auf das Datenschutzgesetz als sog. Querschnittsgesetz. Die Konzentration auf das DSG als Querschnittsgesetz führt dazu, weitere datenschutzrechtliche Vorgaben in Spezialerlassen sowie die damit in Ansätzen anerkannte systemspezifische Rechtsgestaltung zu übersehen.

1803 Dass die Fokussierung auf ein «Datensubjekt» und auf Personendaten als Quasi-Objekte zu kurz greift, wurde sodann anhand der *Darstellung der beiden wichtigsten faktischen Herausforderungen des Datenschutzrechts* beschrieben: den *Personendatenverarbeitungstechnologien* und ihren Kapazitäten auf der einen Seite sowie der *Ökonomisierung* und namentlich der expansiven Wirkung wirt-

schaftlicher Rationalitäten auf der anderen Seite. Nachgezeichnet wurde, inwiefern diese Techniken und Praktiken ein dicht verästeltes Netzwerk begründen, in welchem Personendaten fliessen. Der individualrechtliche Ansatz stösst vor diesem Hintergrund in der Realität an Grenzen.

1804 Es folgte im VIII. Kapitel des dritten Teils ein Blick auf die *wichtigsten aktuellen Lösungsansätze* und Reaktionen auf die attestierten datenschutzrechtlichen Defizite. Hierbei zeigte sich, dass die *jüngsten Erlasse* spezifisch am faktischen Vollzugsdefizit ansetzen, indem diese konkrete Umsetzungsinstrumente fordern, so das Verzeichnis der Verarbeitungshandlungen. Weiter wurde attestiert, dass zwar die «starke Hand des Staates» eine Stossrichtung gerade in der DSGVO ist, diese indes in beachtlicher Weise die «Verantwortung der Verantwortlichen» durchsetzt. Es sind die personendatenverarbeitenden Stellen, die in erster Linie dazu verpflichtet werden, datenschutzkonform zu handeln, wobei sie insofern stets in der Lage sein müssen, dies zu belegen. Vorgesehen werden umfassende und durchgreifende Dokumentations- und Rechenschaftspflichten. In diesen gesetzlichen Neuerungen lassen sich starke Ergänzungen des bislang abwehrrechtlich, defensiv gedachten Datenschutzrechts, das im Persönlichkeitsrecht gründet, verzeichnen. Datenschutz wird zur Compliance- und Governance-Aufgabe der verarbeitenden Stellen, die neu – sofern nicht Auftragsverarbeitende – als *Verantwortliche* bezeichnet werden. Zudem wird ein risikobasierter Ansatz implementiert. Organisatorische und prozedurale Instrumente sowie technische Massnahmen gewinnen für und im Datenschutzrecht an Relevanz. Obschon auch die Rechte der Betroffenen und damit die individualrechtliche Perspektive ausgebaut werden mit den jüngsten Gesetzesneuerungen, finden sich markante Entwicklungstrends sowohl in der DSGVO als auch im totalrevidierten DSG. Das Datenschutzrecht zeigt sich nicht erst im Fall einer Persönlichkeitsverletzung. Neu müssen personendatenverarbeitende Stellen proaktiv die Datenschutz-Compliance und -Governance durch facettenreiche Massnahmen implementieren. Auch der Risiko-Ansatz setzt einen Kontrapunkt zum individualrechtlich und defensivrechtlich angelegten Persönlichkeitsschutz.

1805 Im Zentrum der von *(rechts-)wissenschaftlicher Seite präsentierten Lösungsansätze* steht die Stärkung der individualrechtlichen Position, wobei sowohl eigentumsrechtliche als auch persönlichkeitsrechtliche Ansätze mit Verwertungskompetenzen diskutiert werden. Allerdings wurde gezeigt, dass die Lösungsstrategie, datenschutzrechtliche Herausforderungen primär durch die Stärkung der Selbstbestimmung und Autonomie zu beantworten, nur beschränkt tauglich ist. Nicht zuletzt, weil die datenschutzrechtliche Einwilligung in Anbetracht der Komplexität der sich in der Realität abspielenden Verarbeitungsprozesse in technischer wie geschäftlicher Natur kaum mehr sinnhaft erteilt werden kann.

Folglich zog sich wie ein roter Faden durch diese Schrift die Erkenntnis, dass die Bedeutung des Verarbeitungszusammenhanges und systemischer, kontextueller Erwägungen für das Datenschutzrecht von Relevanz ist. Sie ist im geltenden Recht angelegt. Allerdings rückte eine solche Dimension hinter diejenige des informationellen Subjektschutzes und damit teilweise aus dem Blickfeld. Ebenso zeigte sich an zahlreichen Stellen die Produktivität einer Betrachtungsweise, die *Personendatenverarbeitungsprozesse als Datenflüsse innerhalb und zwischen verschiedenen Bereichen* in den Fokus nimmt. Es ist eine Perspektive, die sich aufgrund der starken Subjekt-Objekt-Verhaftung gerade des Schweizer DSG nicht aufdrängt. Es ist die *kontextuelle Dimension*, die für ein Datenschutzrecht mitentscheidend ist, damit dieses seine Schutzziele adäquat definiert und wirksam zu gewährleisten vermag. 1806

Die *Relevanz der kontextuellen Dimensionen datenschutzrechtlicher Herausforderungen* weiter zu elaborieren und *mit einem Recht auf informationellen Systemschutz einen neuen Ansatz* zu präsentieren, der einen *Perspektivenwechsel für das Datenschutzrecht der Zukunft* auch in Europa anregt, ist Ziel dieses IX. und letzten Kapitels. Denn auch wenn sich unsere Gesellschaft als Informations- und Kommunikationsgesellschaft bezeichnet, ist sie zugleich eine in plurale Bereiche strukturierte Gesellschaft. Dies anzuerkennen – so die These – ist richtungsweisend für ein in Zukunft tragfähiges Datenschutzrecht. 1807

Der Vorschlag für eine datenschutzrechtliche Rekonfiguration, welche die Vielschichtigkeit und Vielseitigkeit sowie den Facettenreichtum datenschutzrechtlicher Herausforderungen angemessen integriert, soll zunächst anhand einer Konstellation illustriert werden, welche die Schweiz intensiv beschäftigt(e): die geheime Observation von Versicherungsleistungsbezügern durch Privatdetektive.[2325] Die vertiefte Auseinandersetzung mit der Praxis macht es möglich, einen Perspektivenwechsel für ein künftiges Datenschutzrecht vorzuschlagen. Es geht um die Anerkennung, dass der Datenschutz und sein Recht nicht nur Subjektschutz, sondern auch Systemschutz zu gewährleisten hat. Die Tragfähigkeit und Funktionstüchtigkeit dieses Vorschlags wird anhand weiterer Beispiele, die im Zuge dieser Arbeit bereits zur Sprache kamen, erhärtet. Den Abschluss bilden theoretische Ausführungen zu Inhalt, Ausgestaltung und Umsetzung eines Rechts auf informationellen Systemschutz.[2326] 1808

2325 Zu dieser auch Pärli, recht 2018, 120 ff.; zur geheimen Observation von Arbeitnehmenden durch private Arbeitgeber unter Darstellung auch der Rechtsprechung Ders., HAVE 2018, 228 ff. unter Hinweis auf die Anwendbarkeit des Schutzbereichs des Privatlebens gemäss Art. 8 EMRK auch im Arbeitsverhältnis, 230; EGMR Nr. 61496/08 – Bârbulescu/Romania, Urteil vom 12. Januar 2016.

2326 Der Ansatz wird anhand eines Falles aus dem versicherungsrechtlichen Kontext herausgearbeitet; während das vorliegende Buch finalisiert wurde, erging ein weiteres bedeutsames Urteil im Bereich des Datenschutzes im Versicherungskontext – jüngst BVGer A-3548/2018 – Helsana+, Urteil vom 19. März 2018. Das Urteil wäre geeignet, um den hier entwickelten paradigmatischen Ansatz zu verifizieren sowie konkretisierende Elemente zu generieren.

B. Veranschaulichungen

1. Detektiv in geheimer Mission

1809 Am Anfang dieses letzten Kapitels und damit in der Schlussszene dieses Buches schliesst sich der Kreis: Die informativen Geschichtsfragmente des ersten Teils berichteten von Dienern («Server»), Spionen und (märchenhaften) Spionagefällen, himmlischen sowie irdischen Informationsmittlern, dem göttlichen Buch, informationellen Herrschaftstechnologien sowie alten Prozessen dafür, wie aus Informationen bare Münze gemacht wurde. Eine traditionsreiche Figur ist noch heute für eine Studie zum Informations- und Datenschutzrecht beachtenswert: Sie ist nicht nur befähigt, Fälle des Versicherungsbetruges aufzudecken, sondern auch neue Perspektiven für Herausforderungen sowie Ziele des Datenschutzrechts aufzuspüren: der Detektiv.

1.1. Informant für den Datenschutz

1810 Der «Maulwurf», Deckname für den geheimen Ermittler, obschon fast blind, ist prädestiniert, neue Sichtweisen für das Datenschutzrecht ans Licht zu bringen und Indizien dafür freizulegen, wie der datenschutzrechtliche Boden umgegraben werden soll. Die bisherige Datenschutzrechtsdebatte nahm primär die Frage unter die Lupe, ob personenbezogene Daten als Objekte resp. Quasi-Sachen qualifiziert werden können.[2327] Damit wird zugleich der Prozess der Transformation von Personendaten in Wirtschaftsgüter adressiert, was mit einem Plädoyer für ein Recht an eigenen Daten einhergeht. Die Landschaft ist von dualistischen Kategorien geprägt: öffentlich versus privat, Datensubjekt versus Datenobjekt, Persönlichkeitsrecht versus Dateneigentum, ideelle Natur versus ökonomische Natur, Datensubjekt versus Verarbeitende, Datenverarbeitung ja versus Datenverarbeitung nein. Es lassen sich indes weitere Perspektiven einnehmen, woraus sich neue Bilder und Betrachtungsweisen ergeben.

1811 Ein anderes Narrativ vermitteln die nicht nur in Romanen, sondern seit Jahrhunderten in realer Mission agierenden Detektive, Ermittler, Spioninnen. Sie sind zwischen verschiedenen Ländern und Milieus oder Bereichen unterwegs, um Informationen von einer Seite auf die andere zu übermitteln. Unter der Erde, *undercover*, im Dunkeln des Erdreichs und damit jenseits des sichtbaren Lebens wurde und wird ein dichtes Netz von Kanälen und Gängen gegraben, um Informationen aus bestimmten Kreisläufen abzugreifen und die erlangten Informationen weiter und an andere Stelle transportieren zu können.

2327 Vgl. früh und zugleich kritisch zur Subjekt-Objekt-Relation im Informationsrecht Mayer-Schönberger, Information und Recht, 54 ff.

Es ist dieses Bild des *Informationsflusses* innerhalb von und zwischen verschiedenen Feldern, Ländern resp. Bereichen in netzwerkartigen Strukturen und von Akteuren in unterschiedlichen Rollen sowie Funktionen mit jeweils spezifischen Zielen und Zwecken, welches produktive Erkenntnisse für Neugestaltung eines modernen Datenschutzrechts im Zeitalter der Digitalisierung zu liefern vermag. Dies wurde in vorliegender Arbeit erstmals im historischen Teil freigelegt und zeigte sich wiederholt im Zuge dieser Schrift. Dass der Figur des Detektivs nun die Hauptrolle bei der Ermittlung neuer Perspektiven für ein Datenschutzrecht der Zukunft eingeräumt wird, ist allerdings nicht nur durch metaphorische, intuitive oder romaneske Assoziationen begründet. 1812

Vielmehr kommt dem *Detektiv* in der Schweiz unserer Tage eine wichtige Rolle in der Realität, aber auch im Recht und insb. für das Datenschutzrecht zu. Wenige Konstellationen werden in der Schweiz unter dem Gesichtspunkt des Datenschutzes so intensiv und kontrovers beurteilt wie die *verdeckte Observation im Versicherungskontext zwecks Aufdeckung von Versicherungsbetrugsfällen*.[2328] 1813

Im Zentrum der anschliessenden Erwägungen steht eine «Affäre», die zur Verurteilung der Schweiz durch den Europäischen Gerichtshof für Menschenrechte führte. Die versicherungsrechtliche Auseinandersetzung erstreckte sich über unzählige Jahre hinweg. «Der Fall» EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, ein infolge eines Verkehrsunfalles in aller Härte geführter Versicherungskonflikt über den Invaliditätsgrad einer Frau, gibt richtungsweisende Impulse für ein neues datenschutzrechtliches Paradigma. Der Fall kann damit als produktiver Konflikt gelesen werden. Es geht um eine Überwachung im staatlichen Kontext (obligatorische Versicherung), wobei der Entscheid von Gächter als wegweisend beurteilt wurde.[2329] 1814

Die Bedeutung des Falls und Urteils geht weit über die Tatsache hinaus, dass in der Schweiz einer etablierten Observationspraxis im Versicherungskontext wegen EMRK-Widrigkeit durch den EGMR ein Riegel vorgeschoben und der Schweizer Gesetzgebungsapparat angeworfen wurde. Bevor herausgearbeitet wird, inwiefern der Entscheid richtungsweisend ist, werden sein Sachverhalt sowie die 1815

2328 Vgl. BGer 8C_629/2009, Urteil vom 29. März 2010; Pärli, recht 2018, 120 ff.; Banholzer, SRF online vom 2. Mai 2018, Mehr als die Polizei erlaubt, <https://www.srf.ch/news/schweiz/ueberwachung-von-versicherten-mehr-als-die-polizei-erlaubt> (zuletzt besucht am 30. April 2021); Daten:recht, BezGer Meilen: Schranken des DSG für einen Privatdetektiv, Zürich 2003, <https://datenrecht.ch/bezger-meilen-schranken-des-dsg-fuer-einen-privatdetektiv/> (zuletzt besucht am 30. April 2021); vgl. auch BGE 136 III 410, wobei der Entscheid die Observation im öffentlichen Raum unter Rückgriff auf die Sphärentheorie zulässt, E 3.4.

2329 So Gächter, SRF online vom 18. Oktober 2016, Versicherungen dürfen mögliche Betrüger nicht observieren, <https://www.srf.ch/news/schweiz/versicherungen-duerfen-moegliche-betrueger-nicht-observieren> (zuletzt besucht am 30. April 2021); dagegen ging es in EGMR Nr. 61496/08 – Bârbulescu/Romania, Urteil vom 12. Januar 2016, um die Observation eines Arbeitnehmers in einem *privaten Kontext*, wobei in beiden Entscheidungen ähnliche Bewertungen vorgenommen wurden, vgl. insofern die Beiträge von Pärli.

Erwägungen des EGMR umrissen. Dargestellt werden zugleich die Ausführungen des Bundesgerichts, das von der Rechtmässigkeit der Observation ausgegangen war.[2330] Es war nicht das erste Mal, dass sich Schweizer Gerichte mit dem Thema zu befassen hatten.[2331]

1816 Es folgt eine Analyse der Praxis sowie der einschlägigen rechtlichen Erwägungen. Davon angeregt entwickelt sich ein Sichtwechsel, der sämtliche der *drei im zweiten Teil beleuchteten Strukturmerkmale* des DSG in ein neues Licht rückt. Insofern wird sich zeigen, dass einzig aufgrund der Tatsache, wonach sich eine bestimmte Praxis (oder Technologie) etabliert hat, selbst wenn diese rechtlich anerkannt ist, diese im Lichte eines neuen Verständnisses datenschutzrechtlicher Schutzzwecke nicht anerkannt werden sollte. Mit anderen Worten beschränkt sich diese Schrift nicht darauf, festzustellen, dass die gesetzlichen Vorgaben nicht erfüllt waren – z. B. das Vorliegen einer gesetzlichen Grundlage für den öffentlichen Bereich oder einer gültigen Einwilligungserklärung. Vielmehr wird die Angemessenheit datenschutzrechtlicher Vorgaben *de lege lata* im Lichte neu definierter Schutzzwecke des Datenschutzrechts *de lege ferenda* betrachtet.

1.2. «Der Fall» EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz

1.2.1. Vorbemerkungen

1817 Die Verurteilung der Schweiz durch den EGMR im Zusammenhang mit der Praxis der geheimen Versicherungsobservation (im staatlichen Kontext der obligatorischen Versicherung) gilt, wie gesagt, als richtungsweisend. Aufschlussreich sind allem voran die *Erwägungen des Europäischen Gerichtshofes für Menschenrechte*. Dass vonseiten der Gerichte vitale Impulse für das Datenschutzrecht ausgehen, zeigte bereits das Studium des Volkszählungsurteils des Bundesverfassungsgerichts.[2332] Die Auseinandersetzung im Rahmen dieser Studie führte vor Augen, dass sich der volle Erkenntnisgehalt eines Entscheides nicht zwingend in den gemeinhin zitierten «Kernaussagen» oder Leitideen zu erschöpfen braucht. Kaum eine Aussage des Volkszählungsurteils wurde öfter rezipiert als diejenige zum Recht auf informationelle Selbstbestimmung: Das «Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen».[2333]

2330 BGer 8C_629/2009, Urteil vom 29. März 2010, der in E 6.1. auf BGE 135 I 169 referiert.
2331 Insofern bereits BGE 132 V 241, BGE 135 I 169, BGE 136 III 410.
2332 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983; vertiefend hierzu zweiter Teil, V. Kapitel, B.4.
2333 BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983, E 173; zum Recht auf informationelle Selbstbestimmung als Schutzgut des Datenschutzrechts vgl. z. B. Rossnagel, digma 2011, 160 ff., 160 f.

Eine eingehende Befassung mit den Urteilserwägungen verdeutlichte, dass der Gehalt des Entscheides nicht auf die Stärkung des Individualrechtsschutz limitiert ist. Vielmehr werden in zentraler Weise *Erwägungen des Systemschutzes* integriert.[2334] Die Ausführungen des Bundesverfassungsgerichts zur Bedeutung des *Verarbeitungszusammenhanges*, also des Verarbeitungszweckes sowie der Zweckbindung, sind von entscheidender Relevanz. Ebenso produktiv ist die Absicherung entsprechender «gebundener Informationsflüsse» durch organisatorische und prozedurale Instrumente. Sie treten in ihrem Bedeutungsgehalt neben die «Definierung» eines neuen Individualrechts. 1818

Dies vorausgeschickt wird nun dem Observationsentscheid, EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, vertiefte Aufmerksamkeit geschenkt. In Bezug auf diesen Entscheid dürfte als zitationswürdig gesehen werden: 1819

> «For the above reasons – and notwithstanding the arguably minor interference with the applicant's Article 8 rights – the Court does not consider that the domestic law indicated with sufficient clarity the scope and manner of exercise of the discretion conferred on insurance companies acting as public authorities in insurance disputes to conduct secret surveillance of insured persons. In particular, it did not, as required by the Court's case-law, set out sufficient safeguards against abuse. The interference with the applicant's rights under Article 8 was not, therefore, „in accordance with the law" and there has accordingly been a violation of Article 8 of the Convention.»[2335]

Oder in den Worten der Berichterstattung: 1820

> «Verletzung von Art. 8 EMRK wegen unzureichender rechtlicher Grundlage für Überwachungsmassnahmen durch eine Versicherung.»[2336]

Allerdings: Der volle Erkenntnisgehalt aus einer Perspektive des Datenschutzes ergibt sich nicht aus der «ungenügenden gesetzlichen Grundlage», selbst wenn diese das entscheidende Element war, das zur Verurteilung der Schweiz führte. Die Schaffung besagter gesetzlicher Grundlage nimmt der Konstellation keineswegs die datenschutzrechtliche Brisanz. Der volle und reichhaltige Gewinn für diese rechtswissenschaftliche Studie liegt in der Betrachtung der *Affäre* in ihren vielen Kapiteln. 1821

Die zur Beurteilung stehende geheime Observation durch den Detektiv ist zwar die Schlüsselszene, das Urteil des EGMR juristischer Höhepunkt des Falles. Der Konflikt zog sich über Jahre hinweg, mit diversen Divergenzen zwischen Ärzte- 1822

2334 Zweiter Teil, V. Kapitel, B.4.

2335 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016; zu den Anforderungen an die gesetzliche Grundlage sowie die weiteren Voraussetzungen der Verletzung der Privatsphäre gemäss EMRK bei geheimen Überwachungen, allerdings im Arbeitskontext unter Bezug auf ebendieses Urteil Pärli, EuZA 2020, 224 ff., 231 ff.

2336 <https://www.humanrights.ch/de/ipf/rechtsprechung-empfehlungen/europ-gerichtshof-fuer-menschenrechte-egmr/erlaeuterte-schweizer-faelle/verletzung-art-8-emrk-unzureichender-rechtlicher-grundlage-ueberwachungsmassnahmen-versicherung> (zuletzt besucht am 20. September 2021).

schaft, Versicherung und Privatperson. Gerade die Art und Weise, in der sich dieser Fall abspielte, ist datenschutzrechtlich aufschlussreich. Mit ihm werden die dahinterstehenden Konfliktlagen dokumentiert.

1823 Ginge es nicht um eine so ernste Angelegenheit wie den Invaliditätsgrad infolge eines Autounfalles, so würde die «causa», in der unzählige Ärztinnen und Ärzte zu unterschiedlichsten Einschätzungen bezüglich des Gesundheitszustandes und Invaliditätsgrades der Betroffenen kamen, als Posse erscheinen. Der Fall löst Ungläubigkeit aus – selbst bei Menschen, denen bewusst ist, dass die Medizin nicht als exakte Wissenschaft gilt.[2337] Zwischen der Versicherung, bei der V.-B. obligatorisch unfallversichert war, und der Verunfallten entfachte sich eine über 21 Jahre andauernde Auseinandersetzung über die IV-Ansprüche.[2338] Das Handeln der Versicherung sowie die «Orientierungslosigkeit» aufseiten des Gesundheitspersonals lösen einen Vertrauensverlust aus. Und genau dieser Befund wird aus datenschutzrechtlicher Sicht ein wichtiges Stichwort sein. Was bedeutet es, wenn angeblich erst und nur die Ausforschung des «privaten Lebens von Versicherten im öffentlichen Raum» durch einen Privatdetektiv vermeintlich den Gesundheitszustand und daraus folgend die Arbeits(un)fähigkeit zu ermitteln vermag, was der insofern zuständigen, sachlich ausgebildeten Ärzteschaft anscheinend nicht zu gelingen vermochte?

1824 Doch beginnen wir mit dem Sachverhalt, «den Facts», die vom Unfall über daran anschliessende zahlreiche medizinische Untersuchungen mit sich widersprechenden Ergebnissen, die geheime Observation bis hin zu mehreren behördlichen resp. gerichtlichen Entscheidungen reichen.

1.2.2. Szenen eines Versicherungskonfliktes

1825 Der Verkehrsunfall: Am 28. August 1995 wurde die Schweizerin V.-B. beim Überqueren eines Fussgängerstreifens von einem Motorrad erfasst. Sie stürzte mit dem Hinterkopf auf die Strasse.[2339]

1826 Am 2. Oktober 1995 stellte ein Rheumatologe ein Hals- und Schädeltrauma fest, der Hausarzt schrieb V.-B. am 6. Dezember bis Ende des Jahres 1995 zu 100

2337 NZZ vom 2. Februar 2002, Ist die Medizin eine exakte Wissenschaft?, Zürich 2002, <https://www.nzz.ch/article7UOK8-1.364744> (zuletzt besucht am 30. April 2021).

2338 Der EGMR präsentiert unter dem Titel «The Facts» den langjährigen Konflikt zwischen Versicherter und Versicherungsgesellschaft, der von vielen medizinischen sowie gerichtlichen Analysen gestaltet wird. Die Schilderung dieses sich über unzählige Jahre hinweg ziehenden Konfliktes mit seinen Etappen kann nicht nur Prozessrechtlern als reichhaltiges Anschauungsmaterial zwecks Analyse prozessrechtlicher Zuständigkeitsfragen und einschlägiger Rechtsmittel dienen. Trotz der Erkenntnis, wonach die Medizin keine exakte Wissenschaft ist, sind die arbiträren Ergebnisse der unzähligen ärztlichen sowie gerichtlichen Prüfungen schwer nachvollziehbar und hinterlassen einen Eindruck der Irritation.

2339 BGer 8C_629/2009, Urteil vom 29. März 2010; vgl. BGE 135 169.

Prozent krank resp. arbeitsunfähig. Am 29. Januar 1996 wurde V.-B. im Universitätsspital Zürich untersucht.[2340] Der untersuchende Arzt kam zu dem Ergebnis, dass eine partielle Berufsrückkehr möglich sei. Dagegen befand ein anderer Arzt desselben Spitals am 12. Juni 1996, dass V.-B. vollkommen arbeitsunfähig sei. Auf Ersuchen der Versicherung wurde V.-B. in der Folge im Zentrum für medizinische Untersuchungen betreffend Invaliditätsversicherung in St. Gallen mehreren orthopädischen, neurologischen, neuropsychologischen und psychiatrischen Tests unterzogen. Das Untersuchungsergebnis lautete, dass V.-B. per Februar 1997 zu 100 Prozent arbeitsfähig sei.

1827 Daraufhin informierte die Versicherung V.-B., dass der Versicherungsanspruch per 23. Januar 1997 enden würde. Dagegen erhob V.-B. Einspruch. Beigelegt war ein Bericht eines Neurologen, der zahlreiche gesundheitliche Beschwerden dokumentierte. Nachdem der Einspruch von der Versicherung abgewiesen wurde, weil ein Zusammenhang zwischen dem Unfall und den beschriebenen Beschwerden als nicht erstellt betrachtet wurde, gelangte V.-B. an das Sozialversicherungsgericht des Kantons Zürich. Mit Entscheid vom 24. August 2000 hiess das Gericht die Beschwerde gut und forderte weitere Abklärungen. Zwischen den diversen medizinischen Berichten bestünden Divergenzen, welche eine Beurteilung der Kausalität zwischen den gesundheitlichen Beschwerden und dem Unfall nicht möglich machen würden.

1828 In der Folge wurde auf Antrag der Versicherung eine multidisziplinäre ärztliche Untersuchung in Basel angeordnet. Die untersuchenden Ärzte attestierten in ihren Berichten die umfassende Arbeitsunfähigkeit mit Blick auf die Tätigkeit von V.-B. als Coiffeuse. Die Versicherung stellte indes selbst diese Untersuchungsergebnisse auf den Prüfstand. Begründet wurden die Zweifel mit einer Befangenheit: Einer der rapportierenden Ärzte habe in einem frühen Stadium V.-B. privat untersucht. Die Versicherung verlangte eine zusätzliche Untersuchung. Der aus dieser Examination resultierende Bericht vom 11. November 2002 sah die Kausalität zwischen Unfall und der Gesundheitsbeeinträchtigung als erstellt. Beigelegt war ein neuropsychologischer Bericht.

1829 Am 21. März 2002 sprach die Sozialversicherungsanstalt des Kantons Zürich V.-B. eine volle Invaliditätsrente mit Rückwirkung zu. Die Versicherung dagegen liess am 5. Oktober 2003 ein weiteres Gutachten erstellen, basierend auf den bislang verfassten Untersuchungsberichten. Auch dieses stellte die Kausalität zwischen Unfall und Gesundheitsbeeinträchtigung fest, mit einem Invaliditätsgrad von 100 Prozent.

2340 Vgl. zu den einzelnen Untersuchungen und ihren Ergebnissen BGer 8C_629/2009, Urteil vom 29. März 2010, A und E 1 ff.; zum Sachverhalt ebenso EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 5 ff.

1830 Nichtsdestotrotz bestätigte die Versicherung am 14. Januar 2005 ihre Entscheidung, wonach die Leistungen per 1. April 1997 eingestellt würden. Ein anderer Arzt kam am 11. Juni 2005 – erneut auf der Grundlage der vorhandenen Untersuchungsberichte – zu dem Schluss, dass V.-B. höchstens zu 20 Prozent arbeitsunfähig sei. Gestützt auf diesen Bericht wies die Versicherung eine Beschwerde von V.-B. zurück. Das Sozialversicherungsgericht anerkannte mit Entscheidung vom 28. Dezember 2005 die Kausalität zwischen Unfall und gesundheitlichen Beeinträchtigungen. Es wies die Versicherung an, die Leistungen entsprechend festzusetzen. Hierauf forderte die Versicherung V.-B. auf, sich einer medizinischen Evaluation ihrer funktionalen Fähigkeiten zu unterziehen. Ebendies verweigerte V.-B. Sie wurde in der Folge auf die rechtlichen Konsequenzen einer Verweigerung hingewiesen. Eine Informierung über eine allfällige Observation erfolgte nicht.

1831 In der Folge kam es zu einer geheimen Observation von V.-B. durch einen Privatdetektiv: An mehreren Tagen im Oktober 2006 nahm er ein Monitoring von V.-B. im Auftrag der Versicherung vor. Die Observation erfolgte an vier Tagen über jeweils mehrere Stunden hinweg, wobei der Privatdetektiv über weite Strecken unter Einsatz von Video- und Fototechnologien agierte.

1832 Die Beschattungsergebnisse flossen in einen umfassenden Bericht ein. V.-B., so der Bericht, hatte vermutlich am letzten Tag der Aktion Kenntnis von der Observation erlangt. Sie beantragte die Einsichtnahme in den Überwachungsrapport. Dies lehnte die Versicherung am 17. November 2006 ab. Dagegen reichte V.-B. Beschwerde beim Eidgenössischen Amt für Gesundheit ein. Am 14. Dezember 2006 stellte die Versicherung V.-B. den Bericht doch zu. Verbunden wurde dies mit der Aufforderung zu einer weiteren medizinischen Untersuchung, zu welcher V.-B. sich erneut nicht bereit erklärte. Am 2. März 2007 eröffnete die Versicherung ihren Entscheid: Basierend auf der Fotoberichterstattung und dem Rapport des Detektivs sowie der Weigerung, an einer weiteren Untersuchung mitzuwirken, würden keine Leistungen erbracht.

1833 Am 12. April 2007 äusserte sich ein von der Versicherung beauftragter Neurologe mittels einer Expertenmeinung. Sie beruhte auf einer Auswertung sämtlicher vorhandener Dokumente inklusive des Observationsberichtes und namentlich der darin befindlichen Fotos. Er attestierte einen Invaliditätsgrad von 10 Prozent. Die Observationsaufnahmen würden zeigen, dass die gesundheitlichen Einschränkungen von V.-B., ein normales Leben zu führen, marginal seien. Entsprechend wurden die Rentenansprüche auf einen Invaliditätsgrad von 10 Prozent festgesetzt.

1834 Am 14. März 2008 wies das Bundesamt für Gesundheit die Versicherung an, über das Begehren von V.-B. auf Zerstörung der Observationsberichte sowie auf Festlegung der Rente zu entscheiden. Ersteres verweigerte die Versicherung. Die

Rente wurde gestützt auf einen IV-Grad von 10 Prozent festgesetzt. Auch diese Entscheidung blieb nicht unangefochten. Nunmehr machte V.-B. zudem eine Verletzung ihrer Persönlichkeit geltend.

Das Sozialversicherungsgericht entschied am 29. Mai 2009 zugunsten von V.-B. Es hielt fest, dass der Expertenbericht, der auf eine widerrechtliche Überwachungsmassnahme abstellte, keinerlei Beweiswert aufweise. Zudem sei die Klägerin aufgrund der Entscheidung vom 28. Dezember 2005 nicht verpflichtet gewesen, zusätzliche Untersuchungen über sich ergehen zu lassen. Die Versicherung gelangte an das Bundesgericht und rügte die Höhe der festgesetzten Rente.[2341] 1835

Das höchste Schweizer Gericht sah sich zunächst mit der Frage konfrontiert, ob die Beweismittel – die Ergebnisse einer Observation durch einen Privatdetektiv in Gestalt eines Berichtes und von Videoaufnahmen – zulässig waren.[2342] Entgegen dem Entscheid der Vorinstanz, indes in Übereinstimmung mit seiner bisherigen Rechtsprechung, kam das Bundesgericht zu dem Schluss, dass die Observationsergebnisse zur Beurteilung des Versicherungsanspruches verwertbar seien.[2343] In die Erwägungen floss ein, dass sich die Klägerin, die sich mehreren medizinischen Begutachtungen unterzogen hatte, deren erste eine Arbeitsunfähigkeit zu 100 Prozent attestierte, geweigert hatte, im Rahmen einer Einschätzung ihres funktionellen Leistungsvermögens (EFL) mitzuwirken und sich neurologischen Abklärungen zu unterziehen. Das Bundesgericht hiess die Invaliditätsberechnung des Versicherers weitgehend gut. Gerade die Beschattung durch Privatdetektive habe, so das Bundesgericht, gezeigt, dass V.-B. einschränkungslos alltäglichen Dingen nachgehen könne. Dies sei mit dem Ergebnis der ursprünglichen Gutachten nicht vereinbar. Aufgrund solcher Widersprüche seien weitergehende Abklärungen seitens der Versicherung zur Arbeitsfähigkeit von V.-B. angezeigt gewesen. Das Bundesgericht sah keinen Anlass, Beanstandungen gegenüber der geheimen Observation und deren Konsequenzen anzubringen.[2344] 1836

Das Bundesgericht wie der EGMR hatten in der hier im Zentrum stehenden causa zunächst festgehalten, dass eine Versicherungsgesellschaft, die gemäss Art. 68 UVG im Register zur Durchführung der obligatorischen Unfallversicherung eingetragen ist, eine öffentliche Aufgabe wahrnehme. Sie gelte als Behörde i. S. v. Art. 1 Abs. 2 lit. e VwVG, handle hoheitlich und habe den Grundrechtsschutz zu wahren.[2345] 1837

2341 Vgl. EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 33 ff.
2342 Vgl. Bger 8C_629/2009, Urteil vom 29. März 2010, E 6.1. ff.
2343 Vgl. auch BGE 135 I 169, E 5.7.; BGE 129 V 323, E 2.c.
2344 BGer 8C_629/2009, Urteil vom 29. März 2010, E 6 ff.
2345 Vgl. BGE 135 I 169, E 4.1. und E 4.2., auf den in BGer 8C_629/2009, Urteil vom 29. März 2010, E 6 verwiesen wird; EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 43.

1838 Das höchste Schweizer Gericht referierte sodann auf seinen Leitentscheid zur Observation versicherter Personen, BGE 135 I 169 vom 19. April 2010. In besagtem Urteil hatte das Bundesgericht befunden, dass die Unfallversicherung befugt sei, eine versicherte Person durch einen Privatdetektiv observieren zu lassen:

> «Durch die privatdetektivliche Observation einer versicherten Person sollen Tatsachen, welche sich im öffentlichen Raum verwirklichen und von jedermann wahrgenommen werden können (beispielsweise Gehen, Treppensteigen, Autofahren, Tragen von Lasten oder Ausüben sportlicher Aktivitäten), systematisch gesammelt und erwahrt werden. Auch wenn die Observation von einer Behörde angeordnet wurde, verleiht sie den beobachtenden Personen nicht das Recht, in die Intimsphäre der versicherten Person einzugreifen. […] Eine regelmässige Observation versicherter Personen durch Privatdetektive stellt jedenfalls dann einen relativ geringfügigen Eingriff in die grundrechtlichen Positionen der überwachten Personen dar, wenn sie sich auf den in E. 4.3 hievor umrissenen Bereich und damit insbesondere auf den öffentlichen Raum beschränkt […]. In der Lehre wird teilweise gar die Ansicht vertreten, eine solchermassen beschränkte Observation beschlage den Schutzbereich des Grundrechts der Privatsphäre nicht […]. Der Kerngehalt von Art. 13 BV wird durch die Anordnung einer solchen Überwachung nicht angetastet. […] Nachforschungen durch einen Privatdetektiv werden nur in einem verschwindend kleinen Promillesatz der bei den Unfallversicherungen gemeldeten Fällen angezeigt sein […]. Insgesamt sind daher die gesetzlichen Grundlagen für die Einschränkung der grundrechtlichen Positionen der versicherten Personen hinreichend bestimmt (E. 5.4.2). Das öffentliche Interesse an der Einschränkung des Schutzes der Privatsphäre liegt darin, keine nicht geschuldeten Leistungen zu erbringen, um die Gemeinschaft der Versicherten nicht zu schädigen […]. […] Die Anordnung einer Observation durch einen Privatdetektiv ist zur Erreichung des angestrebten Zieles (wirksame Bekämpfung von Missbräuchen) geeignet und auch erforderlich, da nur diese Beweismittel – beispielsweise bei offensichtlich bestehenden Anhaltspunkten einer effektiv bestehenden Arbeitsfähigkeit – eine unmittelbare Wahrnehmung wiedergeben können. Bezüglich der Möglichkeit weiterer medizinischer Abklärungen als Ersatz für die Observation ist zu beachten, dass auch solche – soweit sie überhaupt geeignet wären, einen gleichwertigen Erkenntnisgewinn zu erbringen – ebenfalls einen nicht leichtzunehmenden Eingriff in die grundrechtlichen Positionen der versicherten Person voraussetzen würden. Die Anordnung einer Observation ist schliesslich auch im engeren Sinne verhältnismässig […]. Zusammenfassend ist festzuhalten, dass die Anordnung einer Überwachung versicherter Personen durch die Unfallversicherung in dem in E. 4.3 umrissenen Rahmen zulässig ist; die Observationsergebnisse können somit für die Beurteilung der streitigen Fragen grundsätzlich verwendet werden […].»[2346]

1839 Kernfrage des Leitentscheides war somit, ob die Observation als Grundrechtsverletzung zu taxieren sei, genauer als Verletzung von Art. 13 BV. Erwägungen zu Schutzobjekt, gesetzlicher Grundlage sowie Verhältnismässigkeit standen im Vordergrund.

1840 Um den *Schutzgehalt des Grundrechts* zu konkretisieren, operierte das Bundesgericht mit der *Sphärentheorie*: Während das Eindringen in die Intimsphäre der versicherten Person durch die Observation nicht tunlich sei, sei eine geheime

2346 Vgl. BGE 135 I 169, E 4.3., E 4.4. sowie E 5.

Observation, die das Verhalten im *öffentlichen Raum* aufzeichne, anders zu beurteilen. Die Argumentation vermag unter mehreren Gesichtspunkten nicht zu überzeugen.

An erster Stelle ist es problematisch, wenn das Bundesgericht in anderen Entscheidungen vom Recht auf informationelle Selbstbestimmung spricht, teilweise selbst von einem «Herrschaftsrecht», in diesem Entscheid allerdings von der Sphärentheorie ausgeht. Wenn das Bundesgericht je nach Fall und Fallkonstellation einmal von einem Grundrecht auf Achtung der Privatsphäre, ein andermal von der Garantie eines Rechts auf informationelle Selbstbestimmung ausgeht, dürfte zumindest eine Begründung dafür erwartet werden, wie die unterschiedlichen Grundrechtsdefinitionen und -inhalte begründet werden können. 1841

Eine solche Begründung erübrigt sich nur dann, wenn mit dem Recht auf informationelle Selbstbestimmung und dem Recht auf Achtung der Privatsphäre dasselbe gemeint ist. Mit anderen Worten: Dann werden für einen identischen Rechtsgehalt unterschiedliche Titel resp. Bezeichnungen gewählt. Das ist indes offensichtlich nicht der Fall und kann auch so nicht sein. Die inkongruente Definierung und Anrufung zweier in ihrem Gehalt grundverschiedener Rechtsinhalte dürfte als arbiträr benannt werden. 1842

Weiter ignoriert die bundesgerichtliche Anknüpfung an die Sphärentheorie die fundierte und weitreichende Kritik, die in Anbetracht der neuen Technologien an ihr geübt wird.[2347] Die Orientierung an einer räumlichen resp. geografisch-lokalen Struktur des Schutzobjektes sowie die dichotome Ein- resp. Zweiteilung zwischen einem privaten resp. intimen *vis-à-vis* eines öffentlichen Raumes kann datenschutzrechtliche Aufgaben nicht bewältigen.[2348] Es ist unbestritten, dass das Konzept datenschutzrechtliche Herausforderungen nicht angemessen zu adressieren vermag.[2349] 1843

2347 M. w. H. Aebi-Müller, N 512 ff. mit einer Würdigung unter N 519 ff.

2348 Eine räumlich konnotierte Konzeptionierung findet sich namentlich bei Warren/Brandeis, Harv. L. Rev. 1890, 193 ff.; zum Schutz des privaten Raums unter Art. 8 EMRK Schiedermair, 197 ff.; zu den im Internet relevanten Schutzgütern gemäss Art. 8 EMRK auch Paefgen, 7 ff.; kritisch zum Sphärenmodell auch Hoppe, ZEuP 2005, 656 ff., 661 f.; vgl. dazu, dass sich die aktuelle Gesellschaft nicht mit der Sphärentheorie mit einer Trennung von öffentlich und privat mit hieran anknüpfenden Rechtsfolgen bewältigen lässt; Ders., ZUM 2000, 879 ff., 885 ff., auch mit dem Hinweis, dass es nicht auf quasi-räumliche Sphären, stattdessen vielmehr auf den Informationsgehalt ankomme.

2349 Vgl. insb. auch mit Blick auf den Dienst von Google Street View, wobei ein grundlegender Unterschied zwischen einer *en passant* wahrgenommenen «Strassenszene» durch das menschliche Auge und Gehirn gegenüber der Aufzeichnung ebensolcher «Strassenszenen» durch die Videokamera, montiert auf dem Google-Street-View-Auto, besteht: Die technisch unterstützte Aufzeichnung und die anschliessende Einspeisung in das Internet, welche weitreichende Analyse- und Verknüpfungsmöglichkeiten gibt, welche im «stillen Kämmerchen» auch durch die Nutzenden ermöglicht werden, verleihen der Angelegenheit einen gänzlich neuen Charakter. Diese Transformation eines Vorganges mittels Einsatzes von Technologien wird vom Bundesgericht in keiner Weise reflektiert; vertiefend Nissenbaum, 51 f., 192 f., 219 ff.; Dies., Dædalus 2011, 32 ff.; zu einer (falschen) Idee der gänzlichen Anonymität der Internetnutzenden unter Hinweis auf die berühmte, im New Yorker veröffent-

1844 Die Problematik der Anwendung eines sphärentheoretischen Konzeptes erschöpft sich indes nicht in der unbefriedigenden Definierung des Schutzobjektes im Lichte der technologischen und geschäftlichen Realitäten. Darüber hinaus kontaminiert der Einsatz der Sphärentheorie weitere Verarbeitungsgrundsätze resp. -vorgaben. Damit breiten sich die Defizite der Sphärentheorie über das Schutzobjekt hinweg aus. So referiert das Bundesgericht für die Beurteilung der Verhältnismässigkeit des Grundrechtseingriffes auf das «sphärische» Denken: Eine geheime Observation sei ein «relativ geringer Eingriff» in die Grundrechtsposition der versicherten Person, wenn sie sich auf die bezeichneten Bereiche – sprich den öffentlichen Raum – beschränke. Zudem sei nur ein «verschwindend kleiner Teil» der Versicherten von einer solchen Massnahme betroffen.

1845 Mit diesen Erwägungen versäumt das Bundesgericht die Kenntnisnahme weiterer problematischer Dimensionen der Observationspraxis im Lichte des Rechts und spezifisch des Datenschutzrechts: Die Betroffenheit ist für das konkret betroffene – weil observierte – Subjekt resp. Datensubjekt keineswegs gering. Ebenso wenig ist nur ein verschwindend kleiner Teil von Versicherten betroffen. Vielmehr hat die Praxis weiter- und tiefgreifendere Konsequenzen. Diese Aspekte sind zu vertiefen.

1846 Für den konkreten Fall ist sogleich anzufügen: Ganz offensichtlich konnte gerade *nicht* von einem erhärteten Verdacht eines Versicherungsbetruges gesprochen werden. Ein solcher aber liefert potentiell die Legitimation für eine geheime Observation. Im vorliegenden Fall ist es vielmehr so, dass von einer Unmöglichkeit oder Unfähigkeit der medizinischen Expertinnen und Experten, den Gesundheitszustand und Invaliditätsgrad, die Arbeits(un)fähigkeit sowie die daraus abzuleitende IV-Rente hinreichend konsistent zu beurteilen, auszugehen ist.

1847 Es geht damit unter Umständen um Graubereiche und Unschärfen. Mit solchen hat nicht bloss die Medizin umzugehen, sondern auch andere Wissenschaften mit ihren Anwendungen. In die rechtliche Sprache übersetzt lautet die Frage: Wer trägt die Konsequenzen, wenn eine Tatsache nicht hinreichend sicher belegt oder bewiesen werden kann resp. wenn Bewertungsdifferenzen bestehen? Im vorliegenden Fall könnte weniger von einer Unmöglichkeit, sondern selbst von der ungenügenden Expertise seitens des Medizinalpersonals auszugehen sein. Noch näherzuliegen scheint aber der Schluss, dass unter Umständen rein ökonomische Motive vonseiten der Versicherung entscheidend waren: Die Versicherung stellte

---

lichte Karikatur mit dem Internet vor dem Computer und der Sentenz «On the Internet, nobody knows you're a dog» vgl. Waidner/Karjoth, digma 2004, 18 ff., 18; zu den Grenzen der Anonymität im Internet Weber H./Heinrich, ZSR 2013, 477 ff.; dazu, dass das Internet keineswegs ein Raum der Anonymität, stattdessen einer der Dauerbeobachtung ist, Bergelson, UC Davis L. Rev. 2003, 379 ff.

nahezu jedes der vielen ärztlichen Atteste, die eine Invalidität auswiesen, in Frage. Erst hieraus resultierte eine Veranlassung zur Observation.[2350]

Das Bundesgericht beurteilte im Falle von V.-B. die privatdetektivische Observation als rechtmässig. In der Folge gelangte V.-B. mit Beschwerde an den EGMR. Sie rügte, dass die Überwachungsmassnahmen sowie die rechtlichen Grundlagen insb. vor Art. 8 EMRK nicht standhalten.[2351] Zudem machte sie einen Verstoss gegen das Recht auf ein faires Verfahren gemäss Art. 6 EMKR geltend. 1848

Der EGMR trat auf die Beschwerde ein und führte sie einem materiellen Entscheid zu – zugunsten der Beschwerdeführerin. Das Kernargument war dabei nicht materiell-inhaltlicher Natur: Es war die rechtliche Grundlage, die im schweizerischen Recht als ungenügend beurteilt wurde, um eine Observation durch einen Privatdetektiv zu legitimieren. Weil in der Schweiz keine hinreichende gesetzliche Grundlage für die geheime Observation im Versicherungskontext bestand, beurteilte der EGMR das Vorgehen der Versicherung im konkreten Fall als nicht rechtmässig und damit als Verstoss gegen Art. 8 EMRK.[2352] 1849

Es lohnt sich, den Entscheid und die Argumentation des EGMR zu beleuchten. Er ist zwar vielleicht (noch) keine *cause célèbre*. Dennoch kann er als Treiber für die Weiterentwicklung des Datenschutzrechts interpretiert werden. Das Urteil gibt Impulse, die sich gerade *nicht* darin erschöpfen, dass eine «präzise gesetzliche Grundlage» für die Observation im Versicherungskontext fehlte und geschaffen wird (resp. wurde).[2353] 1850

Selbstredend ging der EGMR davon aus, dass der Schutzbereich von Art. 8 EMRK betroffen sei. Nur deshalb aktualisierte sich eine Überprüfung der vorhandenen gesetzlichen Grundlage. Somit ist zunächst der Konkretisierung des Schutzgutes «Achtung des Privatlebens» gemäss Art. 8 EMRK durch den EGMR 1851

2350 Anzumerken bleibt, dass die Versicherung offensichtlich jede Beurteilung, die für eine Invalidität eintrat, als nicht anerkennungswürdig beurteilte. In diesem Zusammenhang ist auf die jüngste Thematisierung und Problematisierung von Gutachten im Zusammenhang mit Invaliditätsfällen hinzuweisen, die kaum je zugunsten der betroffenen Personen ausfallen, vgl. jüngst zu skandalösen IV-Gutachten: <https://www.blick.ch/news/politik/skandaloese-iv-gutachten-berset-kommt-in-der-sp-unter-druck-id15669522.html> (zuletzt besucht am 30. April 2021); bereits früher: <https://www.srf.ch/sendungen/kassensturz-espresso/themen/versicherungen/unfaire-iv-gutachter-in-der-kritik> (zuletzt besucht am 30. April 2021); <https://www.tagesanzeiger.ch/schweiz/standard/die-bevorzugten-gutachter/story/23064699> (zuletzt besucht am 30. April 2021); <https://www.nzz.ch/schweiz/der-weg-fuehrt-ueber-viele-gutachten-aber-nirgends-hin-ld.1367566> (zuletzt besucht am 30. April 2021).

2351 Zur erhöhten Bedeutung von Art. 8 EMRK auch in arbeitsrechtlichen Streitigkeiten Pärli, EuZA 2020, 224 ff.

2352 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 59 ff.

2353 Am 25. November 2018 wurde in der Volksabstimmung die gesetzliche Grundlage für die Überwachung von Versicherten angenommen: <https://www.admin.ch/gov/de/start/dokumentation/abstimmungen/20181125/uberwachung-versicherte.html>; vgl. <https://www.handelszeitung.ch/news/ab-oktober-sind-sozialdetektive-fur-versicherungen-im-einsatz> (zuletzt besucht am 30. April 2021).

Aufmerksamkeit zu schenken. Ein Blick auf die Argumentation des EGMR zeigt beachtliche Divergenzen gegenüber der Rechtslage in der Schweiz.

1852 Art. 8 EMRK verbürgt den Schutz auf Achtung des Privat- und Familienlebens. Wiederholt hatte sich der EGMR mit dem Schutzbereich von Art. 8 EMRK, allem voran im Zusammenhang mit medialen Berichterstattungen über Prominente, zu befassen.[2354] Doch welche Erwägungen finden sich zum Schutz des Privatlebens im vorliegenden Fall, der die geheime Observation durch einen Privatdetektiv im Versicherungskontext betrifft? Der EGMR hält im Entscheid V.-B. gegen die Schweiz fest:

> «The Court reiterates that „private life" within the meaning of Article 8 is a broad term not susceptible of exhaustive definition […].»[2355]

1853 Hervorzuheben ist, dass der EGMR über Art. 8 EMRK eine im *common law* etablierte Figur in den kontinentaleuropäischen Rechtskreis einführt. Es sind die *«reasonable expectations of privacy»*, die unter Art. 8 EMRK einschlägig seien.[2356] Die *«reasonable expectations of privacy»* lassen sich somit für die Weiterentwicklung des Datenschutzrechts reflektieren: Die Figur transportiere wie kaum eine andere eine Idee der *kontextuellen Integrität* in das Recht auf Privatheit und den Datenschutz.[2357]

1854 Der EGMR führte zu den *«reasonable expectations of privacy»* aus, dass der Gerichtshof primär das Folgende zu evaluieren habe: Entscheidend sei, ob eine Person vernünftigerweise dieselbe Privatheit, wie sie sie im privaten Raum geniessen könne, auch geniessen könne, während sie sich in der öffentlichen Sphäre bewege. Die vernünftigen Erwartungen betreffend die Privatheit wendet der EGMR ebenso im Zusammenhang mit arbeitsrechtlichen Konflikten und namentlich verdeckten Überwachungen an.[2358] Damit findet sich, wie es schon die Formulierung des «Privatlebens» als Schutzobjekt von Art. 8 EMRK indiziert, eine *Distanzierung* von einem lokal-sphärisch geprägten Schutzbereich statt. Das räumlich-statisch konzeptionierte Zweikammersystem von öffentlich versus privat wird über die Figur der *«reasonable expectations of privacy»* aufgebrochen.[2359] Mit der Formel wird der Fokus auf *Lebensbereiche* gerichtet. Hierbei können ein privater Lebensbereich resp. die private Lebensführung durchaus ebenso im öffentli-

2354 Hierzu Büchler, AcP 2006, 300 ff., 302 ff.; vgl. auch Hoppe, ZEuP 2005, 656 ff.
2355 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 52.
2356 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 48, E 54, E 107; vgl. mit Blick auf frühere Urteile m. w. H. Hoppe, ZEuP 2005, 656 ff., 662; vertiefend bereits zu dieser Figur im Zusammenhang mit dem Verarbeitungsgrundsatz von Treu und Glauben zweiter Teil, V. Kapitel, B.2.3.
2357 Hierzu Nissenbaum, 233 ff.
2358 Vertiefend hierzu Pärli, EuZA 2020, 224 ff., 228.
2359 Nissenbaum, 232, tritt dafür ein, sowohl den Dualismus von öffentlich versus privat als auch denjenigen von besonders schutzwürdigen versus gewöhnlichen Personenangaben als Konzepte des Privaten zu überwinden.

chen Raum stattfinden. Das private oder persönliche *Leben* ist eben kein *Raum*. Es erschöpft sich nicht in einer lokalen und analogen Fixierung innerhalb der eigenen vier Wände.[2360] Vielmehr geht es um eine *Lebensdimension* in verschiedenen Facetten. Über die vernünftigen Erwartungen von Privatheit entfaltet sich ein *variabler sowie facettenreicher Charakter des* Schutzbereiches *des Privatlebens*. Es wird als *Kategorie der Lebensführung resp. -gestaltung* verstanden, und zwar bezüglich persönlicher, individueller, aber auch familiärer Aspekte, Belange resp. Beziehungen, also sozialer Bezüge.[2361]

Einen Kernaspekt des Privatlebens bildet das *Führen von persönlichen Beziehungen*.[2362] Der Befund korreliert mit der Gesetzessystematik: Der Schutz des Privatlebens wird gemeinsam mit demjenigen des Familienlebens in Art. 8 EMRK verbürgt.[2363] Es geht unter Art. 8 EMRK ebenso um den Schutz persönlicher sowie familiärer Beziehungen und damit um einen *relationalen Aspekt*. Doch selbst darin erschöpft sich der Schutzbereich von Art. 8 EMRK nicht. 1855

Damit zusammenhängend, aber mit einer eigenständigen Dimension versehen, wird zudem im Rahmen von Art. 8 EMRK der Aspekt der *Identität und Persönlichkeit sowie der Autonomie und Selbstbestimmung* adressiert.[2364] Um die freie, autonome und persönliche Lebensführung und -gestaltung zu gewährleisten, ist ein Bereich (nicht beschränkt lokal-geografisch verstanden) anzuerkennen, innerhalb dessen Entscheidungsfreiheiten zu gewährleisten sind.[2365] 1856

Besagter Aspekt des Rechts auf autonome Entscheidungen bezüglich der eigenen Lebensführung wird eindrücklich anhand eines anderen Schweizer Urteils im Versicherungskontext sichtbar. Es handelt sich um das Helsana+-Urteil, BVGer A-3548/2018 vom 19. März 2019, das in Kürze im Sinne eines Einschubes erwähnt wird. Anhand des Falles zeigt sich zunächst, inwiefern autonome Entscheidungen über die persönliche Lebensführung – so das eigene Ess- und Trinkverhalten, Schlafgewohnheiten, Sportverhalten, Freizeitaktivitäten oder der Umgang mit Genussmitteln usf. – auch und gerade über das Datenschutzrecht gewährleistet werden sollen. Allerdings ist das Datenschutzrecht akzessorisch zu den jeweiligen Kontexten mit ihren rechtlichen Grundprinzipien und damit Logiken: Im konkreten Fall führte eine Praxis und Technik des Rapportierens von 1857

2360 Zu diesem Teilaspekt Schiedermair, 197 ff.

2361 Für eine Übersicht über die facettenreichen Schutzaspekte, die von Art. 8 EMRK erfasst werden, Gonin/Bigler, HK-EMRK/CEDH, Art. 8 EMRK, N 19 ff.; spezifisch zum Schutz des Privatlebens in der Öffentlichkeit Hoppe, ZEuP 2005, 656 ff.

2362 Vgl. m. w. H. BGE 133 I 58., E 6.1.

2363 Vgl. zur Auslegung von Art. 8 EMRK durch den EGMR Schiedermair, 171 ff. und 179 ff. zum Schutz des Familienlebens.

2364 Vgl. vertiefend Marsch, 7 ff.

2365 Den Wert des Privaten als Garant für das autonome Leben betonte insb. Rössler, 10 ff.; vgl. Gonin/Bigler, HK-EMRK/CEDH, Art. 8 EMRK, N 23, N 38, N 19; zum Schutzbereich gemäss EMRK auch Schiedermair, 165 ff.

sog. gesundheitsförderlichen Verhaltensweisen durch die Versicherten an eine Versicherung im Resultat dazu, dass indirekt die Prämien der Grundversicherung beeinflusst wurden. Dies führt zu einer Kollision mit Prinzipien der Grundversicherung. Namentlich zu nennen ist der Grundsatz der Einheitlichkeit der Prämie in der Grundversicherung. Die vom Bundesverwaltungsgericht zu beurteilende Technologie sowie Geschäftspraxis führten im Resultat zu einer *Erodierung dieses Grundprinzips*. Das Grundprinzip dient gerade auch dem Schutz eines Bereichs der persönlichen und freien Lebensführung. Ein unbeschränkt paternalistisches Regime, wonach nur gesund lebende Personen in den Genuss der Sozialversicherung gelangen, wird damit verworfen. Vielmehr werden in bestimmten Schranken auch Lebensführungen, die gesundheitsschädigend sind, hingenommen und als Ausdruck der Gewährleistung von Bereichen freier Lebensführung respektiert. Die Grundversicherung soll prinzipiell ungeachtet gewisser potentiell gesundheitsabträglicher Lebensentscheidungen und -weisen gewährleistet werden. Damit ist das Zusammenspiel und die Interdependenz zwischen Datenschutzrecht, Schutz des privaten Lebensbereiches zwecks Gewährleistung autonomer Lebensführung, aber auch Schutz von spezifischen Prinzipien der jeweils einschlägigen Kontexte umrissen. Im Ergebnis zeigt sich, dass das Datenschutzrecht die Kontexte absichert.

1858 Eine Gegenüberstellung der beiden Schweizer Fälle fördert eine gewisse Wertungsdivergenz zu Tage. In beiden Fällen standen datenschutzrechtliche Herausforderungen im Sozialversicherungskontext im Zentrum. Beide Fälle führen vor Augen, dass das Datenschutzrecht *kein isoliertes*, *kontextuell losgekoppeltes oder satellitenhaftes Rechtsgebiet* darstellt. Vielmehr ist es *akzessorisch zu den jeweils spezifischen Rechtsgebieten*, die ihrerseits *relativ zu etablierten Gesellschaftsbereichen* sind. Damit sind und werden sie von spezifischen Rationalitäten geprägt. Allerdings: Im Rahmen des Falles Helsana+ wird eine Entscheidung im Rahmen der persönlichen resp. privaten Lebensführung, z. B. die Bewegung an der frischen Luft bei einem Spaziergang, als gesundheitsfördernd beurteilt und positiv bewertet. Anders dagegen die Situation für eine Person, die medizinisch bedingt als arbeitsunfähig und in der Folge als IV-berechtigt gilt. Sie riskiert, infolge von Gängen und Tätigkeiten im öffentlichen Raum – einem Spaziergang, einem Einkauf, einem Treffen mit Freunden – wegen einer geheimen Observation als Versicherungsbetrügerin taxiert zu werden.

1859 Dass die Angelegenheit komplexer ist, liegt auf der Hand: Die Arbeit als Coiffeuse kann durchaus wegen einer medizinischen Beurteilung als nicht mehr möglich beurteilt werden. Sie geht mit hohen körperlichen Belastungen, vielen Stunden im Stehen, oftmals gebückt, und einer Arbeit einher, bei der man Chemikalien ausgesetzt ist. Dass ein Spaziergang, ein Einkauf oder ein Treffen mit Freunden in der Öffentlichkeit nur den Schluss legitimieren würde, dass jemand ein Versi-

cherungsbetrüger sei, geht fehl. Die folgende Analyse wird besser verständlich machen, was damit gemeint ist.

Insofern ist wiederum auf das Schutzobjekt gemäss EGMR und damit auf den hier primär interessierenden Fall der Versicherungsobservation zurückzukommen. Gezeigt wurde, dass der Schutzbereich von Art. 8 EMRK mehrere Teilelemente umfasst. Besonders hervorgehoben wurde *eine relationale Dimension* im Sinne der Gestaltung und des Führens persönlicher und familiärer Beziehungen. Zugleich wurde eine *individualistische Dimension* benannt mit Blick auf die Autonomie der individuellen Lebensführung in weiteren Bereichen. 1860

Eine Schnittmenge ist dahingehend auszumachen, dass persönliche Beziehungen auch der Bildung und dem Ausdruck der eigenen Identität dienen. Mit anderen Worten: Die Persönlichkeit und Identität eines Menschen wird von seinen Beziehungen mitkonstituiert. Dieser Aspekt realisiert sich keineswegs nur im «innerhäuslichen Bereich». Art. 8 EMRK schützt unter anderem ein Recht auf Identität, persönliche Entfaltung sowie auf Etablierung und Gestaltung von Beziehungen zu anderen Menschen und der Aussenwelt. Hierzu der EGMR im Entscheid V.-B. gegen die Schweiz und dem insofern bereits in früheren Entscheidungen herausgearbeiteten Gehalt von Art. 8 EMRK: 1861

> «There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of „private life" […]. The guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings. This may include activities of a professional or business nature and may be implicated in measures effected outside a person's home or private premises.»[2366]

Es ist folglich nicht ausgeschlossen, dass das Privatleben einer Person durch Massnahmen beeinträchtigt wird, die sich *ausserhalb ihres Hauses* vollziehen. Mit seinen Erwägungen arbeitet der EGMR die Relevanz des «Privatlebens» als *Lebensbereich und als Gesellschaftsbereich* heraus. Dieses kann auch in der «Aussenwelt», im öffentlichen Raum stattfinden. 1862

Die vernünftigen Erwartungen einer Person hinsichtlich ihres Privatlebens seien ein wesentlicher, nicht aber exklusiver Faktor zur Beurteilung eines Sachverhalts im Lichte von Art. 8 EMRK.[2367] Weitere Elemente seien zur Beurteilung der Rechtmässigkeit eines Monitorings im öffentlichen Raum unter Einsatz von Foto- und Videoaufnahmen einschlägig, z. B., ob es sich um eine Kompilation von Angaben zu einer bestimmten Person handle, ob es personenbezogene Angaben seien und/oder ob die Informationen in einem Ausmass «jenseits des normalerweise Voraussehbaren» weiterverbreitet werden. 1863

2366 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 52 f.
2367 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 54.

1864 Im zu beurteilenden Fall wurde die Beschwerdeführerin systematisch und bewusst während mehrerer Tage über jeweils mehrere Stunden hinweg durch einen Privatdetektiv beobachtet und gefilmt. Das im Rahmen der geheimen Observation gesammelte Material wurde gespeichert, selektiert sowie ausgewertet und verwertet, indem gestützt darauf eine (Re-)Evaluation des Gesundheitszustandes der Beschwerdeführerin vorgenommen wurde und die Ergebnisse in der Folge im Versicherungsstreit weiterverwendet wurden. Besagte Vorgehensweise beurteilte der EGMR als Beeinträchtigung des Anspruchs auf Achtung des Privatlebens i. S. v. Art. 8 EMRK. Sie bedürfe einer entsprechenden *Rechtfertigung resp. Legitimation*.[2368]

1865 In diesem Zusammenhang hatte die Beschwerdeführerin die *ungenügend konkrete gesetzliche Grundlage im schweizerischen Recht* vorgebracht. Die geheime Observation sei ebenso wenig voraussehbar gewesen. Weiter warf die Beschwerdeführerin (m. E. zu Recht) die Frage auf, ob eine geheime Observation bei inkonsistenten Arztgutachten überhaupt zugelassen werden solle.[2369] Eine medizinal-gutachterliche Inkonsistenz – so die Argumentationsrichtung – wäre dann dem Verantwortungsbereich der Versicherung zuzuweisen. Sie sei es, welche die zuständigen und kompetenten Ärzte beauftrage.

1866 Die Gegenpartei vertrat den Standpunkt, dass die gesetzliche Grundlage gegeben sei.[2370] Ein Eingriff in Gestalt der geheimen Observation erfolge, wie es bereits das Bundesgericht befunden hatte, sehr selten. Die geheime Observation werde als *ultima ratio* vorgenommen und betreffe wenige Personen. Zudem sei zu berücksichtigen, dass die Beschwerdeführerin ihren Mitwirkungspflichten nicht nachgekommen sei. Die Überwachung sei, weil im öffentlichen Raum und auf bestimmte Zeitfenster limitiert, gerechtfertigt gewesen. Mit ihr würde ein der Versicherung auferlegter Zweck – Invaliditätsleistungen nur dann zu erbringen, wenn diese auch geboten und geschuldet seien – erfüllt.[2371]

1867 Der EGMR hielt vorab fest, dass er wiederholt auf die zentrale Bedeutung der «Voraussehbarkeit» im Kontext der geheimen Überwachung hingewiesen habe.[2372] Damit sei nicht gemeint, dass ein Individuum im konkreten Fall eine Überwachung voraussehen müsse, um in der Folge ihr Verhalten anpassen zu können. Vielmehr liege das Risiko geheimer Überwachung im *willkürlichen Handeln*. Die Überwachungsmethoden würden dank neuer Technologien immer sophistizierter. Es gehe darum, anhand der hinreichend konkreten Gesetzesgrundlage den Men-

2368 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 59.
2369 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 61 ff.
2370 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 64 ff.
2371 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 64.
2372 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 67.

schen angemessene Indikatoren sowohl mit Blick auf die Umstände als auch die Bedingungen, unter denen die Observation eingesetzt werden dürfe, zu geben.[2373]

Für den konkreten Fall äusserte sich der Gerichtshof zur Voraussehbarkeit dahingehend, dass das eidgenössische Recht keinerlei spezifische Vorgaben für die geheime Observation im *Kontext von Versicherungsstreitigkeiten* vorsehe.[2374] Von Gesetzes wegen greife kein zeitliches Limit für Überwachungsmassnahmen. Damit kämen den Versicherungen, die im Rahmen der obligatorischen Versicherung öffentliche Aufgaben wahrnehmen, beträchtliche Ermessensspielräume zu. Solch weite Ermessensspielräume bestünden weiter infolge der fehlenden konkreten gesetzlichen Vorgaben zu Speicherung, Auswertung, Zugang und Zerstörung der Überwachungsergebnisse. Folglich müsse das Vorliegen einer hinreichend konkreten Gesetzesgrundlage verneint werden.[2375] Hieran ändere auch der Einwand der Beschwerdegegnerin nichts, wonach der Eingriff relativ gering sei im Verhältnis zu dem von der Versicherung verfolgten Interesse, einen Versicherungsbetrug aufzudecken. Letzten Endes ginge es darum, öffentliche Gelder korrekt zu verwalten, was bei der Beurteilung der hinreichend konkreten gesetzlichen Grundlage zu berücksichtigen sei.[2376] Der EGMR befand zwar, dass der Eingriff geringer sei als beispielsweise derjenige bei Telefonabhörungen. Gleichwohl aber genüge die *gesetzliche Grundlage* in der Schweiz für die geheime Observation im Versicherungskontext *nicht*; namentlich würden keine hinreichenden Garantien vorgesehen, die einen Missbrauch verhindern würden.[2377] 1868

Hinsichtlich der (un-)genügenden gesetzlichen Grundlage sei im Sinne eines Einschubes in Erinnerung zu rufen, dass im EU-Raum und basierend auf der DSGVO die Anforderungen an die gesetzlichen Grundlagen höher sind als das bislang für die Schweiz vertreten wurde.[2378] 1869

Der EGMR kam in der Folge, anders als das Urteil des schweizerischen Bundesgerichts, zu dem Schluss, dass die *Überwachung unrechtmässig* war. Die Urteilsfindungen unterscheiden sich zunächst in der Argumentation betreffend den grundrechtlichen Schutzbereich: Während das Bundesgericht sich mit Blick auf das Schutzobjekt auf die überholte Sphärentheorie stützt, weisen die Ausführungen zum Schutzgehalt des Privatlebens gemäss Art. 8 EMRK auf andere Bezugspunkte hin. Es geht um den Schutz einer «persönlichen Zone», namentlich um persönliche Beziehungen zu führen, was zugleich Ausdruck autonomen Handelns sowie Element der Identität sei. Dabei könnten die individuelle Beziehungspflege 1870

2373 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 70 ff.
2374 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 74.
2375 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 72 ff.
2376 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 76.
2377 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 76.
2378 Insofern wird auch eine Differenz zwischen der schweizerischen Konzeption gegenüber derjenigen im europäischen Raum sichtbar, auch mit Blick auf das Schutzniveau im Datenschutz.

und ein individuelles Verhalten im sog. öffentlichen Raum ebenso vom Schutzbereich des Privatlebens erfasst sein. Anders verharrte das Schweizer Bundesgericht in seinem Entscheid der statisch-räumlichen und dichotomen Konzeptionierung, obschon es in anderen Urteilen von der Verbürgung eines Rechts auf informationelle Selbstbestimmung im Sinne eines Herrschaftsrechts schreibt. Beides entspricht nicht den Ansätzen des EGMR gemäss Art. 8 EMRK. Der Gerichtshof rückt die *«reasonable expectations of privacy»* und die Bedeutung individueller Beziehungsführung sowie die Elemente von Identität sowie Autonomie unter dem Schutzobjekt des Privatlebens in den Vordergrund. Seine Erwägungen basieren weder auf einer räumlich verstandenen Zweiteilung des öffentlichen gegenüber dem privaten Raum noch auf einem Recht auf informationelle Selbstbestimmung oder einem Herrschaftsrecht an Personendaten.

1871 Dessen ungeachtet: *Beide Urteile bilden die Herausforderungen der Praxis von geheimen Versicherungsobservationen aus einer erweiterten Datenschutzperspektive nicht ab*. In der Argumentation des EGMR zum Schutzbereich lassen sich Richtungshinweise finden, die einer genaueren Analyse unterzogen werden sollen. Es geht um die Erwägungen zu den Auswirkungen, welche die geheime Observation – über die Einzelfallbetrachtung hinaus – zeitigt. Zentrale Bedeutung gewinnen hier die auf dem Spiel stehenden *gesellschaftlichen Bereiche*. Die Auswirkungen der Praxis erschöpfen sich keineswegs in den Observationen im Einzelfall. Sie sind weit- und tiefgreifender.

1872 Die Praxis wird nunmehr von einer anderen datenschutzrechtlichen Perspektive aus betrachtet. Sie soll nicht aus der traditionellen Sichtweise behandelt werden, wonach die Relevanz des Datenschutzrechts erst mit der Verletzungshandlung der Rechtsposition des konkreten Datensubjektes und Individuums getriggert wird. Hierzu die *These:* Die *Praxis strapaziert bereits aufgrund ihrer abstrakten Möglichkeit die Integrität verschiedener Gesellschaftsbereiche*. Die enge Linse eines isoliert individualrechtlich gedachten Datenschutzrechts verkennt dies. Nachfolgend wird anhand der Praxis der geheimen Observation im Versicherungskontext ein *neues Paradigma* für das Datenschutzrecht der Zukunft elaboriert. Damit wird verdichtet, was im Laufe dieser Schrift an verschiedenen Stellen sichtbar wurde: warum, inwiefern und wie datenschutzrechtliche Aufgaben resp. Schutzziele neu zu erfassen sind, wobei Herausforderungen einzig unter Anerkennung der facettenreichen sowie komplexen Schutzdimensionen bewältigt werden.

1.2.3. Produktiver Konflikt (1) – Indizien für kollektive Dimensionen

1873 Der EGMR anerkannte, dass das Recht auf Achtung des Privatlebens auch im öffentlichen Raum verletzt werden kann. Er machte die ungenügende gesetzliche Grundlage in der Schweiz zum Schlüsselelement seines Verdikts. Hieraus könnte

geschlussfolgert werden, dass mit der Schaffung einer Gesetzesgrundlage, die hinreichende Garantien gegen Missbräuche vorsieht, das Thema der geheimen Observation im Versicherungskontext mit dem Plazet des EGMR rechtschaffen *ad acta* gelegt werden könnte.

Dies scheint die Schweiz zu intendieren: Sie setzte nach der Verurteilung durch den EGMR ihre Gesetzgebungsmaschinerie in Gang, um die geforderte hinreichend konkrete *gesetzliche Grundlage* zu schaffen.[2379] In der Volksabstimmung vom 25. November 2018 wurde eine Gesetzesgrundlage zwecks Überwachung von Versicherten gebilligt; sie ist per 1. Oktober 2019 in Kraft.[2380] 1874

Allerdings gibt es – gerade in Kenntnis der *Affäre V.-B.*, in ihrer Gesamtheit betrachtet – *robuste Argumente, die Frage umzuformulieren, oder genauer, grundsätzlicher zu stellen:* Soll eine verdeckte, systematische Ausforschung der persönlichen Lebensführung, also des Privatlebens (selbst wenn sich dieses im öffentlichen Raum abspielt), über längere Zeiträume und unter Einsatz von Aufnahmetechnologien zulässig sein, mit dem Zweck, potentielle Fälle von Versicherungsbetrug aufzudecken oder Unschärfen medizinischer Einschätzungen auszumerzen? Welche *Auswirkungen* hat die Zulassung entsprechender Personendatenverarbeitungen über die Durchführung im konkreten Einzelfall hinausgehend – selbst wenn sie durch eine gesetzliche Grundlage legitimiert wird? Die Fragen zielen auf eine vertiefte und zugleich erweiterte Analyse der «materiellen», der inhaltlichen Konsequenzen entsprechender formell zugelassener Personendatenverarbeitungen. Es geht um eine Betrachtungsweise, welche die Problematik über das einzelne Subjekt hinausgehend anerkennt. Es geht damit auch um die Frage des *Datenschutzrechts de lege ferenda.* 1875

Es sind nicht nur Erkenntnisse, die im Laufe dieser Arbeit erschlossen wurden, die Anlass dazu geben, die Herausforderung der beschriebenen Praxis einer inhaltlichen Re-Evaluation zu unterziehen und anhand des beschriebenen Konflikts produktive Impulse für das Datenschutzrecht zu generieren. Grund dazu gibt das fortdauernde gesellschaftliche Unbehagen gegenüber der Praxis.[2381] Das gesellschaftliche Unbehagen dient Nissenbaum als Seismograf resp. Indikator des 1876

2379 Vgl. NZZ vom 19. November 2018 unter dem Titel «Frau V. und die Versicherungsschnüffler», abrufbar unter: <https://www.nzz.ch/schweiz/frau-v-und-die-versicherungsschnueffler-ld.1436236?reduced=true> (zuletzt besucht am 30. April 2021).

2380 Vgl. <https://www.admin.ch/gov/de/start/dokumentation/abstimmungen.html> (zuletzt besucht am 30. April 2021); vgl. Handelszeitung online, ab Oktober sind Sozialdetektive für Versicherungen im Einsatz, Zürich 2019, <https://www.handelszeitung.ch/news/ab-oktober-sind-sozialdetektive-fur-versicherungen-im-einsatz> (zuletzt besucht am 30. April 2021).

2381 Zu solchen gesellschaftlichen Widerständen als datenschützerisches und datenschutzrechtliches Metrum Nissenbaum, 3, 142, 158, 181 ff., 186 ff., 235; auch im Titel eines NZZ-Beitrages, der über diese jüngsten Entwicklungen berichtet, klingt mit den Worten «Detektive sollen legal werden» zumindest Ambivalenz an, <https://www.nzz.ch/schweiz/sozialbetrug-observationen-kuenftig-zulassen-ld.125694> (zuletzt besucht am 30. April 2021); jüngst kritisch auch ein Anwalt <https://www.srf.ch/news/schweiz/ueberwachung-von-versicherten-mehr-als-die-polizei-erlaubt> (zuletzt besucht am

Datenschutzes. Damit beschäftigen sich die nächsten Seiten für die hier gewählte Fallkonstellation.

1877 Der Praxis wurde sowohl im Vorfeld der Volksabstimmung als auch nach der positiven Volksabstimmung zur Schaffung einer gesetzlichen Grundlage kritisch begegnet.[2382] Dass die geheime Observation im Versicherungskontext als neuralgisch beurteilt wird, zeigt vorab eine bemerkenswerte Entwicklung im Zuge der Gesetzgebungsarbeiten: Im Rahmen des Gesetzgebungsprozesses wurde die Einführung einer weiteren Hürde für die geheime Observation diskutiert. Eine solche sollte nur dann zulässig sein, wenn ein Gericht eine Observation zugelassen hätte.[2383] Es scheint so, als ob Restzweifel betreffend die Legitimität der Praxis geheimer Observation fortbestünden. Die Schaffung einer hinreichenden gesetzlichen Grundlage gilt nicht *uni sono* als Gestaltungs- und Sicherungsinstrument, um die Massnahme als angemessen zu beurteilen.

1878 Pointiert zur gesetzlichen Grundlage als Fluch oder Segen resp. als illegitimes Legitimationsinstrument hatte sich in anderem Zusammenhang bereits Eugen Bucher geäussert. In seinem Beitrag unter dem Titel «Das Horror-Konstrukt der «Zwangsmedikation»: zweimal (ohne Zuständigkeit) ein Ausflug ins juristische Nirwana» führt Bucher scharfsinnig aus:

> «Näheres Zusehen wird weder Bösewichter noch Polizisten sichtbar machen, wohl aber andere Schrecken zutage fördern: Für Anwendung von Zwang fordert das Gericht mit Persistenz eine «gesetzliche Grundlage». Wenn aber Zwang gleichzeitig als Zufügen von Ungemach, ja von Plagen oder gar als Quälerei verstanden (und zum Überfluss gar in die Nähe der Folter gerückt) wird und die Grundaussage des hohen Gerichts auf die Formel hinausläuft: «Quälen (nur, aber immerhin) mit gesetzlicher Grundlage zulässig», hört die Gemütlichkeit auf: Irgendetwas stimmt da nicht mehr.»[2384]

1879 Die *gesellschaftlichen Reaktionen* gegenüber bestimmten Personendatenverarbeitungspraktiken sowie -technologien erfüllen – erstens – in der bahnbrechenden Theorie Nissenbaums eine Schlüsselfunktion. Vehementer Widerstand resp. breit angelegte Billigung gegenüber bestimmten Personendatenverarbeitungsprozessen dienen Nissenbaum als *Indikator und Detektor,* um ihre Theorie der «Privacy in Context» *zu begründen und inhaltlich zu konkretisieren.*[2385]

1880 Der Ansatz von Nissenbaum geht – zweitens – davon aus, dass es beim Schutz des Privaten um die *Gestaltung und Gewährleistung angemessener Datenflüsse*

30. April 2021); kritisch weiter <https://www.blick.ch/meinung/das-meint-sonntagsblick-detektiv-spielen-ist-sache-der-polizei-id15011593.html> (zuletzt besucht am 30. April 2021).

2382 Vgl. vonseiten der Rechtswissenschaften auch Pärli, recht 2018, 120 ff., dessen Aufsatz den aussagestarken Titel «Observation von Versicherten – Der Gesetzgeber auf Abwegen» trägt.

2383 Observation mit zusätzlicher Hürde: Observiert wird nur, wenn es der Richter erlaubt, NZZ vom Samstag, 27. Januar 2018.

2384 Bucher, ZBJV 2001, 764 ff., 764.

2385 Nissenbaum, 3, 142, 158, 181 ff., 186 ff., 235; vgl. den Hinweis, wonach sich der Wert von Personendaten nur anhand ihres Kontextes bestimmen lässt, bei Karg, digma 2011, 146 ff., 148 ff.

zwischen verschiedenen Kontexten geht.[2386] Damit wird eine Neukonzeptionierung für das Datenschutzrecht zur Debatte gestellt, das noch heute – wenn auch mit den jüngsten Rechtsneuerungen nicht mehr exklusiv – auf dem Axiom des Persönlichkeitsschutzes basiert. Datenflüsse können sehr unterschiedlich gestaltet werden: vom freien Fluss über die Blockierung mittels Geheimhaltungspflichten bis hin zu mehr oder minder weit geöffneten oder geschlossenen Schleusen. Es geht um die Differenzierung der Vorgaben dafür, wie die Datenflüsse gestaltet werden sollen. Ein «Ja» oder «Nein» in Bezug auf die Zulassung oder Unterbindung von Datenflüssen genügt nicht; es gibt nicht nur ein «Alles oder Nichts». Unbeschränkte Flüsse oder Blockaden in Gestalt von Geheimhaltungspflichten sind lediglich die beiden «radikalen Lösungen». Dazwischen gibt es ausdifferenzierte Gestaltungsmöglichkeiten für Personendatenflüsse. Diese haben sich am Persönlichkeitsschutz, zudem aber am Systemschutz zu orientieren: Es geht datenschutzrechtlich stets um die Frage, «wie» Personendatenflüsse gestaltet werden sollen – nicht nur zum Schutz der Persönlichkeit des Datensubjektes, sondern auch zum Schutz der Integrität involvierter Kontexte. Von besonderem Interesse ist die Gestaltung der Datenflüsse zwischen verschiedenen Bereichen. Exemplarisch ist insofern, dass seit jeher Zugriffsbegehrlichkeiten des Staates auf im privaten Kontext gesammelte Daten (und umgekehrt) kritisch diskutiert werden

Für das datenschutzrechtliche Kontextparadigma ist – drittens – entscheidend, 1881
dass nicht nur Interessen des einzelnen Datensubjektes geschützt werden. Das Axiom des Subjekt- und Persönlichkeitsschutzes wird dabei nicht aufgegeben. Vielmehr hat das Datenschutzrecht darüber hinaus Gesellschaftsbereiche mit ihren jeweiligen Zielsetzungen, Prinzipien, Zwecken und Logiken abzusichern.[2387] Schutzzweck resp. Schutzobjekt des Datenschutzrechts ist ebenso die Garantie von kontextrelativen Zielen und Werten.[2388] Die Relevanz des Datenschutzrechts geht weit über den Individualgüterrechtsschutz hinaus. Das *Datenschutzrecht ist ein hoch bedeutsamer Garant zum Schutz von etablierten sowie tragenden Institutionen und Kontexten der Gesellschaft*. Letztere verleihen Gesellschaften Robustheit und Widerstandskraft. Vielleicht liegt genau in dieser systemischen Schutzdimension die Erklärung begründet, wonach gewisse Datenschutzverletzungen breit angelegtes und vehementes gesellschaftliches Empören auslösen. Der in dieser Arbeit thematisierte Facebook-Skandal, bei dem es letztlich um die Erodierung der Demokratie geht, ist insofern illustrativ. Es geht nicht nur um das Problem, dass über illegitime Personendatenverarbeitungen

2386 Vgl. Nissenbaum, 2, 231 ff.; Dies., Sci. Eng. Ethics 2018, 831 ff.
2387 Dies., 32 ff., 38 ff., 132 ff., 180 ff., Dies., in: Heinrich-Böll-Stiftung (Hrsg.), 53 ff., 60 ff.
2388 Vgl. weiter auch Nissenbaum, Sci. Eng. Ethics 2018, 831 ff., 849.

unter Umständen einzelne Menschen manipuliert wurden. Besagte illegitime und kontextfremde Verarbeitungshandlungen strapazieren die Demokratie.

1882 Die Eckpfeiler eines Rechts auf informationellen Systemschutz sollen anhand der Praxis der geheimen Observation im Versicherungskontext herausgearbeitet, illustriert und erhärtet werden. Dies geschieht in Anlehnung an die Theorie von «Privacy in Context», wie sie Nissenbaum entwickelt hat.

1883 Zur *Herleitung eines datenschutzrechtlichen Paradigmenwechsels* ist einleitend eine Textpassage aus der Zeitung aufschlussreich:

> «99 Mal hat die Versicherungsstelle der IV 2013 eine Verdachtsmeldung erhalten. Diese Fälle zu beurteilen ist nicht immer einfach, denn in manchen Fällen zeigen die Krankenakten einen anderen Sachverhalt auf als das Verhalten der Verdächtigten. Beim zweiten Versuch hätte er sich seine IV-Rente fast erschlichen. Zwei Psychiater glaubten dem ehemaligen Giesser, als er ihnen von seinem eigenbrötlerischen Leben erzählte – ein Alltag, angeblich ohne menschliche Kontakte. Sie bezeugten dem 50-jährigen Schweizer Ende August 2010 volle Arbeitsunfähigkeit […]. Nur eine anonyme Anzeige verhinderte den Betrug, der sich anbahnte. Die IV schickte den Sozialdetektiv los und liess den Mann während zweier Monate überwachen. Was der Detektiv sah, widersprach den Gutachten. Die Observation zeigte einen geselligen Menschen, der Kontakte pflegte, ohne dabei in erkennbarer Weise durch Schmerzen behindert zu werden. […] „Den wirklich psychisch Kranken hat der Mann einen Bärendienst erwiesen. Solche Fälle fördern einen Generalverdacht", so der IV-Chef. „Ein Sozialdetektiv soll nicht normal sein", sagt Gabl. „Die Anzahl der Betrüger ist gering. Aber ein Betrugsfall kostet schnell sehr viel."»[2389]

1884 Die mediale Berichterstattung ist indikativ. Sie deutet an, inwiefern die Praxis geheimer Observation *nicht nur die im einzelnen Fall betroffene Person tangiert*. Vielmehr geraten ein ganzes Kollektiv und damit in der Folge ganze gesellschaftliche Kontexte unter Druck.

1885 In diese Richtung ebenfalls aufschlussreich sind mediale Stellungnahmen vonseiten des Gesundheitspersonals: Im Zuge der Volksabstimmung zum neuen Gesetz zur Versicherungsobservation wies eine Psychiaterin darauf hin, dass die *Angst vor Überwachung Kranke kränker mache*. Zudem seien die Bild- und Tonbandaufnahmen aus dem Bereich der persönlichen Lebensführung wenig aussagekräftig, sofern diese Beobachtungen nicht in den medizinischen Kontext gesetzt würden.[2390]

2389 Vgl. Fluri, Solothurner Zeitung vom 15. Februar 2014, Missbrauch, Um manche IV-Betrüger zu entlarven, braucht es die Hilfe eines Sozialdetektivs, <https://www.solothurnerzeitung.ch/solothurn/kanton-solothurn/um-manche-iv-betrueger-zu-entlarven-braucht-es-die-hilfe-eines-sozialdetektivs-127672084> (zuletzt besucht am 30. April 2021).

2390 Vgl. Cerletti, Blick vom 10. November 2018; vgl. auch Chappuis/Hardegger, HAVE 2018, 204 f., welche die verschiedenen Standpunkte darlegen und von einem kontrastreichen Bild betreffend die Ansichten sprechen, die zu dieser Praxis sowie der gesetzlichen Grundlage vertreten werden.

Rechtswissenschaftlich hat sich namentlich Pärli kritisch mit dem neuen Gesetzesartikel sowie der Praxis auseinandergesetzt.[2391] Der Experte für soziales Privatrecht sowie Datenschutzrecht beschränkt sich nicht darauf, die fehlenden Schranken und (zu) weitreichenden Kompetenzen, die den Sozialversicherungsträgern mit dem zur Abstimmung gebrachten Gesetzesentwurf bei der Observation eingeräumt würden, zu problematisieren. Vielmehr führt die Argumentation von Pärli die Notwendigkeit, kontextuelle Erwägungen zu integrieren, vor Augen. Der Autor hält zunächst fest: 1886

> «Sozialversicherungsmissbrauch ist nach Art. 148a Strafgesetzbuch (StGB) strafbar. Für die Strafverfolgung sind die entsprechenden Strafrechtsbehörden zuständig.»[2392]

Die Aufdeckung von Sozialversicherungsbetrug ist Aufgabe der Strafverfolgungsbehörde. Sie soll nicht in den Händen der Versicherungsgesellschaften sowie den von ihnen entsandten Privatdetektiven liegen. Weiter die Argumentation von Pärli: 1887

> «Die nun gesetzlich erlaubten Überwachungsmöglichkeiten durch die Sozialversicherungen stellen sämtliche Bezüger/innen von Leistungen unter Generalverdacht des Missbrauchs, und sie fördern eine gegenseitige Misstrauenskultur. Es ist in Erinnerung zu rufen, wofür Sozialversicherungen da sind: Sie dienen der Absicherung wirtschaftlicher Folgen elementarer Lebensrisiken wie Krankheit, Unfall, Invalidität oder Arbeitslosigkeit. Die Versicherten leisten auf der Grundlage ihres Erwerbseinkommens nicht unerhebliche Beiträge an die Finanzierung dieser Sozialwerke. Wie soll die versicherte Person bei Eintritt eines versicherten Risikos den Sozialversicherungsbehörden vertrauen können, wenn diese aufgrund dieses Gesetzes auf blossen Verdacht eines unrechtmässigen Leistungsbezuges hin eine Überwachung in die Wege leiten dürfen? Der Sozialstaatsgedanke wird so mit Füssen getreten.»[2393]

Damit ist das Feld abgesteckt, um den *Ansatz des Rechts auf informationellen Systemschutz* anhand des gewählten Falles zu veranschaulichen. Das neue Systemparadigma geht davon aus, dass sich Aufgabe und Regelungszweck des Datenschutzrechts nicht im Schutz des Individuums und damit Subjektparadigma erschöpfen. Die nun anschliessende Herleitung wählt eine *Stufenfolge*: Ausgehend von der Beschreibung der individualrechtlichen Konfliktlage wird die dahinterliegende kontextuelle und systemische Dimension des Rechtskonfliktes freigelegt. 1888

1.2.4. Produktiver Konflikt (2) – Matrix der Konfliktlagen

Ein Konflikt, wie ihn ein Gerichtsfall nachzeichnet und entscheidet, zeigt sich typischerweise als Rechtsstreit im *Zweiparteienverhältnis*. Zudem entscheiden Ge- 1889

2391 Vgl. Pärli, recht 2018, 120 ff.
2392 Ders., a. a. O., 120 ff., 121.
2393 Ders., a. a. O., 120 ff., 122.

richte konkrete Fälle und damit spezifische Konflikte *de lege lata*. Im Zentrum der Urteile des Bundesgerichts sowie des EGMR standen die Fragen, ob die konkret durchgeführte geheime Observation durch einen Privatdetektiv, eingesetzt von der Versicherung, Grundrechte der Versicherungsnehmerin tangierte resp. verletzte und ob eine allfällige Verletzung legitimiert war. Das Bundesgericht fällte sein Diktum bereits auf der Stufe des Schutzobjektes zugunsten der Versicherung: Die Privatsphäre sei in der öffentlichen Sphäre durch die Observation nicht tangiert resp. verletzt. Anders der EGMR: Das Schutzobjekt von Art. 8 EGMR sei tangiert, ein Privatleben sei ebenso im sog. öffentlichen Raum geschützt. Die Schweiz, so der EGMR, weise keine hinreichende gesetzliche Grundlage für die geheime Observation im Versicherungskontext vor. Der EGMR entschied damit zugunsten der Versicherten V.-B.

1890 Für die Gerichte stand der Schutzbereich des Privatlebens resp. der Privatsphäre und hieran anknüpfend die Rolle von V.-B. als Privatperson im Vordergrund: Das Bundesgericht beurteilte unter Anwendung der «Sphärentheorie» die erfolgten Beobachtungen im öffentlichen Raum mit Blick auf Schutzobjekt, Schwere des Eingriffs, gesetzliche Grundlage und Verhältnismässigkeit als rechtens. Dagegen befand der EGMR, dass vom Recht auf «Achtung des Privatlebens» i. S. v. Art. 8 EMRK ein Verhalten erfasst sein könne, das sich im öffentlichen Bereich zutrage. Dies, sofern «*reasonable expectations of privacy*» hierfür sprechen. Der EGMR führte aus, dass es mit dem Schutz des Privatlebens im Wesentlichen um die Garantie von *Autonomie*, selbstbestimmter Lebensführung, Identität sowie persönlicher Beziehungsgestaltung gehe. Der Zusammenhang zwischen dem Schutz des Privaten und der Autonomie wurde, wie gezeigt, namentlich von Rössler in ihrer Schrift «Vom Wert des Privaten» dargelegt.[2394]

1891 Im hier interessierenden Fall war die Gegenpartei eine *Versicherungsgesellschaft*, die Suva, die im Bereich der IV-Leistungen öffentliche Aufgaben wahrnimmt. Die schweizerische Unfallversicherung Suva ist ein bedeutsamer Teil des schweizerischen Sozialversicherungssystems. Sie versichert als selbstständiges Unternehmen des öffentlichen Rechts Menschen im Beruf und in der Freizeit.[2395]

2394 Ihre Analyse ist stark staatstheoretisch, vom liberalen sowie demokratischen Bezug und einer individualistischen Perspektive geprägt: «Ich denke, dass die plausibelste Theorie zum Wert des Privaten, und damit auch über den Wert informationeller Privatheit, diesen Wert bestimmt durch den Zusammenhang zwischen Privatheit und individueller Freiheit oder Autonomie», Rössler, 136 ff.; das Zusammenspiel zwischen Privatheit, individueller Freiheit, Selbstbestimmung resp. Autonomie und dem, was der EGMR als «Identität und persönliche Entfaltung» als Element von Art. 8 EMRK einfängt, beschreibt die Philosophin wie folgt: «[…] Privatheit [wird] in liberalen Gesellschaften auch geschätzt und gebraucht […], um der individuellen Freiheit und Autonomie willen; und zwar um der Freiheit vor Eingriffen des Staates oder anderer Personen willen wie um der Freiheit zur Ausbildung eines «Lebensplans», der Freiheit zur je individuellen Selbstverwirklichung», vgl. Rössler, 84; zur Identität als Schutzelement nach Art. 8 EMRK Paefgen, 33 ff.; zur Komplexität des Begriffs der Identität allgemeiner Mallmann, 47.

2395 Vgl. insofern die Homepage zur Suva.

In dem Moment, in dem nun diese Gegenpartei, die Versicherung, ebenso in den Blick genommen wird, verändert sich das Bild: Es ist nicht mehr nur der die Observation durchführende Detektiv, der mit dem privaten Lebensbereich der V.-B. interferiert. Vielmehr zeigt sich mit der Versicherungsgesellschaft als Agentin im Konflikt die Rolle von V.-B. als *Versicherte resp. IV-Versicherungsbezügerin deutlich*. Sie ist nicht nur Datensubjekt resp. eine Person, in deren privaten Lebensbereich durch eine Informationsverarbeitung eingegriffen wurde. Der Konflikt spielt sich im *Versicherungskontext* ab. 1892

Allerdings vereinen sich im Rahmen des Konfliktes in der Person von V.-B. *mehrere Rollen*, die für den Rechtsfall relevant sind: V.-B. ist geheim überwachtes Datensubjekt; sie ist eine Person mit privatem Lebensbereich; sie ist IV-Leistungsbezügerin und damit eng zusammenhängend ist sie ebenso eine ehemalige Berufsfrau. Es handelt sich um eine Friseurin, die infolge eines Verkehrsunfalles und der damit einhergehenden Gesundheitsbeeinträchtigungen arbeits- resp. erwerbsunfähig und daraufhin IV-Bezügerin wurde. Die Feststellung dieser verschiedenen Rollen ist auch für eine datenschutzrechtliche Studie relevant. 1893

Um ein künftig schutzzieleffektives und tragfähiges Datenschutzrecht zu konzipieren, *genügt die Adressierung des Datensubjektes als quasi-einheitliches Subjekt nicht*. Die (datenschutz-)rechtliche Problematik und Herausforderung beschränkt sich nicht darauf, einzig und allein eine konkrete Person in ihrer Rolle als «Datensubjekt» zu beachten. Ebenso wenig genügt es, konkret durchgeführte Handlungen zu betrachten, welche in die Privatsphäre resp. das Privatleben eingreifen. Vielmehr sind zusätzliche Dimensionen miteinzubeziehen. 1894

Den Ausgangspunkt für die Analyse und damit die Entfaltung der Matrix bildet die Anerkennung der *pluralen Rollen von V.-B.* Die Erfassung der Herausforderung gelingt nicht, wenn V.-B. nur in ihrer Rolle als «Datensubjekt» oder «Observierte», als «Klägerin» oder «Beschwerdeführerin» betrachtet wird. Vielmehr liegt der Akzent auf ihrer Rolle als *Versicherte*. 1895

Der *Versicherungskontext* mit den Rollen der involvierten Person als Versicherungsnehmerin und Versicherungsbezügerin auf der einen Seite und der Versicherung auf der anderen Seite ist für die Erfassung der datenschutzrechtlichen Herausforderung entscheidend. Die konsequente Anerkennung der Akzessorietät des Datenschutzrechts zu den jeweils einbettenden Kontexten – so die in dieser Studie vertretene These – wird als Hauptstrategie zur Rekonzeptionalisierung des Datenschutzrechts der Zukunft vorgeschlagen. Es gilt, Datenschutzrecht nicht mehr isoliert als Thema des deliktsrechtlichen Persönlichkeitsschutzes (abgeschwächt mit den jüngsten Rechtsneuerungen) resp. Subjektschutzes zu lesen. Eine Konzeptionierung der Materie als quasi eigenständiges, losgelöstes Quer- 1896

schnittsthema ist zu überwinden. Das datenschutzrechtliche Systemparadigma inkludiert seinerseits das Subjektparadigma.

1897 Die Produktivität des gewählten Falles liegt für ein *Datenschutzrecht de lege ferenda* darin, diesen nicht auf seine binäre und eindimensionale Struktur als Rechtsstreit zwischen zwei Rechtssubjekten *de lege lata* zu reduzieren. Der Konflikt erschöpft sich nicht in einer individualrechtlichen *Bipolarität*. Vielmehr sind – von der Versicherung über den von ihr beauftragten Detektiv bis hin zur Versicherten – weitere Dimensionen und Gesellschaftsbereiche betroffen. Ebenso wenig beschränkt sich die rechtliche Problematik in der konkret durchgeführten Handlung, i. c. der durchgeführten geheimen Observation. Vielmehr zieht bereits die abstrakte Möglichkeit dieser Praxis, das Risiko der geheimen Observation, Konsequenzen nach sich, die das Recht zu berücksichtigen hat.

1898 In den Rechtsstreit zwischen Versicherter und Versicherung sind, wenn auch nicht im Gerichtsverfahren, *weitere Akteure involviert*. Es könnte von einem mindestens *triangulären Konflikt* gesprochen werden. Die dritte Position wird indes nicht vom Detektiv besetzt:

1899 Die *erste Position im Dreieck* des konkreten Falles nimmt V.-B. ein. Sie tritt als Klägerin resp. Beklagte und Beschwerdeführerin vor dem EGMR auf und tritt zugleich in ihrer Rolle als Verunfallte und Patientin, als Versicherte und IV-Bezügerin in Erscheinung. Damit verknüpft ist ihre Rolle als ehemalige Berufsfrau, als Coiffeuse. Zudem handelt es sich um eine Privatperson, die in ihrem persönlichen Lebensbereich beobachtet wird.

1900 Die *zweite Position wird von der Versicherung* eingenommen, welche die IV-Leistungen gegenüber V.-B. begleicht resp. begleichen müsste, sofern eine Invalidität vorliegt. Allerdings stellt sie die Erwerbsunfähigkeit resp. Invalidität der Versicherungsnehmerin und damit die Leistungspflicht wiederholt in Frage – trotz zahlreicher medizinischer Gutachten. Die Versicherung engagiert als Auftraggeberin einen *Privatdetektiv*, um einen mutmasslichen Versicherungsbetrug aufzudecken. Der Privatdetektiv beobachtet die Versicherte V.-B. in ihren privaten Aktivitäten, die sie im öffentlichen Raum ausübt.

1901 *Zur dritten Position:* Gemäss Sachverhalt waren über Jahre hinweg zahlreiche *Ärztinnen und Ärzte sowie weiteres Medizinalpersonal* zur Abklärung des *Gesundheitszustandes*, des Invaliditätsgrades resp. der Erwerbsunfähigkeit von V.-B. involviert. Es sind die Expertinnen und Experten des Gesundheitsbereichs, die im Kontext der Invaliditätsversicherung eine wichtige Rolle spielen: Sie sind es, welche die Gesundheitsbeeinträchtigung und damit die Erwerbsunfähigkeit *de lege artis* und mit notwendiger Fachkompetenz zu beurteilen haben. Nur unter Integration dieser Akteure, die eine Hauptrolle im IV-Versicherungskontext spielen, kann die (datenschutzrechtliche) *Konfliktlage* angemessen erfasst werden. Die

Integration des Gesundheitsbereiches mit seinen Akteuren ist damit richtungsweisend für eine sinnvolle Analyse des Rechtskonfliktes.[2396] Sie macht einen *prima vista* bipolaren Konflikt zu einem triangulären Konflikt.

Das *Konflikt-Dreieck* wurde somit anhand des konkreten Falles wie folgt beschrieben: Involviert sind die konkret beobachtete Versicherungsnehmerin, die Versicherungsgesellschaft (mit dem von ihr mandatierten Detektiv) und das Gesundheitspersonal. Die Eigenheiten des konkreten Konfliktes und namentlich des Sachverhaltes verdeutlichen die herausragende Bedeutung des Gesundheitswesens und -personals in der Angelegenheit. Obschon sich gerichtlich lediglich die Versicherte und die Versicherungsgesellschaft gegenüberstanden, handelt es sich nicht um einen bipolaren Konflikt. Es geht um einen triangulären Konflikt. 1902

Dieses anhand des konkreten Falles herausgearbeitete Dreieck lässt sich nunmehr in einen grösseren Zusammenhang einbetten. Es liesse sich von einem einbettenden *grösseren Dreieck* sprechen. Der Konflikt erschöpft sich nicht in der Dimension des individuell-konkreten Rechtsstreites. Ebenso wenig genügt es, die (nach unzähligen medizinischen Untersuchungen und Begutachtungen) durchgeführte geheime Observation datenschutzrechtlich zu problematisieren. Vielmehr ist bereits das *Risiko* resp. die blosse Möglichkeit der geheimen Versicherungsobservation aus einer Datenschutzperspektive *de lege ferenda* kritisch. 1903

Die Praxis zeitigt – selbst wenn eine Observation gesetzlich, so wie es der EGMR fordert, angemessen vorgesehen wird – *einschneidende negative Konsequenzen*. Diese gehen in ihrer Bedeutung weit über den konkreten Eingriff in das Privatleben des konkret beobachteten Datensubjektes hinaus. Die Praxis *betrifft mehrere als schutzwürdig anerkannte und damit etablierte Gesellschaftsbereiche*. 1904

Präzisiert: Die geheime Observation durch einen Privatdetektiv im Sozialversicherungskontext führt aufgrund ihrer abstrakten Möglichkeit zu einer *Kollision zwischen verschiedenen gesellschaftlichen Systemen mit ihren jeweils eigenen Rationalitäten und Zwecken*. Sie setzt die Integrität *des Kontextes eines persönlichen resp. familiären Lebensbereichs*, des Privatlebens, der privaten Lebensführung aufs Spiel. Zudem geraten die *Ziele, Zwecke sowie Rationalitäten des Kontextes der Sozialversicherung* unter Druck. Sodann wird die *Integrität des* 1905

2396 Der bipolare Konflikt zwischen Versicherter und Versicherung ist offensichtlich. In der Lösung des individualrechtlichen Konfliktes in einem Zweiparteienstreit wird ebenso das aktuelle datenschutzrechtliche Subjektparadigma sichtbar: *De lege lata* und entsprechend der Rechtsprechung liegt der Akzent auf der konkret durchgeführten geheimen Observation, die i. c. (nicht) als Verletzung des Privatlebens von V.-B. beurteilt wurde. Der Fokus richtete sich auf eine Art Handlungs(un)recht des Datenverarbeitenden gegenüber dem Datensubjekt. Darin spiegelt sich, was in dieser Schrift mehrfach beschrieben wurde: ein Konzept, nach welchem Datenschutzrecht als Persönlichkeitsschutz gilt, der das Subjekt schützt, und zwar in einer abwehr- resp. deliktsrechtlichen Stossrichtung. Sobald allerdings der Konflikt um die Dimension des Gesundheitskontextes ergänzt wird, präsentiert er sich auch, aber nicht nur datenschutzrechtlich ganz anders.

Gesundheitsbereiches erodiert. Solche disruptiven Effekte gehen von *wirtschaftlichen Rationalitäten und damit von einem ökonomischen Bezug aus*. Sie werden vonseiten des Sozialversicherungskontextes zur Legitimierung der Informationspraxis angeführt. Die im Sozial- und IV-Bereich angerufenen ökonomischen Rationalitäten, welche die Geheimobservation rechtfertigen sollen, untergraben indes Logiken und Erwartungen des Privatlebens, des Sozialversicherungsbereichs und des hieran angekoppelten Gesundheitsbereichs.

1906 Diese systemischen, mehrdimensionalen Lagen des Rechtskonflikts sowie die vielseitige und vielschichtige Bedrohungslage, die aus der Praxis hervorgehen, werden detaillierter ausgefaltet:

1907 Unbestritten ist, dass IV-Renten beziehende Menschen ein *Recht auf Achtung des Privatlebens* haben. Ebenso unbestritten dürfte zugleich sein, dass Personen mit Gesundheitsbeeinträchtigungen, die zu Erwerbsunfähigkeit resp. Invalidität und in der Folge zum Bezug von IV-Leistungen führen, *faktisch bedingt*, nämlich wegen der *gesundheitlichen Beeinträchtigungen*, nicht mehr gleich frei sind in der Gestaltung ihres Lebens, ihres Berufs- und Erwerbslebens, aber auch ihres Privatlebens. Die faktische Freiheit und Autonomie der Lebensführung gesunder resp. nicht invalider Personen differiert. Allerdings sind hier unzählige Schattierungen denkbar. Zudem gilt es, systemisch und kontextuell zu differenzieren: Die Invalidität trifft Aussagen zur Erwerbs(un)fähigkeit und bezieht sich auf den *Arbeitskontext*. Eine Erwerbsunfähigkeit korreliert nicht zwingend und zu 100 Prozent mit dem Untergang der Freiheit und Fähigkeit zu Aktivitäten im privaten Lebensbereich.

1908 Die *Beurteilung* der Auswirkungen und des Zusammenspiels zwischen Gesundheitszustand und Erwerbsfähigkeit obliegt dem insofern kompetenten Personal, dem *Gesundheitspersonal*. Es sind Szenarien möglich, in denen die diagnostizierte Gesundheitsbeeinträchtigung vom Medizinalpersonal zum Befund einer (vollständigen) Erwerbsunfähigkeit führt. Gleichwohl ist denkbar, dass eine Ärztin resp. ein Arzt die IV-Rente beziehende Person aus Erwägungen des Gesundheitsschutzes zu einem täglichen Spaziergang, zur Pflege sozialer Kontakte oder zur Erledigung kleiner alltäglicher Verrichtungen anhält. Die Bewahrung einer gewissen Eigenständigkeit, von gewissen sozialen Kontakten und soweit möglich von Bewegung an der frischen Luft kann erwiesenermassen einen guten Einfluss auf die Gesundheit, namentlich auch die psychische Gesundheit, haben.

1909 Diese Hintergründe sind für die datenschutzrechtliche Analyse relevant: Im Bereich der IV ist es die *Invalidität*, welche der Handlungsfreiheit Schranken setzt, und zwar in erster Linie in Bezug auf den *Arbeitskontext und die Erwerbsfähigkeit*. Damit ist nicht gleichzeitig fixiert, welche Handlungen im sog. *privaten Lebensbereich im Rahmen des Gesundheitszustandes* möglich bleiben resp. nicht

mehr möglich sind. Eine *Gesundheitsbeeinträchtigung, die zur Erwerbsunfähigkeit* führt, hat zwar höchstwahrscheinlich ebenso weitreichende Auswirkungen auf die *Handlungsmöglichkeiten im persönlichen, privaten Lebensbereich und Kontext*.[2397] Allerdings ist eine Erwerbsunfähigkeit nicht zwingend vollständig deckungsgleich mit einer kompletten Handlungsunfähigkeit im Bereich der persönlichen Lebensführung.

Das *Recht und insb. eine informationsrechtliche Normierung* (welche eine geheime Observation im Versicherungskontext zulässt) sollte den faktisch durch den Gesundheitszustand sowieso beschränkten Bereich des privaten Lebens *nicht* weiter beschneiden. Vielmehr ist Menschen mit gesundheitlichen Beeinträchtigungen, die zu Erwerbsunfähigkeit sowie Invalidität führen, der *Anspruch auf ein privates Leben* mit verbleibenden Entscheidungs- und Gestaltungsfreiräumen zu gewährleisten. Solche gesundheitsadäquate Aktivitäten beziehen sich ebenso auf den öffentlichen Raum – soweit diese mit der diagnostizierten Gesundheitsbeeinträchtigung kompatibel sind.[2398] 1910

Die Praxis geheimer Observation beschneidet auch den IV-Rentenbeziehenden garantierten *Anspruch auf Achtung des Privatlebens* empfindlich, selbst wenn *keine* konkrete Observation durchgeführt wird. Der Anspruch auf Achtung des privaten Lebensbereiches ist, wie gezeigt, auch für Aktivitäten im öffentlichen Raum anzuerkennen. Gewährleistet wird damit namentlich die *autonome und persönliche Lebensgestaltung, die nicht nur in den eigenen vier Wänden, sondern ebenso im sog. öffentlichen Raum stattfindet*. Doch genau diese qua Gesundheit reduzierten und verbleibenden Handlungs(frei)räume von Personen, die IV-Renten beziehen, werden durch die Praxis der geheimen Observation weiter *beschnitten*. 1911

Von der Praxis der geheimen Observation ist bereits aufgrund ihrer abstrakten Möglichkeit *ein ganzes Kollektiv von Personen im Bereich des Privatlebens* tangiert. *Potentiell* müssen *sämtliche IV-Versicherungsbezüger* eine geheime Observation ihrer persönlichen Lebensführung, des privaten Lebensbereichs *fürchten*. Die persönliche, ggf. familiäre Lebensführung gerät bei IV-Rente beziehenden Personen unter Druck. Einen Hinweis auf diesen Effekt und seine Ursache gibt der eingangs zitierte Zeitungsbericht: Problematisiert wird der «Generalverdacht» gegenüber sämtlichen Leistungsbezügern. Eine ganze Personengruppe wird und kann sich aus *Angst* vor der geheimen Überwachung mit entsprechen- 1912

2397 Wer erwerbsunfähig ist, wird kaum mehr bergsteigen, Marathon laufen, ausgiebige Shopping-Touren usf. unternehmen können. Dennoch darf eine medizinisch attestierte Erwerbsunfähigkeit resp. Invalidität nicht zwingend zu dem Schluss führen, IV-beziehende Personen könnten einzig und allein in den eigenen vier Wänden im Bett liegen.

2398 Unter Umständen unterstützen resp. stabilisieren solche Aktivitäten – ein kleiner Spaziergang, ein leichter Einkauf usw. – die Gesundheit resp. Genesung.

den Konsequenzen kaum mehr frei resp. im Rahmen der ihnen gesundheitlich gesetzten Schranken im öffentlichen Raum bewegen, entfalten und verhalten. Die Praxis privatdetektivischer Versicherungsobservation setzt folglich, ungeachtet einer angemessenen Normierung, bereits aufgrund des Risikos ihrer Realisierung, *im Ergebnis den Kontext des Privatlebens aufs Spiel*. Was folgt kann ein kompletter Rückzug in die Isolation sein, was – spätestens seit der Corona-Krise für viele offensichtlich – starke (weitere) Beeinträchtigungen, beispielsweise der (psychischen) Gesundheit, bringen kann.

1913 Im Sinne eines *Zwischenfazits* lässt sich festhalten: Die Annahme, wonach *erst und nur die im Einzelfall durchgeführte geheime Observation* im konkreten Fall mit dem subjektiven Recht auf *Privatleben interferiert, greift zu kurz*. Sie basiert auf einer abwehr- und deliktsrechtlichen Konzeption des aktuellen Datenschutz- und Privatheitsrechts; hierbei wird die datenschutzrechtliche Problematik in einer *Handlung* verortet, die den zivil- oder grundrechtlichen Privatheitsbereich verletzt. Es ist aber nicht erst und lediglich eine konkret durchgeführte Observation, welche den Privatbereich auch im öffentlichen Raum einer bestimmten Person (im Illustrationsfall V.-B.) beeinträchtigt. Durch die Praxis wird das *Kollektiv von Personen in der Rolle der IV-Bezüger tangiert*. Ein ganzes Kollektiv von Menschen wird durch die Möglichkeit geheimer Observation in dem ihnen qua Gesundheitsbeeinträchtigung sowieso bereits verengten Bereich autonomer Lebensführung weiter beschnitten. Damit ist neben der *subjektiven Komponente* die *systemische Dimension* in Bezug auf den Bereich des privaten Lebens adressiert. Betreffend den privaten Lebensbereich wurde damit der Fokus auf das Subjekt und die konkrete Informationserhebung gelöst und die systemische Problematik der abstrakten Möglichkeit der geheimen Observation, das Risiko derselben für den Kontext des Privatlebens, beschrieben. Das *Damoklesschwert*, als (potentieller) «Versicherungsbetrüger» auf das Radar der Versicherungen und ihrer Detektive zu geraten, überschattet einen *gesellschaftlichen Bereich*, denjenigen des persönlichen resp. privaten Lebens. Der hiervon angestossene weitere Rückzug (der bereits durch die Invalidität eingeleitet wurde) und der aus Angst vor Überwachungsmassnahmen folgende isolierende Rückzug können zudem einen nachhaltigen negativen Einfluss auf die *Gesundheit* der Versicherungsbezüger haben. Die Gesundheit ist übrigens als Teilaspekt der Identität relevant.

1914 Das Stichwort der Gesundheit resp. Gesundheitsbeeinträchtigung leitet zur nächsten Etappe der Analyse über. Die Rechtslagen werden damit weiter nuanciert. Denn die Praxis torpediert nicht nur *in concreto durchgeführt das Privatleben des betroffenen Subjektes sowie in abstracto als Risiko den Kontext des Privatlebens*. Vielmehr setzt sie *weitere Gesellschaftsbereiche* unter Druck. Ausgangspunkt für die Herausarbeitung weiterer systemischer Dimensionen bildet erneut die individuell-konkrete Situation des Illustrationsbeispiels und -falles.

Der Versicherungsnehmerin gegenüber stand *eine Versicherungsgesellschaft*, die im Bereich der IV-Leistungen und damit der *Sozialversicherung* öffentliche Aufgaben wahrnahm. Die Versicherungsgesellschaft ordnete nach einem *langwierigen Prozedere* die geheime Observation der Versicherten durch einen Privatdetektiv an. Der Fall beschäftigte nicht nur die Parteien des Rechtsstreites sowie die Behörden, sondern über unzählige Jahre hinweg ebenso das *Gesundheitspersonal*. 1915

Dass eine geheime Versicherungsobservation angeordnet wurde, legitimierte die Versicherungsgesellschaft mit folgenden Hauptargumenten: Zunächst hätten die *ärztlichen resp. medizinischen Untersuchungen sowie Gutachten* zu keiner kohärenten resp. stringenten Beurteilung des Gesundheitszustandes resp. der Erwerbsunfähigkeit und des Invaliditätsgrades der Versicherten und ehemaligen Friseurin geführt. Dem ist immerhin anzufügen, dass die Versicherung – soweit ersichtlich – jedes medizinische Gutachten, das eine Invalidität attestierte, hinterfragte. Die Versicherung führte weiter ins Feld, dass die divergierenden Beurteilungen des Gesundheitszustandes resp. des Invaliditätsgrades vonseiten der medizinischen Expertinnen und Experten auszumerzen seien – und zwar durch einen Privatdetektiv sowie eine geheime Observation der Versicherten in ihrer privaten Lebensführung. Zudem würde eine «Schadensminimierung» betrieben, damit Versicherungsgelder nur an wirklich Anspruchsberechtigte fliessen. Ungerechtfertigte Leistungen dagegen, die gerade im Falle umfassender Invalidität in beträchtliche Summen münden, sollen verhindert werden. Die Aufdeckung von Versicherungsbetrugsfällen sei im Interesse des *Versicherungskollektives*.[2399] 1916

Was der Sachverhalt des konkreten Falles allerdings unübersehbar macht, ist, dass es in besagtem Rechtsstreit fehl ginge, von einem *(erhärteten) Verdacht auf einen Versicherungsbetrug* zu sprechen. Vielmehr war es symptomatisch, dass die Versicherungsgesellschaft *jegliche Gutachten der Gesundheitsexpertinnen und -experten*, welche eine Beeinträchtigung der Gesundheit resp. Arbeitsfähigkeit, genauer der Erwerbsfähigkeit, und damit eine Invalidität von V.-B. attestierten, in Zweifel zog. V.-B. hatte sich zahlreichen medizinischen Untersuchungen unterzogen. Es kann ihr damit nicht vorgeworfen werden, an der Abklärung des Gesundheitszustandes durch die Expertinnen und Experten nicht mitgewirkt zu haben. Erst nach diversen medizinischen Konsultationen und Untersuchungen, die sich über unzählige Jahre zogen, sowie nach mehreren behördlichen Entscheidungen verweigerte V.-B. weitere ärztliche Untersuchungen. Das vonseiten der Versicherung ins Feld geführte *ultima-ratio*-Argument, wonach gerade auch wegen des Verhaltens der Versicherten nur noch der Ausweg der privatdetektivischen Observation blieb, ist vor diesem Hintergrund nicht stichhaltig. 1917

2399 Zu diesem Argument auch EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 76.

1918 Dass die Versicherung sämtliche medizinischen Gutachten, die zu einer Leistungspflicht geführt hätten, in Frage stellte und alsdann einen Privatdetektiv einsetzte, war von einem *wirtschaftlichen Motiv*, einem ökonomischen Zweck motiviert. Und diese *ökonomischen Rationalitäten kollidieren mit den anderen, ebenso involvierten Kontexten und erodieren diese.*

1919 Insofern ist die bereichsspezifisch einschlägige Gesetzgebung sowie die (rechts-)wissenschaftliche Expertise relevant: Sozialversicherungen, so führt es u. a. Pärli aus, dienen der Absicherung wirtschaftlicher Konsequenzen infolge «elementarer Lebensrisiken wie Krankheit, Unfall, Invalidität oder Arbeitslosigkeit».[2400] Spezifisch für den Bereich der IV geht es gemäss Art. 8 Abs. 1 ATSG bei der Invalidität um die voraussichtlich bleibende oder längere Zeit dauernde, ganze oder teilweise Erwerbsunfähigkeit. Nach Art. 4 Abs. 1 IVG kann die Invalidität namentlich Folge von Krankheit oder Unfall sein. Mit anderen Worten geht es im IV-Bereich um Leistungen, die erbracht werden, weil insb. infolge von Krankheit oder Unfall eine voraussichtlich bleibende oder längere Zeit andauernde Erwerbsunfähigkeit eingetreten ist. Es sind die grossen Lebensrisiken, die im *Sozialstaat durch die Sozialversicherungen* abgesichert werden.

1920 Die IV-Versicherung als Teilelement der Sozialversicherungen erbringt Leistungen, welche die Folgen von *gesundheitsbezogenen Beeinträchtigungen, die nachhaltig auf die Arbeits- resp. Erwerbsfähigkeit durchschlagen,* zumindest teilweise abfedern sollen. Die in ihrem Zusammenhang zu ergreifenden Massnahmen, Untersuchungen sowie die zu erbringenden Leistungen werden nach *bestimmten Kriterien und Methoden* definiert. Weil im Rahmen der IV die *Gesundheit sowie deren Beeinträchtigung und ihr Einfluss auf die Erwerbsfähigkeit* das zentrale Element ist, kommt der *Expertise sowie den Befunden vonseiten der Ärzteschaft* eine zentrale Rolle zu. Der Gesundheitsaspekt ist im Kontext der Invaliditätsversicherung *ein Kernelement*. Entsprechend kommt dem Gesundheitswesen resp. dem Gesundheitsbereich entscheidende Relevanz zu. Bezogen auf den Gesundheitsaspekt im Kontext der IV und die Praxis geheimer Observation ist hierzu anzumerken:

1921 Im Rahmen der Sozialversicherungen sind die Re-Integration und damit auch die Verbesserung oder zumindest Stabilisierung des Gesundheitszustandes sowie die Reduktion einer Arbeitsunfähigkeit resp. Invalidität anerkannte Ziele. Eine stete Angst vor geheimer Überwachung und ein Generalverdacht, dem IV-Bezüger ausgesetzt werden, sowie eine Kultur des Misstrauens durchkreuzen *eine solche Zielsetzung des Sozialversicherungskontextes*.[2401] Unter Umständen werden Handlungen im öffentlichen Raum, die der Gesundheit von Menschen mit

2400 Pärli, recht 2018, 120 ff., 122.
2401 Ders., a. a. O.

Invalidität zuträglich sind, wegen der etablierten Angst- und Misstrauenskultur unterlassen. Zuhause bleiben und keinerlei Aktivitäten nachzugehen, könnte die Devise für IV-Bezüger werden.

Weiter ist festzustellen, dass *Beobachtungen zu Alltagsverrichtungen aus dem Kontext des Privatlebens durch nicht* spezifisch mit Blick auf die Evaluation von Gesundheitsbefunden geschulte Personen keineswegs zwingend und kausal Rückschlüsse auf die Gesundheit und Arbeits- resp. Erwerbsfähigkeit zulassen. 1922

Zudem ist die Observierung inklusive der Erstellung des Observationsberichts durch den Privatdetektiv ein *selektiver Prozess*, selbst wenn die Observation systematisch erfolgt. Der Privatdetektiv *ohne Schulung im Gesundheitsbereich* trifft bewusste und unbewusste Entscheidungen darüber, was er als «entscheidungsrelevant» wahrnehmen und dokumentieren will. Rückschlüsse aus den durch eine medizinisch kaum geschulte Person ermittelten Informationen, die aus dem privaten Lebensbereich erhoben wurden, auf den Gesundheitszustand resp. die Erwerbsunfähigkeit oder Invalidität und damit den Gesundheits- resp. Arbeitskontext sind heikel. 1923

Alsdann muss festgehalten werden, dass der Privatdetektiv im Auftrag der Versicherung handelt. Seine Neutralität ist zumindest in Frage zu stellen. Wie erwähnt kommt Privatdetektiven regelmässig keine medizinische Expertise zu.[2402] 1924

Geht es um die Beurteilung des *Gesundheitszustandes* eines Menschen und die Frage der Auswirkungen desselben auf die Erwerbsfähigkeit, ist es folgerichtig, diese Aufgabe einzig und allein denjenigen Personen zuzuweisen, denen anerkanntermassen die hierfür erforderliche Kompetenz und Expertise zukommt: an erster Stelle der *Ärzteschaft*, im weiteren Sinne dem *Gesundheitspersonal,* das die erforderlichen Ausbildungen und Fachkenntnisse sowie persönliche Eigenschaften wie Unbestechlichkeit, Sachlichkeit und Unabhängigkeit nachweisen. Das Vorgehen als Gutachtende hat *de lege artis* zu erfolgen. Folglich ist auch vonseiten der Sozialversicherungen sicherzustellen, dass die erforderlichen Kompetenzen sowie die Unabhängigkeit des mit der Evaluation betrauten Gesundheitspersonals gegeben sind. 1925

Herausragende Bedeutung nehmen in der Praxis geheimer Observation *ökonomische Interessen* ein. Sie werden vonseiten der die Observationen durchführenden Versicherungen ins Feld geführt, gemeinsam mit dem gebotenen Schutz des Versichertenkollektives. Die Praxis der geheimen Observation ist jedoch nur *prima vista* im Interesse der *Versicherung sowie des Versicherungskontextes*. Vielmehr zeigt sie sich für den Kontext der IV und damit der Sozialversicherung als disruptiv: Mit ihr wird die *Vertrauens- resp. Glaubwürdigkeit sowie Integrität des Sozi-* 1926

2402 Hierzu auch Gächter, SRF online vom 18. Oktober 2016, <https://www.srf.ch/news/schweiz/versicherungen-duerfen-moegliche-betrueger-nicht-observieren> (zuletzt besucht am 30. April 2021).

alversicherungskontextes erodiert. Die Praxis schafft eine *Kultur des Misstrauens*, welche der Kooperationsbereitschaft, aber auch der Stabilisierung oder Verbesserung des Gesundheitszustandes der Leistungsbezüger abträglich ist. Erodiert wird zugleich das *Vertrauen in die Expertise des zur Abklärung des Gesundheitszustandes* kompetenten medizinischen Personals. Wenn die zur Evaluation des Gesundheitszustandes befähigten Personen die Befunde anscheinend nicht leisten können resp. entsprechende Gutachten von der Versicherung aus ökonomischen Gründen wiederholt und prinzipiell hinterfragt werden, gerät zugleich das *Vertrauen in das Gesundheitswesen und den Gesundheitssektor* unter Druck. Der Schutz der *Integrität sowie des Vertrauens in die IV als wichtige Säule des Sozialversicherungskontextes* und *Sozialstaates, aber auch in den Gesundheitsbereich* ist folglich ebenso als eine *datenschutzrechtliche Aufgabe* anzuerkennen.

1927 «Der Fall» EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz ist damit ein gutes Beispiel zur Illustration der Kollision verschiedener gesellschaftlicher Kontexte mit ihren jeweiligen Zielen, Logiken und Erwartungen. Informationsflüsse und damit das Datenschutzrecht spielen eine Hauptrolle bei der Absicherung oder eben Gefährdung gesellschaftlicher Kontexte.

1928 Es sind ökonomische Rationalitäten, welche die IV-Versicherungen zu einer Praxis veranlassen, die Ziele des privaten Lebensbereiches, aber auch der Sozialversicherung (IV) mit dem hier einschlägigen Gesundheitsaspekt und damit den Gesundheitsbereich zu untergraben. Mittel- und längerfristig betrachtet zeigt sich in der Folge selbst das wirtschaftliche Motiv als problematisch: Die potentielle Überwachung und das Klima des Misstrauens stören die Vertrauensbasis und schüren Ängste sowie Verunsicherungen, die in Isolation und Rückzug münden können. Hieraus dürften weitere finanzielle Kosten resultieren. Es kann nicht ausgeschlossen werden, dass diese unter Umständen gar höher sind als die durch die geheime Observation vermeintlich erzielten Einsparungen.

1929 Welche *Schlussfolgerungen sind zu ziehen und welche Ergebnisse* sind festzuhalten? Eine geheime Observation tangiert nicht nur eine konkret betroffene Person negativ. Die Praxis geheimer Observation beschlägt vielmehr die Integrität mehrerer wichtiger Gesellschaftsbereiche. Ursächlich sind wirtschaftliche Rationalitäten. Untergraben wird *nicht* nur die Integrität des «privaten Lebensbereiches» des konkret betroffenen, weil geheim durch einen Privatdetektiv observierten Individuums. Vielmehr wird der *Privatbereich eines ganzen Kollektivs*, derjenige der IV-Bezüger, bereits durch die abstrakte Möglichkeit der geheimen Observation unter Druck gesetzt. Der Einwand von Versicherung und Bundesgericht, wonach die geheime Observation nur ganz selten als *ultima ratio* zum Einsatz komme, geht fehl. Mit der Praxis wird zudem die Integrität des Sozialversicherungskontextes, aber auch diejenige des Gesundheitswesens mit den ebenda anerkannten Zielen und Rationalitäten torpediert. Die Personendatenver-

arbeitungspraxis zeitigt somit systemisch und kollektiv negative Auswirkungen sowohl für den Bereich des Privatlebens als auch für den Sozialversicherungskontext und damit zusammenhängend für den Gesundheitsbereich. Dies bereits aufgrund ihrer blossen *Möglichkeit*.

1930 *Folglich sind das Schutzziel resp. der Schutzzweck des Datenschutzrechts sowie die Gefährdungspotentiale neu und erweitert anzuerkennen:* Datenschutz und die Gestaltung datenschutzrechtlicher Vorgaben kann, darf und soll nicht isoliert an der Verletzung der Persönlichkeit im Einzelfall, dem Individualgüterrechtsschutz und Schutz des Individuums durch subjektive Rechte ansetzen. Es greift zu kurz, lediglich diesen individuellen Rechtskonflikt zu sehen. Vielmehr sind Gefahren von Personendatenverarbeitungsprozessen auf kollektiver Ebene mit Blick auf etablierte plurale Gesellschaftsbereiche zu evaluieren. Das Datenschutzrecht hat alsdann in einer ausdifferenzierten Ausgestaltung einen Beitrag zum Schutz der jeweils einschlägigen Gesellschaftsbereiche zu leisten. In dem hier gewählten Fall wurde gezeigt, wie der ökonomische Kontext und wirtschaftliche Rationalitäten die Integrität des Privatlebens, aber auch des Sozialversicherungskontextes sowie des Gesundheitsbereichs selbst aufs Spiel setzen.

1931 Damit besteht die Herausforderung bei der Gestaltung zukünftiger datenschutzrechtlicher Vorgaben darin, die *hinter* den Personendatenverarbeitungsprozessen und den dazu gehörigen Datenflüssen stehende Topografie, die gesellschaftlichen Bereiche, Systeme und Institutionen, in welche die Verarbeitungsprozesse eingebettet sind, in die Erwägungen zu integrieren. Stets ist danach zu fragen, welchen Einfluss die jeweilige Gestaltung der Verarbeitungsprozesse und Personendatenflüsse auf die *jeweiligen Systeme* zeitigt. Zweck datenschutzrechtlicher Vorgaben ist nicht isoliert der Schutz des Individuums. Vielmehr geht es auch darum, verschiedene gesellschaftliche Bereiche der pluralen Gesellschaft in ihrer Integrität zu schützen. Dies geschieht, indem «unangemessene» resp. mit den Logiken der jeweiligen Kontexte nicht vereinbare Informationsflüsse beschränkt resp. unterbunden werden, mit den Rationalitäten der Kontexte dagegen kompatible resp. zuträgliche Informationspraktiken abgesichert und zugelassen werden.[2403] Korrumpierenden Einfluss auf gesellschaftliche Teilsysteme wie die Demokratie, den Sozialstaat, das Privatleben oder den Gesundheitsbereich zeitigen, wie diese Arbeit an mehreren Stellen zeigte, Rationalitäten des ökonomischen Kontextes.

1932 Unter Reflexion der disruptiven Effekte der geheimen Observation durch einen Privatdetektiv im Versicherungskontext ist zu schlussfolgern, dass die *Praxis nicht anzuerkennen ist – auch nicht durch den Gesetzgeber*. An dieser Stelle deckt sich das Ergebnis dieser Analyse *nicht* mit dem Verdikt des EGMR. Die

2403 So Nissenbaum, 2 ff., 158 ff., 186 ff., 231 ff.

negativen Effekte der Praxis auf mehrere Gesellschaftskontexte werden selbst mit der Schaffung einer Gesetzesgrundlage nicht beseitigt.

1933 Ein allfälliger Graubereich mit Blick auf medizinische Gutachten zur Gesundheit ist anderweitig zu bewältigen: Für den Befund, wonach der Gesundheitszustand nicht ausnahmslos mit mathematischer Genauigkeit festgestellt werden kann, weil die Medizin keine exakte Wissenschaft ist und nicht jedwede Gesundheitsbeeinträchtigung restlos erklärbar ist, sind andere Ausgleichsmechanismen zu formulieren: Sie sollten im Sinne eines «Restrisikos» dem Versicherungssektor zugewiesen werden. Für die Abklärung von veritablen Versicherungsbetrugsfällen, für die erhärtete Anhaltspunkte aufgrund von nicht geheimen Prüfungsmassnahmen wie z. B. Hausbesuchen, Besuchen am Arbeitsplatz bei Teilinvalidität usf. vorliegen, sollen die *Strafverfolgungsbehörden* zuständig sein. Die Aufgabe der Sozialversicherungen ist eine andere.[2404]

1934 Eine ausdifferenzierende und erweiterte Sichtweise im und für das Datenschutzrecht der Zukunft, welches kollektive Schutzdimensionen integriert, soll nachfolgend anhand weiterer Konstellationen verdichtet werden. Diese kamen punktuell bereits im Laufe dieser Arbeit zur Sprache.

2. Illustrative Verdichtung des Systemparadigmas

1935 Das entwickelte Paradigma eines Rechts auf informationellen Systemschutz für ein schutzeffektives Datenschutzrecht der Zukunft kann anhand weiterer Beispiele erhärtet werden: Einige von ihnen kamen im Zuge dieser Schrift bereits zur Sprache. Bei den meisten handelt es sich um Gerichtsfälle. Obschon es bei diesen um die Beurteilung individuell-konkreter Konflikte ging, die gerichtlich regelmässig im Zweiparteienverfahren behandelt werden, zeigt sich in ihnen die Notwendigkeit eines system- resp. kontextbezogenen Ansatzes im Datenschutzrecht.

1936 Den Boden für *einen kontextuellen Ansatz* zur Bewältigung der «Privacy»-Herausforderungen und damit das Datenschutzrecht hat die Philosophin Nissenbaum bereitet.[2405] Betreffend das Recht beurteilt sie die Figur der *«reasonable expectations of privacy»*, deren Ursprung im US-amerikanischen Recht zu verorten ist, als wegweisend. Sie ist nach Auffassung von Nissenbaum aufs Engste mit dem Konzept kontextueller Integrität verbunden.[2406] Deshalb werden drei US-amerikanische Urteile eingeführt, in denen die *«reasonable expectations of privacy»* eine wichtige Rolle spielen.

2404 In diese Richtung weisend auch Pärli, recht 2018, 120 ff., 122.
2405 Vgl. Nissenbaum, 132: «Contexts are structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes).
2406 Dies., 233.

Sie wurden, wie gezeigt, auch vom EGMR in seinem Observationsentscheid angewendet. Insofern kam der EGMR unter Einsatz der Rechtsfigur der *«reasonable expectations of privacy»* zu der Feststellung, dass sich der *Schutzbereich des Privatlebens gemäss EGMR* auch *auf den öffentlichen Raum erstrecke*.[2407] Eine geheime Observation könne folglich, selbst wenn sie im öffentlichen Raum durchgeführt werde, einen schweren Eingriff in das Privatleben gemäss Art. 8 EMRK darstellen.[2408] Mit dieser Definierung des Schutzbereichs des Privatlebens gemäss Art. 8 EMRK trägt der EGMR ein anderes Konzept in den kontinentaleuropäischen Raum als die ebenda und gerade auch in der Schweiz bis heute wirkende Sphärentheorie. Eine solche Auslegung des Schutzobjektes gemäss Art. 8 EMRK, wonach ein Privatleben auch im öffentlichen Raum anzuerkennen ist, wurde vom EGMR bereits um die Jahrtausendwende anerkannt: 1937

> «La notion de „vie privée" est une notion large, qui ne se prête pas à une définition exhaustive. Des facteurs tels que l'identification sexuelle, le nom, l'orientation sexuelle et la vie sexuelle sont des éléments importants de la sphère personnelle protégée par l'article 8. Celui-ci protège également le droit à l'identité et au développement personnel, ainsi que le droit pour tout individu de nouer et développer des relations avec ses semblables et le monde extérieur. Il peut aussi s'étendre aux activités relevant de la sphère professionnelle ou commerciale. Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la „vie privée" […]. On ne peut donc exclure que la vie privée d'une personne puisse être affectée par des mesures prises en dehors de son domicile ou de ses locaux privés. Ce qu'un individu est raisonnablement en droit d'attendre quant au respect de sa vie privée peut constituer un facteur important, quoique pas nécessairement décisif […].»[2409]

Nachfolgend geht es um eine seit Jahrzehnten bekannte Figur, die wichtige Impulse für ein Datenschutzrecht der Zukunft geben kann. Ein Datenschutzrecht, das seinen Schutzauftrag sowohl in seiner subjektivrechtlichen wie auch in seiner systemrelativen Dimension wirksam zu gewährleisten vermag. Bisher wurde gezeigt, dass es ein rechtlich geschütztes Privatleben ebenso im öffentlichen Raum gibt. Damit wird eine dualistische, räumlich-sphärentheoretische Idee des Privaten durchbrochen. 1938

Die Systemrelevanz des Datenschutzrechts wird anhand der Figur der *«reasonable expectations of privacy»*, allerdings mit einem Blick auf Urteile aus ihrem Herkunftskontinent, noch differenzierter sichtbar. Wie traditionsreich die Rechtsfigur in den USA ist, zeigt das Urteil Katz aus dem Jahr 1967.[2410] Charles Katz war auf das Radar des FBI geraten. Er wurde verdächtigt, illegalen Aktivitäten 1939

2407 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 48, E 54 unter Verweis auf EGMR Nr. 63737/00 – Perry/United Kingdom, Urteil vom 17. Juli 2003, E 37 ff.

2408 EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, E 48, E 54 unter Verweis auf EGMR Nr. 63737/00 – Perry/United Kingdom, Urteil vom 17. Juli 2003, E 52 ff.

2409 EGMR Nr. 63737/00 – Perry/United Kingdom, Urteil vom 17. Juli 2003, E 36 f., unter Verweis auf vorangehende Urteile.

2410 U.S. Supreme Court, 89 U.S. 347 – Urteil Katz v. United States vom Oktober/Dezember 1967.

nachzugehen, genauer: zu gamblen. Folglich wurde sein Verhalten einer Observation unterzogen. Zum Einsatz kam das Wiretapping. Telefongespräche, die er von öffentlichen Telefonzellen aus in codierter Sprache führte, wurden abgehört. Bei diesen Gesprächen ging es um die Verschiebung beträchtlicher Geldsummen. Unmittelbar anschliessend an eine Abhörung wurde Katz vom FBI verhaftet. Katz rügte das Vorgehen des FBI als Verletzung des vierten Amendments: Die Abhörung eines Telefonates solle stets nach denselben Informationsnormen erfolgen. Es könne nicht relevant sein, ob das Gespräch von einer öffentlichen Telefonzelle oder von einem privaten Bereich aus geführt werde. Bei der Beurteilung der Frage, ob die Abhörung verfassungsmässig war oder nicht, wurde festgehalten, dass das vierte Amendment *Menschen* und nicht Orte schütze. Inwiefern Menschen zu schützen seien, war damit nicht beantwortet. Der Supreme Court machte in seinem Urteil die mangelnde vorgängige Autorisierung der Observation durch das FBI zum Entscheidungskriterium. Weil die notwendige Autorisierung der Observationsmassnahmen dem FBI nicht vorlag, entschied der Supreme Court zugunsten von Katz.

1940 In einer *concurring opinion* präsentierte Justice John Harlan *zwei Voraussetzungen* für die Annahme der *«reasonable expectations of privacy»*. Privacy-Erwartungen könnten als vernünftig gelten, wenn *erstens* eine bestimmte Person aktuell einen Schutz auf Privatheit erwarte und *zweitens* diese Erwartung eine sei, welche die Gesellschaft als vernünftige Erwartung anzuerkennen bereit sei.[2411]

1941 Diese Konzeptionierung in Gestalt eines *Zweischrittes* hat sich als Standard etabliert, allerdings nicht ohne Umschweife, wie die Betrachtung eines weiteren Urteils zeigen wird. Der Entscheid Katz gilt als richtungsweisend. Auch er bietet eine alternative Sichtweise zu einer räumlich und binär codierten Idee des Privaten. Verglichen mit einem früheren Entscheid, Olmsted v. United States, der das Abhören von Telefongesprächen noch nicht als unrechtmässige Verletzung der privaten Sphäre beurteilte, anerkannte der Entscheid Katz, dass ein Telefongespräch, selbst wenn es aus einer öffentlichen Telefonkabine geführt würde, unter dem vierten Amendment geschützt werde. Insofern Nissenbaum zur Transformation des Konzeptes des Privaten von einem räumlichen Ansatz in die Richtung der Anerkennung eines Lebensbereiches:

> «Framing this landmark ruling in terms of the dichotomy of realms, it can be understood as effectively transforming telephone conversation into a constitutionally protected private zone.»[2412]

2411 M. w. H. Nissenbaum, 115.
2412 Dies., 101.

Anders die argumentative Stossrichtung im Urteil Riley aus dem Jahr 1989.[2413] Auch Riley wurde illegales Verhalten vorgeworfen. Das Pasco County Sheriff's Office von Florida hatte einen Hinweis erhalten, wonach Michael Riley auf seiner ruralen Liegenschaft Marihuana-Plantagen kultiviere. Der Beweis dafür wurde durch einen Helikopterflug über das Grundstück erhoben. Wegen zweier fehlender Dachverdeckungen waren die Pflanzen mit blossem Auge sichtbar.[2414] Gerichtlich war später die Frage zu beantworten, ob der von einem *Helikopterflug* aus einer Höhe von 120 Metern gewonnene Einblick in die relevanten Bereiche mit dem vierten Amendment vereinbar sei oder nicht. Erstinstanzlich bekam Riley Recht: Das Gericht befand, dass die durch einen Flug über das Grundstück gewonnene Einsicht in das Innere eines Gartenhauses gegen *«reasonable expectations of privacy»* und die im vierten Amendment verbürgten Rechte verstosse. Anders entschied in letzter Instanz der Supreme Court. In das Zentrum seiner Argumentation rückte der Gerichtshof den folgenden Befund: Es gäbe keine *«reasonable expectations of privacy»*, wonach es keine Observationen aus dem Luftraum gäbe – Flugzeuge seien ein hinreichend etablierter *common place*.[2415] 1942

Gegen diese Mehrheitsmeinung brachte Justice Connor eine nachvollziehbare *concurrence* an: Der Akzent in der Argumentation der Mehrheitsmeinung würde sich zu stark an der Praxis und dem Recht der *Luftfahrt* orientieren. Es sei *nicht die Etablierung der Luftfahrt an sich*, von der die *«reasonable expectations of privacy»* abhängen würden. Nur weil das «Erhaschen» des entscheidenden Blickes über die Plantage auf privatem Grund selbst ohne Zuhilfenahme weiterer technischer Instrumente möglich war, konnte das Gericht wohl übersehen, dass das Flugzeug nicht zu der gemeinhin anerkannten Praxis und im Transportkontext im Einsatz stand. Vielmehr diente es als Hilfsmittel zur Observation im *Strafermittlungskontext*. In dieser Funktion und zu diesem Zweck möchte man nicht davon ausgehen, dass der Einsatz von Flugzeugen zur Aufdeckung von unerlaubten Handlungen ungeachtet der Einhaltung von prozessualen Vorgaben einer allgemein anerkannten Praxis entspricht. Die Flugtechnologie wurde gerade nicht zu ihrem genuinen Zweck, dem Transport, eingesetzt. Vielmehr diente sie der Informationsermittlung im Strafermittlungskontext. Nur dank ihr konnte Einblick in die klassischen privaten Lebensbereiche gewonnen werden, woraufhin die so generierten Informationen in den Untersuchungskontext transferiert 1943

2413 U.S. Supreme Court, 488 U.S. 445 – Urteil Riley v. Florida vom Oktober 1988/Januar 1989.

2414 Heute würde man hierfür wohl Drohnen mit integrierten Kameras, Mikrofonen oder Sensoren, beispielsweise zur Messung von Wärme, einsetzen; vgl. zur Thematisierung von Drohnen auch aus einer datenschutzrechtlichen Perspektive resp. unter dem Aspekt des Privatsphärenschutzes Schefer, ZSR 2014, 259 ff., insb. 270 ff.

2415 U.S. Supreme Court, 488 U.S. 445 – Urteil Riley v. Florida vom Oktober 1988/Januar 1989; vgl. auch Nissenbaum, 160.

wurden. Weil der Flugverkehr *sufficiently common place* ist, kann daraus nicht abgeleitet werden, dass die Observation aus dem Flugzeug, die Informationsgenerierung qua Flugzeug im Lichte des vierten Amendments und der *«reasonable expectations of privacy»* unproblematisch ist.

1944 Gleichermassen um den Nachweis von Marihuana-Anpflanzungen auf einer Privatliegenschaft ging es im Entscheid Kyllo v. United States aus dem Jahr 2001.[2416] Die Detektion erfolgte indes, anders als bei Ripley, nicht mittels Augenscheins. Zum Einsatz kam die Technologie der *Wärmebildgebung*. Das Gericht befand, dass die Anwendung der Wärmebildtechnologie, die erhöhte Temperaturen als Folge entsprechender Kulturen nachweisen konnte, keine anerkannte Praxis sei. Im Ergebnis sah das Gericht darin eine Verletzung der *«reasonable expectations of privacy»*.

1945 Die schlaglichtartige Beleuchtung der drei Entscheidungen erhellt mehrere auch informationsrechtlich relevante Aspekte:

1946 Erstens zeigen sich die Bemühungen der US-amerikanischen Gerichte, *Herausforderungen von neuen Technologien im Zusammenhang mit der Informationsermittlung und -verarbeitung* zu adressieren. Die *«reasonable expectations of privacy»* werden als Instrument eingesetzt, um den Grad der Integration und Akzeptanz gewisser Technologien zu bestimmen. Hieraus werden Folgerungen für den Schutzbereich der privacy gezogen. Die *«reasonable expectations of privacy»* zeigen sich damit als Bewältigungsinstrument dort, wo der Rechtsapparat von technischen Apparaturen herausgefordert wird.

1947 Allerdings ist es, zweitens, nicht die Fokussierung auf eine *bestimmte Technologie*, aus der sich überzeugende Antworten für die Herausforderungen, die unter dem Dachbegriff des Privaten, der privacy diskutiert werden, ziehen lassen. Zur Illustration: Technologien können, selbst wenn sie z. B. wie Facebook intensiv genutzt werden, datenschutzrechtlich kritisch sein.[2417] Die Intensität der Nutzung einer Informationstechnologie an sich sagt nicht zwingend gleichzeitig etwas darüber aus, ob mit dieser *«reasonable expectations of privacy»* verletzt werden oder nicht.

1948 In Bezug auf die drei Fälle ist sodann, drittens, festzuhalten: In allen drei Fällen wurden Technologien eingesetzt, um mutmasslich *vorgenommene illegale Handlungen* aufzudecken. Hierzu wurden Informationen aus einem persönlichen Lebensbereich observiert und erhoben, so durch Abhörung der Gespräche aus einer sog. öffentlichen Telefonzelle oder durch die Gewinnung von Bildern von illegalen Plantagen mittels Wärmebildkamera oder Fluggefährt. Für sämtliche Konstellationen wäre zu erwarten gewesen, dass ungeachtet der eingesetzten

2416 U.S. Supreme Court, 533 U.S. 27 – Urteil Kyllo v. United States vom Februar/Juni 2001.
2417 Zu Risiken von Social Media vgl. vertiefend Coen, *passim*.

Technologie die *einschlägigen strafprozessualen Ermittlungsvorgaben*, wie sie für die Observation gelten, zu beachten seien. Hierzu gehört in aller Regel eine behördliche Autorisierung der Massnahme gemäss einer gesetzlichen Grundlage.[2418]

Bestätigt wird viertens, dass jede Technologie bezüglich ihrer Auswirkungen auf 1949
das Private nur dann *sinnvoll* evaluiert werden kann, wenn die Technologie als *sozio-technologisch* gelesen wird.[2419] Ein technisches Gerät isoliert als Maschine, bestehend aus Hardware, Software, Kabeln und Netzen, wahrzunehmen oder in seiner unmittelbarsten Funktion zu analysieren, ist für die Kategorie des Privaten auch im Recht wenig hilfreich.[2420] Vielmehr sind die Geräte stets in ihren Einbettungen und Bezügen zu sozialen Praktiken zu betrachten.[2421] Folglich ist in dieser Schrift mit dem Begriff «System» nicht oder nicht isoliert die Technologie gemeint. Vielmehr geht es beim Terminus «System» resp. «Kontext» um die – auch datenschutzrechtlich relevanten – einbettenden sowie einschlägigen gesellschaftlichen Bereiche.[2422]

Die US-amerikanischen Entscheide richten den Fokus punktuell zu stark auf die 1950
Akzeptanz der *Technologie* an sich. In allen drei Fällen wurde mittels dreier verschiedener Technologien in einen *Lebensbereich* eingedrungen, der vernünftigerweise wohl als privater Lebensbereich nicht nur vom betroffenen Individuum, sondern von der Gesellschaft als solcher beurteilt würde: Das Telefongespräch, auch wenn von einer öffentlichen Zelle geführt, gleichermassen wie die Bepflanzungen auf resp. innerhalb von privaten Liegenschaften dürften als Bereiche der privaten Lebensführung anerkannt sein. Wenn Informationen aus jenen Bereichen mittels Technologien, seien es Abhörgeräte, Überflug oder Wärmebildgebung, abgegriffen werden, um diese alsdann zur Strafverfolgung auszuwerten, sind einheitlich die strafprozessualen Ermittlungsvorgaben einzuhalten. Ein solcher Schluss wurde auch für den hier gewählten Illustrationsfall des EGMR gezogen. Leitend ist stets die Frage, welchen Einfluss Informationsflüsse – Infor-

2418 Auch hier liesse sich die Frage, wie es im Rahmen der Analyse des Versicherungsfalles getan wurde, umformulieren. Der Fokus würde dann vom formellen Kriterium auf die materielle Evaluierung schwenken und danach fragen, ob man zum Zwecke der Aufdeckung illegaler Handlungen – *nota bene:* Es ging nicht um die Aufdeckung von «Kapitaldelikten», sondern in den beleuchteten Fällen Riley und Kyllo ging es um die Frage des verbotenen Hanfanbaus resp. bei Katz um «Gambling» – Informationen aus dem persönlichen Lebensbereich erheben und zur Strafverfolgung in besagten Kontext transferieren darf. Entscheidend zur Beantwortung hierfür ist die Frage, ob ein entsprechender Informationsfluss die Integrität der Kontexte achtet oder vielmehr torpediert.

2419 Vgl. auch Dolata, Berl J Soziol 2011, 265 ff.; Nissenbaum, 4 ff., 189 ff.; vgl. den Essay zu Suchmaschinen in ihren gesellschaftlichen Einbettungen Gugerli, 9 ff.

2420 Vgl. Nissenbaum, 5 f.; zum komplexen Verhältnis von Mensch, Technologie sowie Recht und Analysen von Mensch-Maschinen-Assoziationen, hybriden oder Multi-Aktanten-Systemen vgl. Gruber, 24 ff., 221 ff., 258 ff.; Teubner, AcP 2018, 155 ff.; Karavas, Neue Zeitschrift für Sozialforschung 2010, 95 ff.

2421 Nissenbaum, 5 f.

2422 Der Begriff des Kontextes wird gerade auch vonseiten der Sozialwissenschaften geprägt, indes nicht ganz einheitlich definiert; vgl. Nissenbaum, 132 ff.; Luhmann vertritt, dass unterschiedliche gesellschaftliche Systeme unterschiedliche Funktionen erfüllen, vgl. Systeme, 30 ff.

mationspraktiken, aber auch Informationsnormen – in ihrer Gestaltung auf die einbettenden Gesellschaftsbereiche zeitigen. Dass z. B. die Flugfahrt als Technologie gemeinhin verbreitet ist, hat hierbei nichts zu bedeuten. Denn nur weil die Flugfahrt eine etablierte Praxis im Transportkontext ist, bedeutet dies nicht zugleich, dass sie eine etablierte Technologie zur Observation im Strafverfolgungskontext ist resp. dass die Vorgaben, die aus strafprozessrechtlicher Sicht an diese formuliert werden, nicht zu beachten sind.

1951 Mit diesen Erläuterungen wird fünftens und abrundend nachvollziehbar, weshalb umfassende Überwachungsmassnahmen, denen sich Reisende an Flughäfen unterziehen, breite Akzeptanz finden. Sie werden unter Privacy-Erwägungen kaum kritisiert: Sie dienen der Erfüllung des *Hauptzweckes des Transportsektors*, dem sicheren Transport von Menschen und Gütern. Die Informationserhebungen verfolgen das Ziel, die Sicherheit der Passagiere zu gewährleisten. Sie sind – zumindest solange sie nicht anderen Zwecken zugeführt und in andere Kontexte überführt werden – *systemkonform*. In dieser Systemkonformität verortet Nissenbaum in ihrer Theorie von «Privacy in Context» das Erklärungsmuster, weshalb bestimmte Informationspraktiken breite gesellschaftliche Akzeptanz finden, andere dagegen heftigen Widerstand auslösen. In Bezug auf die kontextuelle Integrität lösen disruptive Praktiken gesellschaftlich regelmässig Empörung aus (ungeachtet der Frage, ob eine Technologie selbst intensiv genutzt wird).[2423]

1952 Nach diesem Ausflug in die US-amerikanische Rechtsprechung, der sich namentlich mit der Figur der vernünftigen Erwartungen mit Blick auf den Privacy-Schutz und den Umgang der Gerichte mit neuen Technologien befasste, soll die *systembezogene Schutzdimension im Datenschutz* nunmehr unter Bezugnahme auf den kontinentaleuropäischen Rechtskreis exemplarisch erhärtet werden.

1953 Parallelen zum Illustrationsfall der geheimen privatdetektivischen Versicherungsobservation finden sich im Fall Logistep.[2424] Für die Verletzung der Verarbeitungsgrundsätze konnten im konkreten Fall keine überwiegenden privaten oder öffentlichen Interessen zur Rechtfertigung erfolgreich vorgebracht werden. Weder das ökonomische Interesse der Logistep AG noch dasjenige an der Aufdeckung von Urheberrechtsverletzungen würden die umstrittene Vorgehensweise rechtfertigen. Auch wenn sich die Erwägungen des Bundesgerichts auf die Beurteilung des konkreten Falles bezogen, zeigt sich über die individualrechtliche Konfliktlage hinausgehend eine Kollision zwischen verschiedenen Kontexten infolge Personendatenverarbeitungen. Erneut sind es Rationalitäten aus dem ökonomischen Kontext, die den privaten Lebensbereich erodieren. Bundesgerichtlich

2423 Nissenbaum, 3, 142, 158, 181 ff., 186 ff., 235; bestätigen lässt sich dieser Befund anhand der Reaktionen auf die geheime privatdetektivische Versicherungsobservation, den jüngsten Facebook-Skandal, Google Street View usf.

2424 BGE 136 II 508.

wurde namentlich die *Verunsicherung* problematisiert, die aus einer verdeckten Ermittlung im Internet resultiere. Wiederum zeitigt bereits die Möglichkeit einer Informationserhebung disruptive Wirkung auf den Kontext des Privatlebens. Letzterer existiert auch im Online-Bereich und verdient ebenda rechtlichen Schutz.

1954 Eindrücklich sichtbar wurde die Relevanz *kontextueller Erwägungen* für den Datenschutz am *Volkszählungsurteil des Bundesverfassungsgerichts*.[2425] Das ebenda geprägte Grundrecht auf *informationelle Selbstbestimmung* erlangte Prominenz. Parallel zum Subjektschutz finden sich gewichtige Hinweise auf die Relevanz des *informationellen Systemschutzes*. Dass *systemische Schutzerwägungen* datenschutzrechtlich relevant und damit zu integrieren sind, wird über die Erwägungen zum Statistikgeheimnis sowie die anknüpfenden Ausführungen zum Zweckbindungsgrundsatz anerkannt: Die im Kontext der Volkszählung erhobenen Personendaten dürfen nicht ohne Anonymisierung anderen Verwaltungseinheiten zur Erfüllung ihrer Aufgaben zugänglich gemacht werden. Nur das Statistikgeheimnis könne die Kooperationsbereitschaft der Bürgerinnen sowie Bürger und damit deren Bereitschaft, die Fragen wahrheitsgemäss und vollständig zu beantworten, sicherstellen. Müssten die Bürgerinnen und Bürger befürchten, dass sie aufgrund der im Rahmen des Zensus erteilten Personenangaben Konsequenzen und Massnahmen in anderen Bereichen des Verwaltungsvollzuges zu gewärtigen hätten, würde das notwendige Vertrauen unterminiert, das Bedingung für eine korrekte Beantwortung der statistischen Fragen ist. Im Ergebnis würde man das Ziel einer aussagekräftigen Statistik torpedieren. Keine Zwangsmassnahme oder deren Androhung könnte die Integrität der Statistik besser gewährleisten als das Statistikgeheimnis. Darüber hinaus wären organisatorische Massnahmen zu ergreifen, welche die Neutralität der Erhebenden sicherstellen.

1955 Der Aspekt des datenschutzrechtlichen Systemschutzes wird, *pro memoria*, gut sichtbar anhand der verschiedenen *Amts- und Berufsgeheimnisse*. Sie gaben bereits einleitend in dieser Schrift den Impuls, datenschutzrechtliche Grundannahmen zu hinterfragen. *Amts- und Berufsgeheimnisse* formulieren Informationsblockaden für den Fluss von Personendaten. Sie verhindern auch zum Schutz gesellschaftlicher Subsysteme den Transfer von Informationen in andere Bereiche. Es ist die Gestaltung von Informationsflüssen innerhalb und zwischen verschiedenen Systemen, die sich namentlich an der Frage orientiert, welchen Einfluss die jeweilige Strukturierung von Informationsflüssen auf die Verwirklichung oder Erosion der Ziele und Zwecke von involvierten, einbettenden Gesellschaftsbereichen zeitigt. Dies ist als Aufgabe des Datenschutzrechts anzuerkennen.

2425 Vgl. BVerfGE 65, 1 – Volkszählung, Urteil vom 15. Dezember 1983; so auch die Erkenntnis einer Analyse des Urteils, gerade auch mit Blick auf die Ausführungen zur Zweckbindung, vgl. zweiter Teil, V. Kapitel, B.4.

1956 Die Gestaltungsmöglichkeiten gehen weit über die Möglichkeit des «Ja» oder «Nein» eines Datenflusses, eines «alles oder nichts» hinaus. Zwischen dem freien Informationsfluss auf der einen Seite und dem Verbot des Informationsflusses namentlich qua Geheimhaltungspflichten auf der anderen Seite – quasi die beiden Extremlösungen – liegt ein weites Spektrum von Gestaltungsvariationen. Sie ermöglichen es, datenschutzrechtlich ausdifferenzierte, nuancierte und kontextadäquate Lösungen zu formulieren.[2426]

1957 Die Gestaltung der Datenflüsse durch datenschutzrechtliche Normen schützt durchaus das konkrete Individuum und ggf. seine konkrete Beziehung. Sie sichert allerdings zugleich die Funktionstüchtigkeit und Integrität gesellschaftlicher Bereiche ab, in welche die Informationsverarbeitungen eingebettet sind. Das hier entwickelte datenschutzrechtliche Systemparadigma inkludiert das Subjektparadigma.

1958 Illustrativ nochmals das Arztgeheimnis: Das *Arztgeheimnis* verfolgt neben dem Schutz der Persönlichkeit der Patientin auch die Absicherung einer Vertrauensbeziehung zwischen Patientin und Ärztin. Damit wird ein Beitrag zur Gewährleistung der *individuellen Gesundheit* geleistet: Nur eine offene, transparente Informierung vonseiten der Patienten gegenüber dem Medizinalpersonal und die vertrauensvolle Kommunikation über Gesundheitsbelange im Ärztin-Patientin-Verhältnis ermöglicht es der Ärztin, angemessene Massnahmen für die betroffene Patientin zu definieren. Zusätzlich hat das Arztgeheimnis eine kollektiv-institutionelle Dimension. Es sichert die Ziele des *Gesundheitssektors* sowie deren Erreichung und damit die Gesundheit als allgemeines Gut ab.[2427] Vertrauen Menschen nicht darauf, dass die der konsultierten Ärzteschaft eröffneten Informationen diskret behandelt werden, wird riskiert, dass unter Umständen ein erforderlicher Arztbesuch unterbleibt, eine konsultierte Ärztin nur ungenügend und unvollständig informiert wird oder von Arzt zu Arzt gepilgert wird. Im Ergebnis würde damit die *Gesundheit der Allgemeinheit* aufs Spiel gesetzt, gerade bei hoch ansteckenden und schweren Krankheiten. Im Gesundheitsbereich

2426 «We have a right to privacy, but it is neither a right to control personal information nor a right to have access to this information restricted. […] these distinctive systems of what I have called context-relative informational norms, governing flows of personal information, are finely tuned to the internal purposes of contexts and also to some degree responsive to fundamental human rights and values», so Nissenbaum, 131 f.; dazu, dass der access resp. der Zugang zum Schlüsselbegriff in der Informationsgesellschaft wird und wie sich Nutzungsbefugnisse und damit auch die Eigentumskategorie wandeln, m. w. H. auch auf Rifkin, Kube, JZ 2001, 944 ff.; gerade im Zuge der Digitalisierung ist der Befund der Dematerialisierung im Sinne des Verschwindens der körperlichen Schicht von zentraler Bedeutung zur Erfassung neuer rechtlicher Herausforderungen, z. B. im Urheberrecht; Rifkin, Access, 9 ff. beschreibt nicht nur die gegenüber dem Eigentum verdrängende Relevanz von access, sondern auch die Kollision verschiedener gesellschaftlicher Kontexte, wie sie in dieser Schrift als Brennpunkt datenschutzrechtlicher Herausforderungen herausgearbeitet werden – vgl. insofern 19 ff., 183 ff.

2427 Vgl. Nissenbaum, 159 f. 171 ff., 187, 201 f.

untergraben folglich nicht kanalisierte Datenflüsse den Gesundheitssektor selbst. Anzufügen ist, dass das Arztgeheimnis, das mit dem Hippokratischen Eid als eine der ältesten und traditionsreichsten Datenschutzbestimmungen zu bezeichnen ist, jüngst gewisse flankierende Differenzierungen findet. Exemplarisch wurde auf die Bestimmungen im Humanforschungsgesetz hingewiesen. Diese ergingen nicht, weil Ärzte weniger Gewicht auf Vertraulichkeit legen. Vielmehr wird die Eröffnung bestimmter Informationen im Interesse des Gesundheitskontextes an sich zugelassen, um dessen Ziele effizienter zu bewerkstelligen.[2428]

Ähnlich kann das *Steuergeheimnis* als Instrument der Absicherung des Vertrau- 1959
ens der Steuerpflichtigen gelten: Sie deklarieren am ehesten dann vollständig und wahrheitsgetreu ihre Vermögens- und Einkommensverhältnisse, wenn sie sich darauf verlassen können, dass die Angaben nicht an Drittpersonen weitergereicht werden. In den Worten von Andrew Mellon, Finanzminister der Vereinigten Staaten im Jahr 1925:

> «While the government does not know every source of income of a taxpayer and must rely upon the good faith of those reporting income, still in the great majority of cases this reliance is entirely justifiable, principally because the taxpayer knows that in making a truthful disclosure of the sources of his income, information stops with the government. It is like confiding in one's lawyer.»[2429]

Aufschlussreich sodann die *Stimm- und Wahlgeheimnisse*.[2430] Auch sie dienen 1960
nicht nur der Gewährleistung individueller Entscheidungsfreiheit und politischer Meinungskundgabe. Sie nehmen zugleich eine *Garantenstellung für das demokratische System* an sich ein.

Für den demokratischen und politischen Kontext ist der jüngste Facebook- 1961
Skandal in Erinnerung zu rufen. Er illustriert in eindrücklicher Weise die Kollision zwischen Gesellschaftsbereichen wegen Informationsverarbeitungen. Personenangaben, die Facebook-Nutzerinnen über das Netzwerk zwecks persönlicher Beziehungspflege austauschten, wurden mutmasslich an Cambridge Analytica weitergeleitet. Das Unternehmen nahm in der Folge Auswertungen vor. Gestützt darauf wurde gezielt auf das Wahlverhalten eingewirkt, indem spezifisch und selektiv Informationen über die Präsidentschaftskandidaten geschaltet wurden. Mit anderen Worten wurden aus Informationen, ausgetauscht über ein Netzwerk zur Pflege persönlicher und familiärer Beziehungen, Vorlieben, Ängste, Einstellungen usf. ermittelt, um hierauf basierend die Entscheidungsfindung und das Wahlverhalten zu manipulieren. Solche Verarbeitungsprozesse untergraben nicht nur den über die Plattform geführten privaten Lebensbereich persönlicher Bezie-

2428 Vgl. Nissenbaum, 177.
2429 Dies., in: Savirimuthu (ed.), The Library of Essays of Law and Privacy, III, V.; zu den jüngeren Diskussionen Nobel, SJZ 2018, 14 ff., 16; zum Verhältnis zwischen Bankkundengeheimnis und Steuergeheimnis Meyer, in: Schmid (Hrsg.), 244 ff., 247.
2430 Vgl. Art. 283 StGB.

hungspflege des Einzelnen sowie die freie und persönliche Willensbildung als Bürgerin und Wahlberechtigte. Sie wirken sich disruptiv auf das demokratische Staatssystem aus.

1962 Mit all diesen Beispielen wurde die *Notwendigkeit eines Paradigmenwechsels für das Datenschutzrecht der Zukunft* erhärtet: Eine angemessene datenschutzrechtliche Regulierung wird möglich, wenn der Fokus auf eine Subjekt-Objekt-Beziehung, ein Datensubjekt und Personendaten als Quasi-Objekte gelöst wird. Notwendig ist eine Betrachtungsweise, die Datenflüsse in das Zentrum der Aufmerksamkeit stellt. Flüsse von Personendaten sind in ihrer Einbettung in verschiedene gesellschaftliche Bereiche zu betrachten.[2431] Das *Datenschutzrecht der Zukunft* hat als *Schutzzweck konsequent nicht nur den Subjektschutz*, sondern *auch den Systemschutz* zu adressieren. Regelmässig inkludiert der Systemschutz den Subjektschutz. In einem die *Kontextintegrität wahrenden Datenschutzrecht* findet ein *ausdifferenzierter Einsatz informationsrechtlicher Gestaltungsmöglichkeiten* statt, der bestmöglich die Integrität der involvierten Gesellschaftsbereiche achtet.

1963 Um ein systemadäquates Datenschutzrecht zu konstruieren, drängt sich die Bildung von *Szenarien* auf. In der Folge wird unter Berücksichtigung der jeweils involvierten Gesellschaftsbereiche, der Personen in ihren verschiedenen Rollen sowie der Ziele und Zwecke der jeweiligen Bereiche evaluiert, welche Auswirkungen unterschiedliche Gestaltungsmechanismen mit Blick auf Personendatenflüsse auf die Funktionstüchtigkeit und die Zielerreichung der auf dem Spiel stehenden Gesellschaftsbereiche zeitigen.

1964 Das ist die Richtung, in welche die bereits zitierten Worte von Simitis weisen, wonach es nicht die Struktur des Persönlichkeitsrechts, sondern die Struktur der Gesellschaft ist, die das Datenschutzrecht bestimmt.[2432] Oder derselbe Autor mit den Worten:

> «In dem Masse freilich, in dem die Verarbeitung personenbezogener Daten zum Unterfall des allgemeinen Persönlichkeitsrechts erklärt wird, verengt sich auch die Regelungsperspektive. Die Auseinandersetzung mit der Verarbeitung und ihren Folgen gerät zum rein individuellen Problem, für dessen Lösung, so scheint es, lediglich die Grundsätze in Betracht kommen können, die ansonsten ebenfalls bei der rechtlichen Bewertung von Eingriffen in individuelle Rechtspositionen zu beachten sind.»[2433]

1965 Der Zweck des Datenschutzrechts wird damit nicht mehr isoliert im Persönlichkeitsschutz verortet. Er wird *ergänzt* um die Dimension des systemischen Schutzzweckes.

2431 Richtungsweisend Nissenbaum, insb. 186 ff. und 231 ff.
2432 Insofern Simitis im Interview, <https://www.datenschutzzentrum.de/artikel/940-Interview-mit-Prof.-Dr.-Dr.h.c.-Spiros-Simitis.html> (zuletzt besucht am 30. April 2021).
2433 Ders., Einleitung: Geschichte – Ziele – Prinzipien, NomosKomm-BDSG, N 26.

Mit den Beispielen wurden in erster Linie *Informationsblockaden* zum Zweck des Schutzes von Systemen und Kontexten angesprochen. In der eingehend diskutierten Konstellation der geheimen Observation im IV-Versicherungskontext wurde die fehlende Informationsblockade resp. der *Transfer von Personendaten*, die durch das geheime Ausforschen des Privatbereiches gewonnen und in den Versicherungsbereich eingespeist wurden, kritisiert. Korrumpiert würde die Integrität des Kontextes des privaten Lebens, der Sozialversicherung sowie des Gesundheitsbereichs. 1966

Es gibt aber auch die entgegengesetzte Konstellation: die Situation, in welcher das *bisherige weitreichende Verbot eines Informationstransfers disruptive Auswirkungen auf die Kontexte* zeitigt. Das Beispiel, das den bis vor Kurzem weitgehend unterbundenen Informationstransfer problematisiert, ist im *Institut der Adoption und im Adoptionsrecht* zu finden. Anhand der informationsrechtlichen Regelungen zur Adoption zeigt sich die Relevanz von (unterbundenen) Informationsflüssen für die Persönlichkeit, Identität und einen privaten Lebensbereich sowie für das Familienleben resp. die Gestaltung familiärer Beziehungen.[2434] Die Schweiz kannte bis zum 1. Januar 2018 einzig die sog. Inkognitovolladoption, in deren Konzept grundsätzlich keine informationelle Verbindung zwischen dem adoptierten Kind (und der Adoptivfamilie) auf der einen Seite und der leiblichen Familie auf der anderen Seite gewahrt werden soll. Das Konzept des *clean break* sollte, so wurde es lange vertreten, dem Wohl des Kindes dienen, ebenso den Adoptiveltern wie den leiblichen Eltern. Man zielte darauf ab, allen Beteiligten die Führung eines Lebens zu ermöglichen, «als ob» es nie zu einer Adoption gekommen wäre, als ob nie eine Mutter ein Kind weggegeben hätte, Eltern kein Kind geboren hätten usf. Die Adoptivfamilie sollte durch die geheime Volladoption eine «ganz normale», sprich quasi natürliche Familie sein können, was zusätzlich durch die Fiktion der Geburt durch die Adoptiveltern mittels Registervorgangs symbolisiert wird. Besagtes Modell wurde im Zuge der jüngsten Revision angepasst, wobei der adoptionsrechtliche *clean break* relativiert wird und in differenzierter(er) Weise Informationenflüsse zugelassen werden.[2435] Für diese Anpassungen sprachen viele Argumente aufseiten aller Parteien des Adoptionsdreiecks.[2436] 1967

Bei der geheimen Adoption torpedieren die Nichtinformation des Kindes über seine Herkunft, der unterbundene Fluss von Informationen über seine Herkunftsfamilie, die Motive der leiblichen Eltern für ihren Entscheid, ihre Lebenssituation, über vorhandene Geschwister, Gesundheitsthemen in der leiblichen Familie usf., aber auch zu seiner Herkunftskultur das *Kindeswohl*, das seine Identität, die Identitätsbildung und die Gesundheit umfasst. Für das adoptierte Kind sind 1968

2434 Vertiefend Pfaffinger, N 179 ff.
2435 Vgl. neu Art. 268b–e ZGB.
2436 Vgl. Pfaffinger, N 139 ff.

insofern (unter anderem) seine beiden familialen Bezüge relevant und somit die Zulassung des Informationsflusses zum familialen und kulturellen Herkunftssystem. Die Unterbindung von Informationsflüssen zwischen Kind und Herkunftskontext bei der geheimen Adoption untergräbt nachweislich das Wohl, die Integrität des Kindes als Individuum und seine Identität(sbildung), die aus zwei familialen und kulturellen Welten mitkonstituiert wird. Diese erfolgte – vermeintlich – zum Schutz des Systems der Adoptivfamilie. Erfahrungen und Studien zu dieser «Informationspraxis» im Adoptionsrecht haben deutlich werden lassen, dass die *Unterbindung des Informationstransfers* die Kontextintegrität stören kann. Für dieses Feld wurde ein differenziertes Regime vorgeschlagen, wobei der schweizerische Gesetzgeber mit der jüngsten Revision des Adoptionsrechts einen Schritt in diese Richtung vorgenommen hat. Etwas allgemeiner betrachtet lässt sich feststellen, dass sich innerhalb des Familienrechts ein «Familieninformationsrecht» herauszubilden scheint. Die Anerkennung von Informationsansprüchen im Kontext familiärer Systeme basiert regelmässig auf Erwägungen zur Persönlichkeit und Identität, womit das «Privatleben», der persönliche, individuelle Lebensbereich in Abgrenzung zum familiären Lebensbereich adressiert und koordiniert wird.[2437]

1969 Um der Notwendigkeit Rechnung zu tragen, im und über das Datenschutzrecht plurale Verarbeitungszusammenhänge miteinander zu harmonisieren, gibt es *diverse Möglichkeiten zur Gestaltung von Informationsflüssen*. Der differenzierende Einsatz der Instrumente («Transmissionsprinzipien» in der Terminologie von Nissenbaum) ist ein Kernelement für ein kontextgerechtes Datenschutzrecht, ein Recht auf informationellen Systemschutz.[2438] Das Datenschutzrecht der Zukunft hat verstärkt die einbettenden Gesellschaftsbereiche zu berücksichtigen.[2439] Es geht um die rechtliche Gestaltung von Datenflüssen. Zur Harmonisierung der jeweils auf dem Spiel stehenden Kontexte qua informationsrechtlicher Gestaltung dienen manchmal die Blockade des Informationsflusses, womit die Geheimhaltung das Instrument der Wahl ist. In anderen Konstellationen ist es die differenzierte Zulassung von Informationsflüssen oder die Einwilligung.[2440] Es sind weder Kontrollen oder Einwilligungskonstruktionen noch Geheimnisse *per se*, die über sämtliche Bereiche hinweg in hegemonialer Weise vonseiten des Da-

2437 Vgl. auch Dies., FamPra.ch 2014, 604 ff.

2438 Nissenbaum, 145 ff., 201 f., 217 ff.; auf Deutsch übersetzt mit dem Terminus der Übertragungsgrundsätze, Dies., in: Heinrich-Böll-Stiftung (Hrsg.), 53 ff., 60 f.; vgl. Druey, in: Brem/Druey/Kramer/Schwander (Hrsg.), der z. B. die Unterbindung von Information als organisatorisch radikale Lösung beurteilt, 877 ff., 889; nicht spezifisch für das Datenschutzrecht zu verschiedenen rechtlichen Gestaltungsmöglichkeiten von Informationsflüssen bereits Dreier, in: Bizer/Lutterbeck/Riess (Hrsg.), 65 ff., 71 ff.

2439 Vgl. Nissenbaum, 189 ff.

2440 Für die Umsetzung von Zugangsbeschränkungen resp. Informationsblockaden sind technische Massnahmen wie Firewalls von hoher Bedeutung, hierzu Cavoukian/Chibba/Williams/Ferguso, Jusletter IT vom 21. Mai 2015, N 11.

tenschutzrechts die angemessene Antwort liefern können.[2441] Vielmehr ist unter Berücksichtigung der jeweiligen Ziele und Zwecke der hinter den Verarbeitungsprozessen stehenden Kontexte und Systeme zu evaluieren, wie die Verarbeitungsprozesse zu gestalten sind, damit diese mit ihren spezifischen Zielen bestmöglich geschützt werden.[2442]

1970 Die Beispiele, anhand derer die systemische Schutzdimension datenschutzrechtlicher Herausforderungen illustrierbar ist, liessen sich beliebig fortführen. Um nur ein weiteres zu nennen: die Omnibus Information Providers, die Informationen aus diversen Quellen und von unzähligen Akteuren sammeln und ebenso diffus distribuieren.[2443] Für die hier generierten enormen Datenbestände wurden namentlich drei Kernprobleme systematisiert: erstens Sicherheitsaspekte infolge und im Sinne von Zugriffen durch «unerwünschte» Personen und damit die Zuführung in andere Kontexte, zweitens die Irrtumsraten, indem bei grossen Datenbeständen Verwechslungen sowie Fehlschlüsse vorkommen – zu nennen sind insofern Bonitäts- und Krediteinschätzungen sowie (falsche) medizinische Behandlungen –, und drittens das sog. Social Sorting, womit der Konnex zwischen privacy und Gleichheit angesprochen wird: Personen werden in Slots eingeteilt, ggf. diskriminiert, und erhalten unterschiedliche Behandlungen aufgrund solcher Entscheidungen, woraus unter Umständen eine segmentierte Gesellschaft resultieren kann.[2444] Manipulatives Marketing untergräbt die freie und informierte Wahl der Konsumenten. Müssen Konsumenten eruieren, was ihnen nicht angeboten wird usf., wird das Element der Ineffizienz in den Markt eingeführt. Oder sie verzichten auf den Konsum resp. suchen nach Alternativen. Gegenseitiges Vertrauen in den Markt ist fundamental; geht es verloren, resultieren negative Konsequenzen, hier ebenso auf den freien, wettbewerbsbasierten Marktplatz.[2445] Entsprechend wird die Bedeutung des Datenschutzrechts auch für den wirtschaftlichen Fortschritt und namentlich den digitalen Handel neu explizit von der DSGVO anerkannt.[2446]

1971 Im *Anstellungskontext* ist ein System, das keinerlei Restriktionen für die Erhebung von Informationen zu potentiellen Arbeitnehmenden vorsieht, zwar geeig-

2441 Vgl. Druey, in: Brem/Druey/Kramer/Schwander (Hrsg.), 379 ff., 395, der nicht spezifisch datenschutzrechtlich auf die optimale Gestaltung von Informationsflüssen hinweist, womit weder ein maximales noch ein minimales Mass an Information per se erstrebenswert ist; vgl. zu verschiedenen rechtlichen Gestaltungsmöglichkeiten von Informationsflüssen bereits Dreier, in: Bizer/Lutterbeck/Riess (Hrsg.), 65 ff., 71 ff.; dazu, dass privacy nicht Kontrolle an Personendaten bedeutet, Schwartz, Wis. L. Rev. 2000, 743 ff., 755 ff.

2442 Richtungsweisend Nissenbaum, 1 ff., 231 ff.

2443 Vgl. z. B. Weichert, wrp 1996, 522 ff., 523 ff.; hierzu dritter Teil, VII. Kapitel, B.2.

2444 Vgl. Nissenbaum, 205 ff., insb. 208 mit einem Verweis auf den Juristen Strahilevitz, dem gemäss Differenzierungen nicht per se unzulässig seien; unzulässig sollen unfaire Differenzierungen und nicht nachvollziehbare Sortierungen sein.

2445 Dies., 213.

2446 Vgl. insb. ErwG 2, 5, 7, 9.

net, die Interessen einzelner Unternehmen gut zu bedienen, allerdings ggf. Menschen bestimmter Religionen oder mit Handicaps oder Frauen zu exkludieren. Im Ergebnis können unbeschränkte Datenverarbeitungen in einer suboptimalen Nutzung der Human Resources münden.[2447] Der Anstellungskontext ist ein besonders konfliktbehaftetes Feld, da hier ein intensiver Informationsaustausch stattfindet, der aber nicht immer harmonisch ist. Er kollidiert mit einem Recht auf Autonomie des Subjektes im Sinne der Selbstpräsentation der Kandidierenden, das seinerseits vom Interesse des Arbeitgebers konterkariert wird, die Informationen zu verifizieren. Auch solche Prozesse sollen bezüglich der Ziele, Zwecke und Werte der Kontexte analysiert werden. Zu viel Autonomie beim Subjekt führt ggf. zu Fehlanstellungen mit Produktivitätseinbrüchen, wohingegen zu viel Kontrollmöglichkeit bei den Unternehmen ggf. zurückhaltende oder überkorrekte Kandidatinnen verhindert.[2448]

1972 In Bezug auf die *politische Teilhabe* etabliert sich ein Vorgehen, wonach politische Parteien vermehrt Unternehmen einschalten, die «hoch qualitative Informationen für politische Organisationen» beschaffen. Beim Facebook-Skandal wird zwar von einem Datenleck gesprochen, doch das Ergebnis war, dass Personen, welche die Plattform zur persönlichen Kommunikation nutzen wollten, gezielt für den Wahlvorgang des amerikanischen Präsidenten manipuliert wurden. Man riskiert, dass die öffentliche Debatte vermindert wird, womit man dem politischen Kontext an sich schadet, gelten doch die informierte Bürgerin und der autonome Bürger als relevant für eine funktionierende Demokratie.[2449] Während in einer Demokratie Bürger unter Geheimhaltung wählen und abstimmen, wird politischen Repräsentanten, die Rechenschaft ablegen müssen, nicht dieselbe Autonomie zugestanden. Ihre Autonomie ist anders und geringer als diejenige der Bürgerinnen und Bürger bei der Wahl.[2450]

1973 Im Kontext der *Erziehung* lässt sich eine Kollisionskonstellation beschreiben, wenn beispielsweise Personendaten aus einem Studierendenerfassungsprogramm – wie es ein sog. Primius-Programm einer Universität darstellt – an die Arbeitgeber gereicht werden. Eine solche Praxis, wonach Angaben über die besten Studierenden an Arbeitgeber eröffnet werden, birgt Risiken dergestalt, dass Unternehmen Ideen hinausziehen, Schulen ihre Curricula anpassen, Unternehmen

2447 Vertiefend zum Fall Söbbing, InTeR 2018, 182 ff.; Nissenbaum, 214.
2448 Nissenbaum, 177.
2449 Kübler, SDF, 1; in diesem Sinne auch in Bezug auf das E-Voting Engi/Hungerbühler, medialex 2006, 17 ff., 20; Nissenbaum, 214; Spiecker genannt Döhmann, in: Epiney/Sangsue (Hrsg.), 1 ff., 3 ff.; kritisch zur Relevanz der Informiertheit Milic, NZZ am Sonntag vom 16. Juni 2018, Die Informiertheit des Stimmvolks ist gar nicht so wichtig, <https://nzzas.nzz.ch/meinungen/die-informiertheit-des-stimmvolks-ist-gar-nicht-so-wichtig-ld.1395421?reduced=true> (zuletzt besucht am 30. April 2021).
2450 Nissenbaum, 176 ff.

Einfluss auf die Universität nehmen: Der Bildungskontext kann korrumpiert werden durch entsprechende Datenflüsse.[2451]

Sämtliche Beispiele zeigen, dass es aus einer Datenschutzperspektive zu kurz greift, isoliert das Individuum und Datensubjekt, seinen Schutz, seinen Willen, seine Persönlichkeitsverletzung zu adressieren. Vielmehr ist es ebenso Aufgabe und damit Zweck des Datenschutzrechts, die gesellschaftlichen Bereiche, Kontexte und Systeme angemessen zu schützen, in welche die Personendatenflüsse und Verarbeitungsprozesse eingebettet sind. Die diversen etablierten Gesellschaftsbereiche bilden die Hintergrundfolie für die datenschutzrechtliche Thematisierung. Das Datenschutzrecht zeigt sich damit nicht als isolierte, eigenständige und losgekoppelte Rechtsmaterie. Vielmehr ist *Datenschutzrecht systemrelatives Recht*. Die rechtliche Strukturierung der Vorgaben an die Datenflüsse und Verarbeitungshandlungen haben nachhaltigen Einfluss auf den Schutz der Integrität resp. die Erosion von sozialen Kontexten, die ihrerseits bestimmte Ziele und Zwecke verfolgen. Folglich ist für das Datenschutzrecht *nicht von einer dualistischen Struktur der Gesellschaft von öffentlich versus privat* auszugehen, stattdessen von einer *pluralistischen Struktur*. Gleichermassen ausdifferenziert zum Einsatz zu kommen haben dann die verschiedenen Mechanismen und Instrumente, die Datenverarbeitungsprozesse strukturieren und gestalten. Kein Instrument ist im Alleingang in der Lage, diese komplexen Herausforderungen angemessenen Lösungen zuzuführen. Mit diesen Ausführungen ist es möglich geworden, Strukturmerkmale eines Rechts auf informationellen Systemschutz zu umreissen. 1974

C. Systemrelatives Datenschutzrecht

1. Theoretischer Rahmen, Einbettung und Elemente

Für die Entwicklung einer Theorie vom Recht auf informationellen Systemschutz ist das Konzept der kontextuellen Integrität resp. die «Privacy in Context»-Theorie von Nissenbaum leitend. Ihr Konzept der «Privacy in Context» knüpft an Studien namhafter Vertreter systemischer resp. kontextueller Gesellschaftstheorien an, namentlich an die von Weber, Goffman, Parsons, Powell, Luhmann, Walzer oder Bourdieu.[2452] Die US-amerikanische Philosophin Nissenbaum statuiert: 1975

2451 Dies., 169 ff.

2452 Für eine rechtswissenschaftliche Studie, die ein Recht auf informationellen Systemschutz vorschlägt, sind sodann namentlich die Beiträge von Teubner massgeblich.

> «A right to privacy is a right to context-appropriate flow. The point of departure is a commitment to appropriate flow and not to control or secrecy.»[2453]

1976 Angemessen meint hier gerade nicht, was Zivilrechtswissenschaftler der Schweiz gemeinhin mit Art. 4 ZGB und dem Ermessensbegriff assoziieren würden. Es geht nicht um die Realisierung der Einzelfallgerechtigkeit unter Berücksichtigung sämtlicher Umstände des Einzelfalles. Vielmehr gelten Personendatenflüsse dann als angemessen, wenn ihre Gestaltung die grösseren gesellschaftlichen Herausforderungen zu adressieren und die Integrität der jeweiligen sozialen Bereiche mit ihren spezifischen Zielen, Zwecken und Rationalitäten zu schützen vermag. Hierzu nochmals Nissenbaum:

> «[…] privacy as contextual integrity is a complex, delicate web of constraints on the flow of personal information that itself brings balance to multiple spheres of social and political life.»[2454]

1977 Der Ansatz der Autorin ist stark sozialwissenschaftlich geprägt. Nissenbaum macht sich zur Detektion und Verifizierung ihrer These und ihres Konzepts die gesellschaftlichen Reaktionen zunutze, welche bestimmte Personendatenverarbeitungen auslösen oder gerade nicht auslösen. Nicht alle Personendatenverarbeitungen stossen in der Allgemeinheit auf Skepsis, Widerstand oder Entrüstung. Einige Datenverarbeitungen werden, trotz ihrer Breite und Tiefe, gesellschaftlich gut akzeptiert. Im Zuge der COVID-19-Krise dürfte das sichtbar geworden sein. Die *gesellschaftlichen Reaktionen* setzt Nissenbaum als Seismografen zur Aufdeckung von *Verletzungen kontextueller Integrität* ein.[2455]

1978 Zur Illustration: Die Unterbreitung von Buchvorschlägen auf Amazon wird, vergleichbar zur Empfehlung durch eine kompetente Buchhändlerin, als positive Dienstleistung verstanden.[2456] Anders dagegen wird das Cross-Side-Tracken, wie es z. B. DoubleClick vornimmt, kritisch wahrgenommen.[2457] Beispielloses Empören löste die Nutzung von Personendaten aus, die auf Facebook – einer Plattform zur Pflege persönlicher Beziehungen – gesammelt und der (Aus-)Nutzung im politischen Zusammenhang zugeführt wurden.[2458]

1979 Die Rahmenstruktur für Nissenbaums Theorie der «kontextuellen Integrität» basiert zudem auf der Erkenntnis, wonach der Umgang mit Datenverarbei-

2453 Nissenbaum, 127.
2454 Dies., 128.
2455 «Generally, people are unnerved to discover they are „known" when they enter what they believe to be a new setting; we dislike having information about ourselves divulged out of context», vgl. Nissenbaum, 50; zur sog. «Gefühlstheorie» von Ehrlich vgl. Rehbinder, 46.
2456 Vgl. Vesting, in: Ladeur (Hrsg.), 155 ff., 160 f.
2457 Vgl. Toubiana/Narayana/Boneh u. a., 1 ff.; Nissenbaum, 195; hierzu auch Langheinrich/Karjoth, digma 2012, 116 ff., 121 ff.
2458 Illustrativ hierfür die Titulierung als (Daten-)Skandal auch in wissenschaftlichen Beiträgen Söbbing, InTeR 2018, 182 ff.

tungstechnologien als *sozio-technische Praxis* zu beschreiben ist.[2459] Für die Geistes-, Sozial- und Rechtswissenschaften folgt hieraus, dass die jeweiligen Technologien in ihrer Einbettung und den daraus resultierenden Auswirkungen auf die sozialen Interaktionen zu analysieren sind.[2460]

Nachfolgend sollen zwecks Theoriebildung vor dem Hintergrund besagter Studien sowie der in dieser Schrift zum Datenschutzrecht gewonnenen Erkenntnisse Kernbegriffe und -elemente eines Systemparadigmas im Datenschutzrecht präzisiert werden. 1980

Von grundlegender Bedeutung ist der *Terminus des Systems resp. Kontextes*. Die Begriffe «Systeme», «Kontexte», «gesellschaftliche Bereiche» oder «Sphären», aber auch «Institutionen» kamen in dieser Schrift bislang mit einer gewissen Differenzlosigkeit und Ungenauigkeit zum Einsatz. Dieses schematische Vorgehen geschah wohl wissend, dass sich die Begriffe teilweise überlappen, teilweise unterscheiden.[2461] Die Unschärfe kann hingenommen werden, da es in erster Linie darum geht, (anti-)thesenhaft einen Kontrapunkt zu benennen: Alle Begriffe repräsentieren einen *Gegenbegriff* oder ein *neues Paradigma* gegenüber einem am Subjekt, der Person, dem einzelnen Individuum ausgerichteten Schutzkonzept. Ersteres lässt sich als *systemisches oder auch kontextuelles Datenschutzparadigma*, kurz *informationelles Systemschutzparadigma* charakterisieren. Letzteres lässt sich als *individualistisches Datenschutz- resp. Privatheitsparadigma* resp. *Subjektschutzparadigma* beschreiben. 1981

Kontexte sind strukturierte soziale Systeme, die sich entwickelt haben, um bestimmte als grundlegend angenommene Aspekte des Lebens zu organisieren und entsprechende Werte und Ziele zu erreichen.[2462] Sie werden durch Beobachtung der Gesellschaft festgestellt. Beschrieben werden soziale Kontexte in erster Linie durch die Anthropologie sowie die empirische Sozialforschung.[2463] Die strukturierten sozialen Bereiche haben sich über die Zeit herausgebildet. Bedeutsame gesellschaftliche Kontexte resp. Systeme sind der Gesundheitsbereich, der Erziehungs- und Bildungskontext, der Arbeitskontext, Familie, Ehe und Elternschaft sowie Freundschaft, der religiöse oder politische Kontext sowie der kommerzielle 1982

2459 Nissenbaum, 148 ff., 161, 189 ff.; der Terminus wird in Bezug auf den Beschäftigungskontext auch von Bosse/Dietrich/Kelbert u. a., Jusletter IT vom 28. Februar 2020, N 175 ff., N 180 verwendet.

2460 Unter Referenz auf Luhmann und die sich im Zuge der Corona-Krise präsentierenden Konflikte zwischen verschiedenen gesellschaftlichen Systemen, insb. Wissenschaft und Politik, Sienknecht/Vetterlein, NZZ vom 3. Juni 2020, 8.

2461 Zu den Grundbegriffen der Soziologie auch Rehbinder, 40 ff.

2462 Der Begriff wird vonseiten der Sozialwissenschaft und Philosophie definiert, allerdings nicht immer einheitlich; vgl. zu den verschiedenen gesellschaftlichen Sphären resp. Kontexten und namentlich zur Verteilung verschiedener Güter Walzer, 26 ff. und in Bezug auf die verschiedenen Sphären wie den Marktplatz, 167 ff., Ämter, 195 ff., Erziehung und Bildung, 288 ff., Verwandtschaft und Liebe, 327 ff. oder politische Macht, 399 ff.; vgl. zum Begriff auch Nissenbaum, 132.

2463 Nissenbaum, 135.

Marktplatz, auf welchem Subjekte als Händler, Anbieter oder Konsumentinnen agieren.[2464] Bei den Kontexten handelt es sich mit anderen Worten um *abstrakte Repräsentationen von sozialen Strukturen*, die im täglichen Leben erfahren, erlebt und gelebt werden.[2465]

1983 Charakterisiert werden sie durch *spezifische Aktivitäten, Rollen, Beziehungen, Machtstrukturen, Normen und Regeln sowie intrinsische und interne Werte sowie Rationalitäten*, die mittels *Zielen und Zwecken* umschrieben werden.[2466] Zudem sind oft spezifische Lokalitäten und Güter sowie Distributionsprinzipien für die jeweiligen Systeme typologisch. Menschen agieren nicht einfach von Mensch zu Mensch. Sie handeln in *Rollen*, die von den sozialen Sphären strukturiert werden.[2467] Aufgrund ihrer Rolle in den jeweiligen Kontexten agieren sie mit typischen Kapazitäten und Eigenschaften: z. B. als Patientin, als Schüler oder Studentin, als Professorin oder Lehrer, als Nachbarin, Arbeitgeber, Therapeutin, Freund, Ehefrau usf.[2468] Menschen bewegen sich in der Regel *parallel* in mehreren Gesellschaftsbereichen.[2469] Hieraus können sog. Rollenkollisionen resultieren. Exemplarisch insofern die Chefin, die über eine Anstellung des eigenen Cousins entscheiden soll (Meritokratie versus Nepotismus), oder der Vater, der im Zuge der COVID-19-Krise gleichzeitig neben der Elternrolle als Lehrer das Home-Schooling bewerkstelligen und seine Rolle als Arbeitnehmer in einem Unternehmen wahrnehmen soll.

1984 Die jeweiligen sozialen Bereiche werden von *spezifischen internen Logiken* beherrscht.[2470] Über ihre aktuelle Rolle werden Personen in den spezifischen Kontexten an einschlägige Spielregeln sowie Normerwartungen gebunden. Mit den spezifischen internen Rationalitäten und Logiken von Kontexten sowie Rollen eng verknüpft sind somit *Normen und Normerwartungen:* Sie strukturieren Kontexte resp. soziale Systeme ganz wesentlich. Normen und Normerwartungen leisten einen Beitrag zur Erreichung der Ziele und Zwecke eines Kontextes.[2471] Normen definieren die Pflichten, Erwartungen und Privilegien der Akteure in ihren Rollen und differenzieren zwischen akzeptablem und nicht akzeptablem

2464 Dass privacy in grundlegender Weise mit dem Schutz von Zielen und Beziehungen fundamentaler Bereiche wie Freundschaft oder Vertrauen zusammenhängt, wurde insb. von Fried, Yale L.J. 1968, 475 ff., 477 ff., beschrieben.

2465 Nissenbaum, 134; vgl. zur Gesellschaft als System mit ihren ausdifferenzierten Subsystemen Donos, 33 ff.

2466 Nissenbaum, 132 ff.

2467 Vgl. Rehbinder, 40 f.; vgl. auch Rössler, Eurozine vom 27. Februar 2015.

2468 Auf das Recht und spezifisch das Persönlichkeitsrecht übertragen, bedeutet dies nichts anderes, als dass es eine «einheitliche» Persönlichkeit nicht gibt; sie ist – abhängig vom jeweils einbettenden Kontext – variabel.

2469 Vgl. Nissenbaum, 136 f.

2470 Nissenbaum, 131; hierzu auch Teubner, in Brüggemeier (Hrsg.), 155 ff., 161 ff. und Ders., Der Staat, 2006, 161 ff., 165.

2471 Vgl. zu den sozialen Normen und den soziologischen Rechtsbegriffen Rehbinder, 44 ff.; Nissenbaum, 139.

Verhalten. Es lässt sich eine grosse Variabilität von Normentypen feststellen, von den «gesetzlichen» Normen des Rechtssystems, die in vorgesehenen Rechtssetzungsverfahren formell erlassen und behördlich durchgesetzt werden, über Brauch und Sitte bis hin zu Knigge und «Netiquette».[2472] Normen und Normerwartungen finden sich nicht erschöpfend im positiven Recht. Gerade im Familienkontext gibt es wirkungsmächtige Normerwartungen, die nicht rechtlich verankert sind. Im Erziehungskontext, in welchem Kinder als Lernende, Lehrerinnen als Lehrende agieren, wird erwartet, dass Lehrpersonen sowohl fachlich als auch pädagogisch kompetent sind, dass Schülerinnen und Schüler aufmerksam sind, sich korrekt verhalten und ihre Hausaufgaben machen.

1985 Damit werden Kontexte resp. soziale Systeme durch spezifische *Werte* geprägt, die ihrerseits durch Zwecke und Ziele repräsentiert werden: Die Transmission von Wissen, Können und sozialem Verhalten im Bildungskontext, die Heilung, Linderung und Bewahrung von Gesundheit im Gesundheitskontext usf.

1986 Regelmässig finden sich für bestimmte Kontexte typische *Lokalitäten*, so im Bildungsbereich Schulen und Universitäten, im Gesundheitsbereich Praxen und Spitäler, im religiösen Kontext z. B. Kirchen. Die Kontexte werden weiter von charakteristischen *Aktivitäten* strukturiert, so das Interview im Rahmen von Stellenbesetzungen, die Erhebung der Familienanamnese bei medizinischen Behandlungen oder das Beten in der Kirche. Oft lassen sich spezifische, formalistische und formalisierte Abläufe und Sequenzen beschreiben, etwa in Meetings, Gottesdiensten usf. Sämtliche Elemente verleihen Kontexten und Systemen ihren Charakter und ihre Struktur. Der Grad der Strukturierung und Institutionalisierung variiert von Kontext zu Kontext: Gewisse Kontexte und kontextuelle Aktivitäten sind wenig, andere hoch ausdifferenziert.[2473]

1987 Ein *wesentlicher Faktor der sozialen Differenzierung* ist das *Gut*. Die jeweiligen Sphären werden, zumindest teilweise, durch jeweils unterschiedliche soziale *Güter* geprägt.[2474] Walzer hat, dies reflektierend, in «Spheres of Justice: A Defense of Pluralism and Equality» einen *pluralistischen Ansatz für seine Gerechtigkeitstheorie* präsentiert: Walzers Ausgangspunkt ist eine Gesellschaft mit multiplen Sphären – Erziehung und Bildung, Marktplatz, Politik, Religion und Gesundheit.

2472 Rehbinder, 44 ff.; Nissenbaum, 139.

2473 Hochausdifferenziert ist die Kindergeburtstagsparty, die mit einer «kindgerechten» Einladung eingeleitet wird, zu der man infolge «natürlicher» Bedürfnisse der Kinder wie Essen und Mittagsschlaf pünktlich erscheinen muss. Eltern verlassen in der Regel die Party, während der Geburtstagsfeier werden Spiele gemacht, Kuchen und Süssigkeiten verspeist, Geschenke gebracht, ausgepackt usf.; das Recht hat seinerseits eine starke Strukturierungswirkung; vgl. Nissenbaum, 130 ff.

2474 Walzer, 26 ff. und 30 ff.

Sein Augenmerk richtet er auf die sozialen Güter und die Distributionsprinzipien.[2475] Der Philosoph geht von einer komplexen Gleichheit aus.

1988 Soziale Güter gewisser Sphären werden nach den *Prinzipien der jeweiligen Sphäre* verteilt, die mit den Zielen und Prinzipien besagter Sphäre kompatibel sind: Studienplätze sollen an die Talentiertesten und Besten (Meritokratie), nicht an die Reichsten vergeben werden; die Besetzung einer Arbeitsstelle orientiert sich am Ziel, die am besten geeignete Person, ungeachtet des Geschlechts oder einer allfälligen Verwandtschaft mit der stellenbesetzenden Person, zu finden. Politische Ämter werden in einem demokratischen System nicht erkauft oder aufgrund von «Familiendynastien» (vergleichbar mit einem Erbgang) erlangt. Vielmehr ist die Überzeugungskraft ausschlaggebend. In einer Demokratie stellt hinsichtlich der Vergabe von Politikämtern das Majoritätsprinzip und nicht das Geld oder die Familienzugehörigkeit das Distributionsprinzip dar. Dagegen sollte eine Beförderung auf Leistungen, Einsatz und Qualifizierungen basieren und nicht einer Wahl. Akademische Titel werden durch den wissenschaftlichen und didaktischen Verdienst erlangt, wohingegen Kumpanei die Rationalitäten universitärer Institutionen und damit der Forschung sowie deren Fortschritt durchkreuzt. *Ungerechtigkeit* wird in erster Linie dort verortet, wo *Güter einer bestimmten Sphäre* nicht *nach den Prinzipien der einschlägigen Sphäre* verteilt werden, stattdessen nach anderen, kontextfremden Kriterien.[2476] Wird ein spezifisches Gut wie z. B. die familiäre Herkunft oder das Geld expansiv über zahlreiche Kontexte hinaus zur Währung, resultiert hieraus ggf. Ungerechtigkeit. Die Dominanz eines bestimmten Gutes über verschiedene Kontexte hinweg kann gleichzeitig Ursache wie Ausdruck der *Korrumpierung* eines Bereiches durch einen anderen sein.[2477]

1989 Der Beitrag Walzers lieferte eine Inspirationsquelle für die Schöpfung der Theorie von «Privacy in Context» durch Nissenbaum.[2478] In der vorliegenden Arbeit wurde u. a. gezeigt, inwiefern Personendaten resp. Informationen zu Gütern transformiert werden.[2479] Damit zusammenhängend wurde die expansive Wirkung ökonomischer Rationalitäten problematisiert.

1990 Vor diesem Hintergrund ist geklärt, warum ein *Eigentum an (Personen-)Daten* als durchschlagende und monistische Lösung nicht in Frage kommt. Personendaten könnten ungeachtet ihrer Bedeutung für kontextuelle Erwägungen «er-

2475 Vgl. zu Distributionsfragen im Zusammenhang mit privacy rule Allen, Harv. L. Rev. Forum 2013, 241 ff., 251, mit dem Fazit, wonach diese distributive Effekte haben; lesenswert im Zusammenhang mit einer Auseinandersetzung mit Gerechtigkeit zu den verschiedenen Konzepten der Gleichheit Dworkin, Gleichheit, 7 ff.
2476 Walzer, 35 ff., 440 ff.
2477 Grundlegend Walzer, *passim*.
2478 Nissenbaum, 166 ff.
2479 Vgl. dritter Teil, VII. Kapitel, B.2.; Vesting, in: Ladeur (Hrsg.), 155 ff., 164; Schwartz, Harv. L. Rev. 2004, 2055 ff., 2069.

kauft» werden: durch Rabatte, «Gratis-Dienstleistungen» usf. Eine Rechtsfigur, die einem Kauf resp. Verkauf von Personendaten entspricht und mit der die Einwilligung des Rechtssubjektes sowie eine Gegenleistung für die Übertragung resp. Nutzungsberechtigung seiner Personendaten entscheidend ist, ist vor dem Hintergrund eines Systemparadigmas als datenschutzrechtliche Pauschallösung nicht überzeugend. Ein «Kauf» von Personendaten mag isoliert im Konsumsektor unter Umständen angemessen sein. Ein «Herrschaftsrecht» des Datensubjektes, das pauschal und ungeachtet der Verarbeitungszusammenhänge sowie der einbettenden gesellschaftlichen Kontexte erfolgt, riskiert die Korruption bereichsspezifischer Rationalitäten, Ziele und Zwecke durch den Markt, durch ökonomische Rationalitäten. Die *datenschutzrechtliche Aufgabe, die Integrität der Kontexte mit ihren eigenen Handlungslogiken, Werten, Zwecken und Zielen zu schützen, würde unterminiert.*

1991 Dem Datenschutzrecht sollen die anhand der umrissenen Elemente beschriebenen Kontexte als Orientierungspunkt dienen. Die Flüsse von Personendaten sind unter Berücksichtigung ihrer Ankoppelung an Gesellschaftsbereiche und an regelmässige multiple Gesellschaftsbereiche zu gestalten.[2480] Die jeweiligen gesellschaftlichen Bereiche bilden quasi die Landschaften, durch welche Datenflüsse verlaufen. Die Grenzgebiete oder Knotenpunkte sind spezifisch relevant und neuralgisch für die datenschutzrechtliche Perspektive.

1992 Kontextuelle Überschneidungen oder Begegnungen bedeuten nicht zwingend Kollision und Konflikt. Als konflikthaft werden (informationelle) Praktiken wahrgenommen, wenn in diesen Schnittstellen unvereinbare Erwartungen der involvierten Kontexte aufeinandertreffen. Logiken des einen sozialen Bereichs stören oder korrumpieren diejenigen eines anderen. Damit werden die Funktionstüchtigkeit und Integrität der Kontexte an sich, namentlich die Gewährleistung ihrer *Werte, Funktionslogiken, Ziele und Zwecke* aufs Spiel gesetzt.[2481]

1993 *Kollisionen* können ebenso aus Informations- und Personendatenerhebungspraktiken resultieren. Beschrieben wurde dies anhand mehrerer Konstellationen. Dabei wurde eine Linse, die sich auf die subjektiv-individuelle Dimension beschränkt, aufgegeben. Sichtbar wurde die systemische Komponente der Konflikte.

1994 Zur Beschreibung von systemischen Konfliktdimensionen die Worte von Hensel/Teubner zu manipulativen Publikationspraktiken von klinischen Studien durch Pharma-Unternehmen:

2480 Hierzu auch der Fall oben; Nissenbaum, 135.
2481 Vgl. Dies., 136.

> «Zentrum des Konflikts ist die Kollision von unverträglichen Handlungslogiken: Ökonomisch rationales Handeln korrumpiert strukturell die Eigenlogiken von Wissenschaft und Gesundheitswesen.»[2482]

1995 Oder wie es Teubner in einer Studie zur Funktion der Institution der «Expertise» umrissen hat:

> «„Expertise" als soziale Institution stellt die Verbindung – systemtheoretisch: die strukturelle Kopplung – zwischen institutionalisierter Wissenschaft und anderen gesellschaftlichen Praktiken her. […] Offensichtlich dient Expertise anderen Zwecken als der Kumulation von methodisch geprüftem Wissen als solchem. Aber sie transferiert die Eigenlogik wissenschaftlicher Forschung in soziale Felder, die einer ganz anderen Rationalität unterworfen sind. Andererseits kann Expertise nicht einfach gleichgesetzt werden mit jeder Art von Informationsproduktion durch Professionelle. Vielmehr greifen gesellschaftliche Akteure erst dann auf „unabhängige Expertise" als Institution zurück, wenn sie die Grenzen des Routinehandelns, die Grenzen von Verhandlungen, wirtschaftlichen Kalkulationen, politischen Machtprozessen, rechtlicher Konfliktregelung, Familienbeziehungen oder Freundschaft als Problemlösungsmechanismen – mehr oder weniger leidvoll – erfahren haben. Sie lösen das konkrete Problem aus seinem alltäglichen Kontext und subsumieren es unter die besondere Rationalität der Expertise, die, gerade weil sie sich deutlich von den Alltagspraktiken der Gesellschaft unterscheidet, eine Problemlösung verspricht. Die fast zwangsläufige Folge sind akute Rationalitätenkonflikte. Wissenschaftliche Expertise ist, wenn sie für außerwissenschaftliche Projekte herangezogen wird, massiven Orientierungskonflikten ausgesetzt. Expertise selbst ist eine höchst fragile soziale Institution, deren Funktionieren davon abhängt, dass sie gegen Interferenzen rivalisierender Rationalitäten strikt abgeschirmt wird. Während die Wissenschaft selbst als soziale Institution wenigstens den Schutz des Elfenbeinturms genießt, also eine gewisse institutionelle Abschirmung in Universitäten und akademischen Publikationen gegen die gröbsten interessengebundenen Interventionen des sozialen Lebens, ist die Expertise systematisch massiven Versuchungen von Einfluss, Überredung, Machtbeziehungen, Familienbanden, Profitmotiven ausgesetzt. Jetzt erst stoßen wir auf das oben gesuchte vertrauensexterne Kriterium, das für die Expertise die juristische Absicherung des sozialen Vertrauens rechtfertigt. Das der Expertise immanente Risiko der Verfälschung durch Interferenz fremder Rationalitäten ist der eigentliche Grund dafür, dass der oben angesprochene soziale Mechanismus des Vertrauens in die Expertise selbst keinen ausreichenden Schutz bietet, sondern der Abstützung durch Rechtsnormen bedarf. Eine Vielzahl öffentlich-rechtlicher Vorschriften haben genau dies zum Ziel: die Integrität der Expertise zu schützen.»[2483]

1996 Teubner leistet bedeutsame Beiträge zur Systemtheorie des Rechts. Der Rechtswissenschaftler entwickelt sein Konzept, wonach es darum geht, Kollisionen und Interferenzen zwischen verschiedenen Sozialsystemen in den Blick zu bekommen und einer Lösung zuzuführen, nie abstrakt. Regelmässig dient ihm ein konkreter (Vor-)Fall als Ausgangspunkt.[2484] Damit wird eine neuralgische Fokussierung auf den Einzelfallkonflikt symbolisiert. Die Unterbeleuchtung der strukturellen

2482 Hensel/Teubner, KritJ 2014, 150 ff., 156.
2483 Teubner, in: Brüggemeier (Hrsg.), 303 ff., 318 ff.
2484 Im Zusammenhang mit seiner Auseinandersetzung mit Grundrechtstheorien und -konzepten: Ders., Der Staat, 2006, 161 ff.

Dimension veranschaulicht Teubner anhand diverser Konstruktionen der «modernen (Zivil-)Rechtsdogmatik». Aus Betrachtungen der individuellen Konflikte, wie sie von juristischer Seite her regelmässig erfolgen, können zwar Lösungen für den Einzelkonflikt formuliert werden. Das grössere, dahinterstehende gesellschaftliche Problem allerdings bleibt bestehen. Teubners Vorschlag ist folglich, einen Konflikt zwischen Privaten in einen institutionellen Konflikt zwischen verschiedenen Rationalitäten umzudeuten. Damit wird die gesamtgesellschaftliche resp. polykontextuelle Problematik freigelegt, die hinter individuellen Konflikten steckt.

Kontextuelle Ansätze zielen folglich darauf ab, systematisch die grösseren gesellschaftlichen Probleme freizulegen, die hinter isoliert individualrechtlich wahrgenommenen Konflikten stehen.[2485] 1997

Spezifisch für das Datenschutzrecht wurde gezeigt, dass nicht erst eine konkret durchgeführte Verarbeitungshandlung störende Auswirkungen haben kann. Bereits die abstrakte Möglichkeit, das Risiko, kann sich negativ auf die Integrität von Gesellschaftsbereichen auswirken. 1998

Ausgangspunkt kontextueller Ansätze ist die Tatsache, dass die *Gesellschaft keine einheitliche Sphäre* ist. Vielmehr wird sie von mannigfaltigen Kontexten mit ihren jeweils eigenen Zielen, Logiken, Erwartungen konturiert. Es geht in der Folge ebenso von rechtlicher Seite her darum, die Kollisionen und Interferenzen betroffener Sozialsysteme zu adressieren und Lösungen zuzuführen. Letztere werden auch als Kompatibilisierungsinstrumente bezeichnet.[2486] Sie dienen dazu, den Schutz der Integrität der jeweiligen Bereiche zu gewährleisten. 1999

Informations- und Personendatenflüsse sowie das Datenschutzrecht, das diese Datenflüsse gestaltet, spielen unter diesen Gesichtspunkten eine bedeutsame Rolle. Insofern nochmals Simitis: 2000

> «In dem Masse freilich, in dem die Erarbeitung personenbezogener Daten zum Unterfall des allgemeinen Persönlichkeitsrechts erklärt wird, verengt sich auch die Regelungsperspektive. Die Auseinandersetzung mit der Verarbeitung und ihren Folgen gerät zum rein individuellen Problem, für dessen Lösung, so scheint es, lediglich die Grundsätze in Betracht kommen, die ansonsten ebenfalls bei der rechtlichen Bewertung von Eingriffen in individuelle Rechtspositionen zu beachten sind.»[2487]

Simitis war es, der früh betonte, dass es nicht das Persönlichkeitsrecht ist, das die Struktur des Datenschutzes bestimmt, stattdessen die *Gesellschaft*.[2488] Die 2001

2485 Vgl. insofern auch Teubner, KritV 2000, 388 ff., der einen konkreten Fall zum Ausgangspunkt nimmt, um den strukturellen Konflikt zu thematisieren.
2486 Zum Begriff auch Karavas, Körperverfassungsrecht, 195 ff.
2487 Simitis, Einleitung: Geschichte – Ziele – Prinzipien, NomosKomm-BDSG, N 26.
2488 Vgl. Simitis im Interview, <https://www.datenschutzzentrum.de/artikel/940-Interview-mit-Prof.-Dr.-Dr.h.c.-Spiros-Simitis.html> (zuletzt besucht am 30. April 2021).

datenschutzrechtliche Systemschutz-Komponente bringt er sodann akzessorisch zu einem spezifischen Bereich zum Ausdruck: Datenschutzrecht sei Demokratieschutz.[2489]

2002 Damit ist es abrundend angezeigt, spezifisch auf den Begriff der Gesellschaft einzugehen. Regelmässig wird mit dem Terminus *«Gesellschaft»* der private Bereich assoziiert; der Staat dagegen wird mit dem öffentlichen Bereich gleichgesetzt.[2490] In dieser Schrift wird die Gesellschaft weder als Gegensatz zum Staat verstanden noch als monistische oder dualistische Entität. Vielmehr ist die heutige Gesellschaft eine pluralistische, facettenreiche Gesellschaft.

2003 Dies reflektierend ist auch der Mensch kein einheitliches Subjekt. Er handelt nicht als monolithisch gedachte Person und Persönlichkeit. Ebenso wenig ist er ein Einheitsdatensubjekt. Vielmehr agiert er in diversen Kontexten und Rollen: als Patient, als Konsumentin, als Vater oder Mutter, als Partnerin, als Freund, als Vereinsmitglied oder als Parteizugehörige, als IV-Bezügerin, als Arbeitnehmer usf. Sein Status als Datensubjekt hat in Entsprechung zu diesen Rollen diverse Ingredienzen. Damit erschöpft sich «das Private» nicht in einem einheitlich fixen, monistischen Schutzbereich. Vielmehr variiert der Privatheitsschutz akzessorisch zu seiner Anknüpfung an die jeweils einschlägigen Gesellschaftsbereiche.

2004 Der Schutz des Privaten oder der Datenschutz können sich folglich nicht auf den Schutz *des* Menschen, *einer* Autonomie beschränken. Das Datenschutzrecht hat die Person *im Lichte der dahinterstehenden Gesellschaftssysteme zu schützen.* Damit und zugleich nimmt das Datenschutzrecht eine Garantenstellung auch für den systemischen Schutz ein. Bei der Gestaltung des Datenschutzrechts ist folglich stets danach zu fragen, welche Auswirkungen gewisse Gestaltungsmöglichkeiten von Personendatenflüssen auf die jeweilige Integrität der Kontexte zeitigen. Im Ergebnis inkludiert das Recht auf informationellen Systemschutz, das kontext-relational ist, den informationellen Subjektschutz, der seinerseits kontext-relational ist.

2005 Für das Datenschutzrecht der Zukunft geht es darum, die Pluralismen der Gesellschaftsstruktur sowie der datenschutzrechtlichen Gestaltungsmöglichkeiten anzuerkennen. Ziel ist es, das *komplexe Gefüge an Bedingungen gegenüber Datenflüssen*, *welche facettenreiche soziale Sphären tangieren, in eine Balance zu bringen*.[2491] Mit anderen Worten wird der Pluralismus nutzbar gemacht, um

2489 Vgl. auch Spiecker genannt Döhmann, in: Epiney/Sangsue (Hrsg.), 1 ff., 3 ff.; Karg, digma 2011, 146 ff., 150; Epiney, in: Epiney/Theuerkauf, 1 ff., insb. 7 ff. weist darauf hin, dass Datenschutz ein Teil des Persönlichkeits- und Privatheitsschutzes sei, damit aber teilweise seine Bedeutung für die Demokratie resp. das öffentliche Interesse übersehen wird.

2490 Zum Dualismus vgl. zweiter Teil, IV. Kapitel und zum Privaten im Privaten erster Teil, III. Kapitel, B.

2491 Nissenbaum, 128.

die netzwerkartigen Personendatenflüsse vor ihren Hintergrundlandschaften zu erfassen und angemessenen Regeln zuzuführen.

Folglich kann unter Anwendung der Methode des Exklusionsverfahrens zunächst gesagt werden, was das *Recht auf informationellen Systemschutz nicht ist:* Es handelt sich um *kein neues subjektives Recht* mit fix definiertem, «einheitlichem» Gehalt. Im datenschutzrechtlichen *Systemparadigma* kommen dem Kontextbezug datenschutzrechtlicher Regulierungen und der systemischen Schutzdimension des Datenschutzrechts pointierte Bedeutung zu. Das Datenschutzrecht ist stets *akzessorisch* zu reflektieren. Schutzzweck des Datenschutzrechts *de lege ferenda* und damit *ratio legis* sind wie folgt zu erfassen: Die Vorgaben an Verarbeitungsprozesse sowie die Gestaltung von Personendatenflüssen sollen so definiert werden, dass diese die Integrität der jeweils involvierten Gesellschaftskontexte bestmöglich gewährleisten. Die *Integrität gesellschaftlicher Systeme, Institutionen resp. Kontexte* zu schützen, ist Kernaufgabe des Datenschutzrechts der Zukunft. Hierbei inkludiert das Recht auf informationellen Systemschutz regelmässig den informationellen Subjektschutz. 2006

Für die Normierung der Flüsse von personenbezogenen Angaben innerhalb und zwischen verschiedenen Kontexten sind damit stets die im Hintergrund stehenden Kontexte mit ihren Zielen und Zwecken vor Augen zu führen. In der Folge wird eruiert, welche Auswirkungen die verschiedenen Gestaltungsmöglichkeiten von Informationsflüssen auf die *kontextuelle Integrität* zeitigen.[2492] 2007

Nissenbaum präsentiert ein *konkretes Prüfungsschema*. In seinem Zentrum steht die sog. *kontextrelative Informationsnorm*. Sie ist nicht im streng juristischen Sinne als positivierte (datenschutzrechtliche) Vorgabe zu verstehen. Vielmehr beschreibt der Begriff den Fluss von Daten von *einem Akteur* in seiner *Rolle* gemäss dem *Kontext* zu einem anderen Akteur in dessen Rolle entsprechend bestimmter *Transmissionsprinzipien*.[2493] Verarbeitungstechnologien und -praktiken lassen sich gemäss der folgenden Anleitung *evaluieren*: In einem *ersten Schritt* sind der dominante Kontext resp. die überlappenden resp. konfligierenden Kontexte zu bestimmen.[2494] In einem *zweiten Schritt* werden die Schlüsselakteure als Informationssender, -empfänger und -subjekte sowie anhand ihrer qua Hintergrundkontext definierten Rollen charakterisiert. Neue Technologien und Praktiken inkludieren oft neue Datenempfänger. So beispielsweise die analoge gegenüber der neueren elektronischen Autobahnmaut: Nutzer mit einem Badge kön- 2008

2492 Ein Konzept der legal integrity wurde insb. von Dworkin entworfen, wobei von der Integrität des Rechtssystems dann gesprochen wird, wenn seine Normen aus einem kohärenten Schema von Prinzipien abgeleitet sind und der Erlass in den demokratisch vorgesehenen Strukturen erfolgt, vgl. auch Dworkin, Gerechtigkeit, 553 ff.; Nissenbaum, 178 ff., und 129.

2493 Nissenbaum, 141.

2494 Dies., 149 ff.

nen eine bestimmte Spur nutzen, wobei die Registrierung der Fahrstrecke resp. Mautgebühr elektronisch erfolgt. Beim «analogen» Mautkassierer, der das gezogene Einfahrtsticket einliest und die geschuldete Gebühr ermittelt, ist der Datentransfer insb. bei einer Barzahlung sehr beschränkt. Dagegen empfangen im elektronischen Mautsystem weitere Akteure, namentlich die Systemanbieter, unter Umständen aber auch die Strassenverkehrsämter sowie Kreditkarteninstitute, generierte Informationen. In einem *dritten Schritt* ist eine Informationstypologie vorzunehmen. Insofern wird gefragt, welche Attribute resp. Informationsinhalte von einer Datenverarbeitung betroffen sind. Geprüft wird, ob eine neue Technik die Art von Information, die übermittelt werden soll, verändert. Elektronische Ein- und Austrittskarten messen nicht mehr nur, *dass* eine Person eingetreten ist und *dass* sie den Ort wieder verlassen hat. Sie registrieren ebenso, *wie lange* eine Person sich in einem bestimmten Bereich aufgehalten hat. In einem *vierten Schritt* sind Veränderungen bei den Transmissionsprinzipien gerade auch bezüglich der Positionierung resp. des Vordringens neuer Technologien zu eruieren. Kann im Strassenverkehr eine Person wählen zwischen «analoger Mauterhebung» (Ticket ziehen, Ticket einer Person bei einer Station vorweisen, (Bar-)Zahlung) und elektronischem System, verändern sich Transmissionsprinzipien dann, wenn das elektronische Mautsystem *zum einzig möglichen System* wird. Wird der Prozess zudem an ein Kreditkartensystem gekoppelt, verändert sich die Situation weiter.

2009 Das präsentierte *Vier-Stufen-Raster* gibt eine Anleitung, wie eine (Re-)Evaluierung sozio-technischer Systeme und Praktiken im Licht der kontextuellen Integrität erfolgen kann.[2495] *Verändert* eine neue Datenverarbeitungstechnologie und -praxis Akteure, Attribute oder Transmissionsprinzipien, kann dies als *Indikator* für eine Verletzung etablierter und systemisch eingebetteter Informationsnormen gesehen werden. Hier könnte auf eine «Vorqualifizierung» im Sinne einer Verletzung der kontextuellen Integrität geschlossen werden.[2496]

2010 Zu ergänzen bleibt, dass sich der kontextuelle Ordnungsrahmen auf Systeme innerhalb von Institutionen resp. Organisationen und Unternehmen übertragen lässt. Ansätze lassen sich z. B. in der sog. *attribute-based access control* (ABAC) innerhalb von Unternehmen verorten. Mit ihr wird informationelle Zugangsberechtigung organisatorisch anhand von Zuständigkeiten und Aufgabenbereichen fixiert.[2497] Dies geschieht über Funktions- und Rollenbeschreibungen. Informationszugänge werden eingeräumt, sofern sie zur Erfüllung der jeweiligen Aufgabe durch die jeweilige Aufgabenträgerin erforderlich sind. Die Umsetzung von Zugangsberechtigungen resp. -schranken erfolgt über technische Instrumente.

2495 Nissenbaum, 189 ff.
2496 Als rote Flagge beschrieben von Dies., 127 ff., 141 ff.; Dies., in: Heinrich-Böll-Stiftung (Hrsg.), 53 ff., 61 f.
2497 Hierzu Cavoukian/Chibba/Williams/Ferguso, Jusletter IT vom 21. Mai 2015, N 15 ff.

Im Ergebnis macht die Theorie der kontextuellen Integrität die komplexen Varianten in den Reaktionen der Menschen auf Flüsse von personenbezogenen Angaben erklärbar und plausibel sowie *vice versa*.[2498] Keineswegs alle der neuen Personendatenverarbeitungsprozesse und -technologien lösen Widerstand, Empörung, Irritation oder Angst aus. Wie erwähnt interpretiert die Autorin die jeweiligen Reaktionen als Indiz für die Einhaltung resp. Verletzung kontextrelativer Erwartungen.[2499] In Bezug auf soziale Plattformen im *Internet* die Worte von Nissenbaum, die zum nächsten Titel überleiten: 2011

> «If only researchers and commentators would acknowledge and pay attention to the complex norms that govern the flow of information in the social, professional, ethnic, age-cohort contexts in which social network sites are embedded, they would discover that participants are anything but illogical […]. Users, believing that the flow of information about them and others posted to their sites (in their profiles) is governed by certain context-relative norms, are rightly surprised and indignant, when, for whatever reasons, other actors have diverted these flows in unexpected ways that breach informational norms. These diversions challenge understandings of nature of the context as well as the nature of the relationship that online social networks embody and foster.»[2500]

2. Einschlägigkeit für den Online-Bereich

Ein Grossteil der Herausforderungen des Daten- und Privatheitsschutzes wird heute für das *Internet* diskutiert.[2501] Die *Online-Privacy wird* als *eigene Domäne* beschrieben, für die folglich eigene Regelkonzepte und -ansätze zu suchen seien. Insofern lässt sich erneut eine Strategie ermitteln, die Welt zweizuteilen: online versus offline, virtuelle Welt versus analoge Welt, Cyberspace versus reale Welt.[2502] Die komplexe Struktur des Internets wird so nicht selten mit derselben Methode reduziert, wie sie für «das Private» gewählt wurde. Das Netzwerk wird ähnlich rhetorisch kaschierend mit dem bestimmten Artikel – «das» Internet – beschrieben. Das Internet wird damit als *eigener Kontext*, als eigenständiges Milieu wahrgenommen.[2503] Allerdings greift die Zweiteilung und Gegenüberstellung 2012

2498 Nissenbaum, 163.
2499 Dies., in: Heinrich-Böll-Stiftung (Hrsg.), 53 ff., 61 f.
2500 Dies., 227; die Infiltration des Kontextes der Freundschaft auf sozialen Plattformen beschreibt eindrücklich Rössler, Eurozine vom 27. Februar 2015.
2501 Hierzu exemplarisch Schwartz, Wis. L. Rev. 2000, 743 ff., unter Hinweis auf das richtungsweisende Werk von Lessig; vgl. zum Reformeifer in Deutschland insofern Bull, NVwZ 2011, 257 ff., 257.
2502 Vgl. illustrativ Cachelin, *passim*; zur Debatte, die auch Meinungen beinhaltet, wonach im Cyberspace die Gesetze der realen Welt keine Geltung hätten, vgl. Meyer-Schönberger, in: Schweizer/Burkert/Gasser (Hrsg.), 853 ff.; zum Internet als sozialem Raum, dessen Perzeption zwischen dem Spiegelbild der realen Welt und einer Utopie schwankt, Eifert, NVwZ 2008, 521 ff., 521; vgl. auch Weber/Heinrich, ZSR 2013, 477 ff., 493 ff., welche der traditionellen Welt die Online-Welt gegenüberstellen, letztere aber nicht als rechtsfreien Raum verstanden wissen wollen.
2503 Vgl. Nissenbaum, Dædalus 2011, 32 ff.; zugleich wird er regelmässig als sog. öffentlicher Raum konzipiert, vgl. Bull, NVwZ 2011, 257 ff., 262; hierzu mit Blick auf die Ausführungen des Bundesverfassungsgerichts in seinem sog. Urteil zum Computer-Grundrecht Böckenförde, JZ 2008,

des Internets quasi als eigenständiger Kontext gegenüber einer analogen Welt zu kurz. So wenig «öffentlich» als Synonym für «informationsrechtlich ungeschützt und zugriffsoffen» stehen kann,[2504] so wenig soll «online» als Synonym für «zugriffsoffen» verstanden werden. Aus technischer und sozio-technologischer Sicht zeigt sich die Ausgangslage erneut facettenreich.[2505]

2013 «Das» Internet wird deshalb oft als «eigener und eigenständiger Kontext» wahrgenommen, weil sich unzählige Verarbeitungsformen und Praktiken nachweisen lassen, welche die Kernelemente des Konzeptes der kontextuellen Integrität *verändern*. Neue Akteure treten hinzu, Rollen verändern sich oder Transmissionsprinzipien werden durchbrochen.[2506]

2014 Richtig ist, dass der Einsatz bestimmter, auch neuer Technologien die Ausgangslage für Datenschutzfragen wesentlich verändern kann (aber nicht muss, vgl. die US-amerikanischen Fälle oben). Illustrativ der Dienst von Google Street View: Die Kenntnisnahme eines Hauses mit bestimmten sich davor aufhaltenden Personen in der analogen Welt einzig kraft menschlicher Wahrnehmung ist informationell eine andere Praxis, als wenn Häuser mit davor stehenden Personen fotografiert oder gefilmt werden und die Aufnahmen in der Folge online gestellt werden. Über Google Street View sind diese Personendaten und Informationen jederzeit aus dem «stillen Kämmerchen» von fast jeder Person abrufbar. Besagte Informationen zu bestimmten Personen können mit weiteren Informationen über Online-Dienste angereichert werden.[2507]

2015 Das Internet als eigenständigen Kontext und als quasi öffentlichen Bereich zu verstehen, überzeugt nicht. Das Datenschutzthema kann insofern nur dann sinnvoll erfasst werden, wenn die sich *ebenso im Internet abbildenden gesellschaftlichen Kontexte in die Erwägungen integriert* werden. Das Internet ist «Stätte» für kommerzielle Transaktionen, Bildung, Pflege von Beziehungen, persönlichen und familiären, aber auch beruflichen. Ähnlich wie in «der» analogen Welt finden sich bezüglich Online-Aktivitäten Erwartungen hinsichtlich der Angemessenheit von Flüssen personenbezogener Angaben.[2508] Denn die in der analogen Welt strukturierten Sozialsysteme mit ihren kontextrelativen Informations- und Privatheitserwartungen verleihen ebenso der Online-Welt ihren Fingerabdruck.

---

925 ff., 935 f., wobei mit der Deklaration des Netzes als Öffentlichkeitssphäre nicht gleichzusetzen sei, dass es sich um einen rechtsfreien Raum handle.

2504 Nissenbaum, 217.

2505 Dies., Dædalus 2011, 32 ff., 37 ff.

2506 Dies., 195 ff.; illustrativ auch der Beitrag von Dreier (Hrsg.), in: Hilty/Drexl/Nordemann (Hrsg.), 67 ff., in Bezug auf Informationen zu Straftätern, Online-Archiven und Löschungskonzepten.

2507 Nissenbaum, 219 ff.; zu Google Street View auch Wermelinger, digma 2012, 134 ff.; dazu, dass im Zuge des Street-View-Projektes zusätzlich weit angelegt ein WLAN-Scanning durchgeführt wurde, Dies., HRRS 2011, 72 ff.

2508 Dies., 217.

Damit ist erklärt, weshalb der Transfer von Informationen via Facebook – eine Online-Plattform zur Pflege persönlicher und familiärer Beziehungen – an ein Unternehmen mit wirtschaftlichen Intentionen inklusive der anschliessenden Beeinflussung im politischen Kontext als Skandal taxiert wurde und Empören auslöste. Bei Facebook agieren Nutzerinnen und Nutzer primär in ihren Rollen als Freunde und Familienmitglieder, um persönliche Beziehungen zu pflegen (wohingegen LinkedIn als soziale Plattform primär der Pflege beruflicher Relationen dient). Die in diesem Kontext geteilten persönlichen Angaben wurden zu einem anderen Zweck ausgewertet. Man beeinflusste Nutzerinnen und Nutzer gezielt in ihrer politischen Willensbildung, wobei insb. Personen eruiert wurden, die hinsichtlich ihrer Wahlentscheidung als wankelmütig einzustufen sind, um diese gezielt mit «Propaganda» zu adressieren. Dies geschah über einen «Dritten»: Cambridge Analytica. Das Unternehmen agierte wohl getrieben von wirtschaftlichen Interessen. Dieser Vorfall macht nicht nur die Manipulation der Willensbildung des einzelnen Individuums als Problem sichtbar. Vielmehr führt er die Beschädigung des politischen Kontextes und des demokratischen Systems sowie des Bereiches privater Lebensführung vor Augen. 2016

Die pluralen sozialen Kontexte sind gleichermassen für den Datenschutz in der sog. «Online-Welt» einschlägig. Datenschutzrechtliche Erwägungen – auch *de lege ferenda* – haben in Bezug auf digitale Technologien und Netze im Rahmen der (geplanten) Datenverarbeitungspraktiken die betroffenen sozialen Kontexte, für welche die Technologie(n) nutzbar gemacht werden, einzubeziehen. Insofern sind die jeweiligen Funktionen und Funktionsweisen der Kontexte zu (be)achten: Facebook als soziale Plattform soll der Pflege von persönlichen Beziehungen dienen und nicht zur politischen Beeinflussung oder gar Manipulation missbraucht resp. zweckentfremdet werden, getragen von wirtschaftlichem Profitdenken.[2509] LinkedIn ist als berufliches Netzwerk im Arbeitskontext angesiedelt, womit die Verarbeitung von Personendaten durch Recruiter systemkompatibel ist (ob im Übrigen die Anforderungen des geltenden Datenschutzrechts eingehalten werden, ist damit nicht gesagt). Entsprechend finden sich mit Blick auf Recherchen zu Kandidatinnen und Kandidaten im Internet über Berufsnetzwerke wie LinkedIn in der Regel Informationen hierzu in den privacy policies.[2510] 2017

Viele der Online-Dienste anbietenden Konzerne haben indes einseitige policy settings. Geschäftsinhaber monitoren oft die Personenangaben, sammeln diese und verkaufen sie an Dritte weiter, was regelmässig etablierte Informationserwar- 2018

2509 Die Worte von Warren/Brandeis kommen hier in Erinnerung, welche die Profitgier der Yellow Press anprangerten, die mit dem Eindringen in das Privatleben bekannter Menschen und der Veröffentlichung entsprechender Informationen die primitive Neugier der Allgemeinheit befriedigten.

2510 Zum Beispiel für LinkedIn in 2.1., unter: <https://www.linkedin.com/legal/privacy-policy> (zuletzt besucht am 30. April 2021).

tungen verletzt.[2511] Das Abschöpfen von Personendaten durch Arbeitgeber oder Recruiter aus Netzwerken, mit denen persönliche, also freundschaftliche und familiäre Beziehungen gepflegt werden, vermag im Lichte eines Rechts auf informationellen Systemschutz nicht zu überzeugen. Als störend und unangemessen erlebt werden Kontaktanfragen mit amourösen Intentionen. Soziale Netzwerke im Internet bilden somit keine neuen Kontexte. Vielmehr sind sie als neue Kommunikations- und Aktionsmedien zu verstehen, die dem Informationsaustausch und der Beziehungspflege in spezifischen sozialen Kontexten mit den diese prägenden Erwartungen dienen:

> «The practice of harvesting information from social networking sites by third-party aggregators as well as by social networking sites operators, job recruiters, and employers is morally troubling because it threatens to disrupt the delicate web of relationships that constitutes the context of social life, injecting into workplace and business context information of the wrong type, under inappropriate transmission principles.»[2512]

2019 Facebook hat in Reaktion auf die Kritik an seinen Praktiken und Techniken (und vor dem jüngsten Skandal) eine breiter angelegte und granularere Kontrolle der Nutzer betreffend den Zugriff auf ihre Profile implementiert.[2513] Neue Plattformen werden entwickelt. Ein Beispiel hierfür ist «Moji», das für verschiedene Kontexte nutzbar gemacht werden kann, wobei unterschiedliche Felder mit variablen Rollen genutzt werden können.[2514]

2020 Nach diesen Ausführungen drängt sich eine *differenzierte Schlussfolgerung* auf: Die Beschreibung des Internets als eigenständiger Kontext ist zugleich richtig wie falsch. Im Internet werden die in der «realen Welt» prägenden sozialen Kontexte gleichermassen wirksam; das Internet ist Marktplatz, Raum politischer Aktivitäten, familiärer und freundschaftlicher Beziehungsbereich, beruflicher Austauschraum, Bibliothek und vieles mehr. Im Internet spiegeln sich soziale Kontexte der Offline-Welt. Ihr Schutz sollte ebenso für die Datenschutzregulierung im Internet leitend sein. Auch hier erlangen Datenflüsse und deren Normierung ihren Bedeutungsgehalt anhand der sich jeweils im Hintergrund aufspannenden Gesellschaftskontexte, in welche die Personendatenflüsse eingebettet sind.

2021 Noch heute finden Datenflüsse im Internet weitgehend unkontrolliert statt resp. werden durch einseitige und isoliert subjektrechtliche Dispositionsformalismen legitimiert.[2515] Im Internet finden sich unzählige Praktiken, die etablierte, kontextgebundene Erwartungen an Datenflüsse verändern: mehr und andere Akteu-

2511 Nissenbaum, 221 ff.
2512 Dies., 228.
2513 Damit werden gewisse, aber nicht alle Privacy-Bedenken adressiert. Kontrolle resp. Selbstbestimmung ist nur ein Transmissionsprinzip neben anderen.
2514 Nissenbaum, 228 f.
2515 Zu den Herausforderungen der datenschutzrechtlichen Einwilligung zweiter Teil, VI. Kapitel, 4.4.–4. 6. sowie dritter Teil, VIII. Kapitel, B.1.1.–5.

re, zeitlich und örtlich unbeschränkte Datenverarbeitungen, veränderte Transmissionsprinzipien. Praktiken wie Google Street View und öffentliche Register online begründen *prima facie* eine Verletzung der kontextuellen Integrität.[2516] Für die rechtliche Gestaltung von Datenflüssen im Internet sollte die leitende Frage sein, ob diese Veränderungen begründbar sind mit systemischen Schutzdimensionen, namentlich den Zielen und Zwecken der jeweils adressierten Kontexte.

2022 Die Harmonisierung der Kontexte via Datenflüsse innerhalb und zwischen den Kontexten im Internet wird, nachdem der Gesetzgeber die entsprechenden Strukturierungsentscheidungen vorgenommen hat, wesentlich durch *technische Massnahmen* und namentlich den Designschutz umzusetzen sein.

2023 Mit den Ausführungen zum Datenschutz im Internet ist auf die *Einwände* einzugehen, die sich bezüglich des Konzepts der kontextuellen Integrität aufdrängen.[2517]

3. Einwände

2024 Der *erste Einwand* lautet, dass das Konzept der kontextuellen Integrität *konservativ* sei. Wenn jede neue Praxis an vorbestehenden sozialsystemischen Informationserwartungen gemessen und jede Veränderung als Ruptur beschrieben werde, sei Fortschritt kaum denkbar. Diesem Einwand begegnet Nissenbaum mit der *Fortführung ihres Prüfschemas*. Sie schlägt vor, die Verletzung etablierter Erwartungen, die sich aus kontextuellen Informationsnormen ergeben, «*nur prima facie*» als Verletzung der kontextuellen Integrität zu taxieren. In einem Folgeschritt sei zu prüfen, ob es Argumente dafür gibt, die neue Praxis trumpfen zu lassen.[2518]

2025 Damit zeigt sich zweierlei: Ein Recht auf informationellen Systemschutz kommt nicht um *wertende Entscheidungen* herum. Diese allerdings sollen nicht isoliert einzelfallorientiert, an einer deliktisch gedachten Verletzungshandlung gegenüber einem generalisierten Datensubjekt, basierend auf der Anwendung von Generalklauseln durch die (rechts-)anwendenden Stellen, erfolgen. Vielmehr ist eine Vorstrukturierung durch die Formulierung von konkretisierten, die Sozialsysteme bestmöglich kompatibilisierenden Verarbeitungsvorgaben vorzunehmen. Diese Aufgabe soll vom *Gesetzgeber* wahrgenommen werden.

2026 In einem *systemrelativen Datenschutzrecht* kommt dem *Selbstregulierungsansatz* sowie der *Integration von bereichs- und branchenspezifischen Erwägungen* ein wichtiger Platz zu. Solche Ansätze vermögen in effizienter Weise eine Integration der Rationalitäten sowie Organisationsprinzipien der spezifischen Gesellschafts-

2516 Nissenbaum, 219.
2517 Dies., 158 ff.
2518 Hierzu Dies., 164 f.

bereiche und Institutionen zu bewerkstelligen. Mit anderen Worten leisten damit kontextspezifisch herausgebildete Logiken und Strukturen aus sich heraus («organisch») einen Beitrag zur Konstitution eines systemgerechten Datenschutzrechts.

2027 Der *zweite Einwand* ist die Kehrseite der Medaille, die *Tyrannei der Normalität*.[2519] Unzählige sozio-technologische Praktiken diffundieren in die Gesellschaft. Soll und darf aus der breiten Nutzung einer Technologie zugleich auf die Akzeptanz mit Blick auf die Datenflüsse geschlossen werden? Wer Facebook nutzt, erwartet nicht, dass die geteilten Personendaten einen Schutz unter dem Titel des Privaten erfahren. Es ist, als ob diese Angaben öffentlich wären.

2028 Gleichwohl überzeugt es nicht, aus der breiten Nutzung einer Technologie auf die parallele Akzeptanz der damit einhergehenden (veränderten) Datenflüsse zu schliessen.[2520] Wenn in der Generation Y der grosse Teil der Jugendlichen Facebook nutzt, um Freundschaftsbeziehungen zu pflegen, kann daraus – selbst wenn eine datenschutzrechtliche Einwilligung erteilt wurde[2521] – gerade nicht kausal gefolgert werden, dass mit dieser Nutzung *telle-quelle* die daran gekoppelten Datenverarbeitungen gutgeheissen werden. Vielmehr ist die breite Nutzung bestimmter Technologien Ausdruck davon, dass diese der Befriedigung gesellschaftlicher und persönlicher Bedürfnisse und damit der Nachfrage dienen. Offensichtlich hat die Globalisierung dazu geführt, dass die Digitalisierung und die Kommunikation qua neuer Medien gänzlich neue Dimensionen erlangt haben. Allerdings gibt es infolge der Marktmacht bestimmter weniger Unternehmen – der Internetgiganten – bis heute kaum Ausweichmöglichkeiten. Anstelle einer wirklichen Gutheissung ebenso der Personenverarbeitungsprozesse ist eher von einem nur formellen Abnicken von privacy policies auszugehen. Viele Datenverarbeitungsprozesse resp. der faktisch ungenügende und im Gegenzug oft rein fassadenhafte und formelle Datenschutz, existierend auf dem Papier, lösen breit angelegte Kritik aus. Umgekehrt ist es so, dass bis heute selbst ein grosser Teil der jungen Menschen aus den Generations Y–Z und damit der Digital Natives in statistischen Erhebungen sagt, dass Datenschutz ein wichtiges Anliegen sei.

2029 Der Wunsch, freundschaftliche, familiäre oder berufliche Beziehungen digital und über das Handy, Facebook, Skype und Zoom zu führen, Waren (und seit der COVID-19-Krise auch Dienstleistungen) online anzubieten resp. zu handeln, übertrumpft datenschutzrechtliche Anliegen. Der Wunsch, online ein Buch zu bestellen, online ein Arbeitsmeeting real werden zu lassen, die alten Eltern per Video-Telefonie zu sprechen und zu sehen, online die Zeitung zu lesen – diese

2519 Nissenbaum, 160 ff.
2520 Dies., 5 f.
2521 Vgl. zur Problematik von Einwilligungskonstruktionen als Legitimationsinstrument in Anbetracht der Realitäten zweiter Teil, VI. Kapitel, 4.4., 5., 6. sowie dritter Teil, VIII. Kapitel, B.1.1.–5.

Interessen setzen sich gegenüber dem Interesse an Datenschutz zumindest für die konkrete Situation durch. Das heisst keineswegs – im Gegenteil, wie diese Studie zu zeigen suchte –, dass sich der Datenschutz erübrigt. Dass Nutzerinnen und Nutzer mit Empören reagieren, wenn ihre persönlichen Daten zur politischen Manipulation ausgebeutet werden, belegt die gleichwohl vorhandenen Erwartungen betreffend ihren Privatheitsschutz. Letzterer hat sein Ziel und Mandat an der richtigen Stelle zu suchen und zu finden sowie in der Folge zielgerichtet zu adressieren: systemorientiert. Einzig, weil bestimmte sozio-technologische Praktiken – heute primär im Online-Bereich – weit verbreitet sind, heisst dies nicht zugleich, dass die damit verbundenen Datenverarbeitungsprozesse zu billigen sind und mit den sog. *«reasonable expectations of privacy»* kompatibel sind.[2522] Die Gestaltung von Datenflüssen und die Formulierung der datenschutzrechtlichen Vorgaben an die Personendatenverarbeitungen durch den Gesetzgeber haben sich nicht daran zu orientieren, wie gemein verbreitet gewisse Technologien sind, wie vertraut Menschen mit diesen sind, sondern daran, wie kompatibel diese mit den Logiken der jeweils einbettenden Sozialsysteme resp. Hintergrundkontexte sind.[2523]

Datenschutzerklärungen und Einwilligungskonstruktionen dagegen zielen gerade im digitalen Bereich hieran allzu oft vorbei. Sie stossen in Anbetracht der datenschutzrechtlichen Realitäten an ihre Grenzen. Wer online ein Buch bestellen will, klickt die Einwilligungserklärung kurzerhand und ohne das Studium seitenlanger, unverständlicher Datenschutzerklärungen an, um sein Hauptziel erreichen zu können. Mit solchen mechanischen und formalistischen Akten den Datenschutz und das Datenschutzrecht als erfüllt zu taxieren, ist ein markantes Versäumnis. Ein Versäumnis, das sich nicht nur auf das einzelne Subjekt nachteilig auswirkt. Damit mittel- und längerfristig etablierte und tragende Institutionen unserer Gesellschaft gerade auch in der Online-Welt nicht erodiert werden, ist ein eingebettetes und einbettendes, systemakzessorisch konzipiertes Datenschutzrecht gefordert. 2030

Online-Privacy-Policies mit allfälligen Checkbox-Instrumenten tragen dem in dieser Studie vorgeschlagenen Systemparadigma – das ebenso online seine Gültigkeit beanspruchen muss – kaum Rechnung. Der Vorstellung, wonach der Online-Bereich ein quasi öffentlicher Bereich sei, in welchem Informationen ungefiltert und unbeschränkt abgegriffen, weiterverteilt und verwertet werden können, wird eine klare Absage erteilt. Einer solchen Realität ist entschieden entgegenzuwirken, auch durch eine Rekonstruktion des Datenschutzrechts. 2031

2522 Nissenbaum, 234.
2523 Hierzu auch Dies., 235.

Zusammenfassende Schlussfolgerungen

Mit dem *Recht auf informationellen Systemschutz* wird ein *neues Paradigma* zur Gestaltung des Datenschutzrechts der Zukunft vorgeschlagen. Seine Entwicklung ging aus einer kritischen Hinterfragung einiger Kernannahmen des aktuellen Datenschutzrechts hervor. Das Recht auf informationellen Systemschutz überwindet einen die Komplexität reduzierenden Dualismus sowie den Monismus aktueller Datenschutzgesetzgebung und zielt darauf ab, *angemessene Regelungen für Personendatenflüsse innerhalb und zwischen pluralen gesellschaftlichen Bereichen* zu definieren. 2032

Damit setzt das neu vorgeschlagene Lösungskonzept an *sämtlichen der drei in dieser Arbeit vorgestellten Strukturmerkmalen des DSG* an: 2033

Der *Dualismus* wird zu einem ausdifferenzierten, pluralistischen System weiterentwickelt. Für das DSG wird somit der entgegengesetzte Weg, als ihn die DSGVO vorsieht, vorgeschlagen. Es geht um die Anerkennung von Pluralismus. 2034

Das Datenschutzrecht soll nicht mehr in erster Linie mittels *Generalklauseln* regulieren. Vielmehr sollen Vorgaben an Personendatenverarbeitungen systemadäquat definiert werden. Dies erfolgt mit dem Ziel, Systeme wie Subjekte zu schützen. Gesetzgeberisch wird mit Szenarien zu arbeiten sein, die evaluieren, welche Auswirkungen verschiedene Gestaltungsweisen von Datenflüssen resp. Vorgaben auf die Integrität der jeweils involvierten Gesellschaftsbereiche haben. Angemessen ist eine datenschutzrechtliche Gesetzgebung, wenn hinreichend konkret definierte Verarbeitungsvorgaben vorliegen und damit die Gestaltung der Personendatenflüsse die Integrität der betroffenen sozialen Kontexte bestmöglich respektiert. Erreicht wird dies durch die Anerkennung der pluralen Hintergrundkontexte von Personendatenverarbeitungen und -flüssen sowie durch einen ausdifferenzierten Einsatz diverser Gestaltungsoptionen datenschutzrechtlicher Vorgaben. Alle bislang bekannten Instrumente werden hierbei selektiv eine Rolle spielen. Keines der Instrumente, auch nicht die informierte Einwilligung, wird alleiniger Lösungsansatz sein können. 2035

Der *Subjektschutz*, der im bisherigen Datenschutzrecht als *Persönlichkeitsschutz* figuriert, wird ergänzt, indem als Schutzzweck des Datenschutzrechts der *Systemschutz* anerkannt wird. Es sind weder nur das Datensubjekt und die Personendaten als Quasi-Objekte noch die konkrete, invasive und in räumlichem Denken verhaftete Verletzungshandlung, die kognitiv im Vordergrund stehen. Vielmehr liegt der Fokus auf Personendatenflüssen innerhalb und zwischen Gesellschaftsbereichen. Bereits die potentielle Möglichkeit, das *Risiko* bestimmter Verarbeitungshandlungen kann (datenschutz-)rechtlich problematisch sein. Das Datenschutzrecht ist damit weiter aus einem deliktsrechtlichen Denken heraus- 2036

zulösen und pointiert in die Richtung eines Risikorechts zu entwickeln. Das Systemschutzparadigma verdrängt das Subjektschutzparadigma nicht. Vielmehr inkludiert der Systemschutz den Subjektschutz, der zu einem kontextuellen und damit sachlich ausdifferenzierten Schutz wird.

2037 Ein Recht auf informationellen Systemschutz geht davon aus, dass ein in Zukunft tragfähiges und wirkungsvolles Datenschutzrecht seine Garantenstellung für die *Integrität und Funktionstüchtigkeit von etablierten Institutionen, Systemen oder Kontexten der Gesellschaft* wahrzunehmen hat. Um dieses neu resp. erweitert definierte Schutzziel zu erreichen, ist anzuerkennen, dass es im Datenschutzrecht um die *angemessene Regelung von Datenflüssen* geht. Die Überzeugungskraft der Gestaltung von Personendatenflüssen misst sich an den Auswirkungen der Datenflüsse auf die Robustheit der involvierten Gesellschaftsbereiche. *Datenschutzrecht ist systemrelatives resp. akzessorisches Recht.*

2038 Personendatenverarbeitungen und -praktiken spielen eine zentrale Rolle bei der Frage, ob gesellschaftlich etablierte Institutionen – der Gesundheitsbereich, die Demokratie, der Sozialstaat, das Privatleben – stabil und geschützt bleiben oder ob diese erodiert werden. Ein generalklauselartiges, auf Formalismen (wie privacy policies) zurückgreifendes, am Subjekt- und Handlungsunrecht anknüpfendes Datenschutzrecht ist nicht in der Lage, den Subjektschutz, geschweige denn den Systemschutz zu gewährleisten. Das Datenschutzrecht muss als Garant der tragenden gesellschaftlichen Säulen eine gänzlich neue Bedeutungsdimension erlangen. Es handelt sich beim Datenschutzrecht keineswegs um ein losgelöstes, isoliertes und eigenständiges Rechtsgebiet, das nur wenige Expertinnen und Experten interessiert, sondern um ein Rechtsgebiet, das in essentieller Weise die Funktionstüchtigkeit der für die Einzelnen und deren Wohl bedeutsamen Institutionen gewährleistet.

2039 In dieser Arbeit wird eine *Theorie* entwickelt, die sich am *Facettenreichtum gesellschaftlicher Kontexte* orientiert. Im Zentrum steht die Erkenntnis, dass es im Datenschutzrecht um die Regulierung von Datenflüssen geht, eingebettet in ihre jeweiligen Landschaften.

2040 Der hier präsentierte Vorschlag für ein Datenschutzrecht der Zukunft weist *nicht* in die Richtung der Reduktion von Komplexität, sondern macht sich die unzähligen Möglichkeiten, Datenflüsse zu gestalten, zunutze und plädiert vor dem Hintergrund pluraler Verarbeitungskontexte für ausdifferenzierte Lösungen.

2041 Das in dieser Schrift freigelegte *Systemschutzparadigma* ist *kein Deus ex machina*. Vielmehr zeigte die Untersuchung, dass systemische Schutzerwägungen schon immer, wenn auch eher subkutan, angelegt waren. Erhärtet wurde die Theorie mit einer Vielzahl von Beispielen, vom Facebook-Skandal über die Volkszählung und von der Yellow Press über das Adoptionsrecht bis hin zur geheimen privat-

detektivischen Versicherungsobservation. Für die Entwicklung der Thesen und die Ausarbeitung des neuen Paradigmas waren verschiedene, etappenweise gewonnene Erkenntnisse erforderlich. Sie werden nachfolgend in Bezug auf ihre Systemrelevanz kompiliert:

Der **erste Teil** dieser Schrift stand unter dem Titel «Vergangene Zukunft». Ein Blick auf historische und literarische Quellen mochte zunächst als anachronistisch und paradox für eine juristische Studie zu einem Rechtsgebiet erscheinen, das von modernen Informationsverarbeitungstechnologien, der Digitalisierung und dem Vertrauen in Erkenntnisse künstlicher Intelligenz herausgefordert wird. Doch diese rückwärts und seitlich gerichtete Betrachtung ermöglichte richtungsweisende Erkenntnisse für die rechtswissenschaftliche Untersuchung und das Datenschutzrecht der Zukunft. Die Analyse von *historischen, geschichtswissenschaftlichen sowie literarischen Quellen* generierte die *These*, wonach es im Datenschutzrecht um die Gestaltung von Personendatenflüssen geht und wonach die Verarbeitung von Informationen und spezifisch von Personendaten nachhaltigen Einfluss auf die Etablierung, den Schutz oder eben die Erosion von Institutionen hat. 2042

Das *erste Kapitel* mit dem Titel «Der geheime Schlüssel» wies den traditionsreichen und sagenumwobenen Geheimworten und Geheimhaltungspflichten die Schlüsselrolle zu, um neue Erkenntnisräume für das Datenschutzrecht zu eröffnen. Anhand zweier Märchen wurde sichtbar gemacht, wie durch Geheimworte und deren Ermittlung diverse soziale Güter erlangt oder verteidigt werden konnten (im Fall von Ali Baba Geld, im Fall von Rumpelstilzchen ein Kind). Solche Geschichten über Geheimworte resp. ihren Bruch rückten das Bild des Informationsflusses innerhalb oder zwischen verschiedenen Welten in das Zentrum der Aufmerksamkeit. Geheimnisse und daraus entspringende Pflichten zeigten sich als Instrumente der Blockade von Informationsflüssen, was sich anhand der alten Geheimhaltungspflichten im Gesundheitsbereich (Hippokratischer Eid), aber auch im Kontext der Kirche (Beichtgeheimnis) bestätigte. In heutiger Terminologie lassen sich diese Geheimhaltungspflichten als die ältesten datenschutzrechtlichen Vorgaben beschreiben. Die untersuchten Beispiele liessen zudem deutlich werden, dass das Rechtsgebiet, das heute Datenschutzrecht genannt wird, nicht nur einzelne Menschen, stattdessen ebenso Institutionen schützt. Dass es um Informationsflüsse geht, wurde weiter anhand von Gestalten, die als Informationsmittler figurieren, namentlich dem Diener, sichtbar. 2043

Das *zweite Kapitel* beschrieb, inwiefern Informationsverarbeitungen als «Herrschaftstechnologien» zum Einsatz kamen. Hier wurde belegt, wie alt systematische und systematisierende Personendatenerfassungen sind – von den biblischen Volkszählungen über das mittelalterliche Buch des Lebens bis hin zur Etablierung absolutistischer Staatsherrschaften (Philipp II. ging mit dem Titel «Papier- 2044

könig» in die Geschichte ein). Derartige Herrschaftstechnologien mit ihren Verarbeitungsprozessen stiessen oft auf Widerstand (eine Genferin wurde inhaftiert, weil sie die Kreidenummerierung an ihrem Haus, welche auch der Personenerfassung diene, entfernte).

2045 Es folgte im *dritten Kapitel* eine Annäherung an den Begriff des «Privaten» und dessen Schutz. Nach einem Blick auf die Bedeutung der Freiheitsrechte für die Entwicklung des *Privatheitsschutzes* und die Herausbildung eines privaten Lebensbereiches im Privatbereich, der stark räumlich konzipiert wurde («my home is my castle»), wendete sich die Studie der Entwicklung der ersten Datenschutzerlasse zu.

2046 Der **zweite Teil** befasste sich unter dem Titel «Die drei Strukturmerkmale des DSG» mit der *Funktionsweise* des schweizerischen Datenschutzgesetzes. Es wurde gefragt, wie das DSG konzeptionell aufgebaut ist. Insofern wurden *drei tragende Säulen* herausgearbeitet, an denen das DSG auch nach seiner Totalrevision festhält. Immerhin bringt die Totalrevision neue Ansätze, womit die drei traditionellen Strukturmerkmale neu kontextualisiert werden.

2047 Im *vierten Kapitel* wurde der «Dualismus» als erstes Strukturmerkmal vorgestellt. Prägend für das schweizerische Datenschutzgesetz ist, dass Personendatenverarbeitungen durch öffentliche Stellen des Bundes anders geregelt werden als Personendatenverarbeitungen durch Private. Hieran ändert weder die Systematik des Gesetzes, beiden Bereichen einen gemeinsamen Teil voranzustellen, in dem auch die allgemeinen Verarbeitungsgrundsätze verortet werden, noch die Bezeichnung des DSG als Einheitsgesetz etwas. Markant wird die Differenzierung der Regelung für die beiden Bereiche anhand der entgegengesetzten Ausgangspunkte implementiert: Für den öffentlichen Bereich gilt ein prinzipielles Verarbeitungsverbot mit Erlaubnisvorbehalt. Die gesetzliche Grundlage ist hier von herausragender Bedeutung. Für den privaten Bereich gilt die prinzipielle Verarbeitungsfreiheit mit Schranken, die in erster Linie durch die allgemeinen Verarbeitungsgrundsätze gesetzt werden. Der Entscheid für ein dualistisches Regime, das Personendatenverarbeitungen durch Privatpersonen anders regelt als Personendatenverarbeitungen durch öffentliche Stellen des Bundes, war Ergebnis der politischen Kräfte. Namentlich wirtschaftsfreundliche Positionen führten dazu, dass die datenschutzrechtlichen Vorgaben stark divergieren und das Schutzniveau für den sog. privaten Bereich geringer ist als für den öffentlichen Bereich. Dualistische Regime können als Grobversionen eines datenschutzrechtlichen Systemschutzes bezeichnet werden, da sie die Differenzierungswürdigkeit zwischen verschiedenen gesellschaftlichen Bereichen anerkennen. Die Schweiz weicht mit der Totalrevision, ungeachtet des Übergangs der DSGVO zu einem monistischen Modell, nicht von ihrem Dualismus ab. Die Vorstellung, wonach die Schweiz ein

Recht auf informationelle Selbstbestimmung verankert, wurde in diesem Teil für den privaten Bereich als unzutreffend beurteilt.

Das *fünfte Kapitel* widmete sich dem «generalklauselartigen Regelungsansatz» als zweitem Strukturmerkmal. Insofern wurden die allgemeinen Verarbeitungsgrundsätze in den Dualismus eingepasst. Die Ausführungen in diesem Kapitel zielten zudem darauf ab, praxisrelevante sowie dogmatische Erkenntnisse zu den tragenden Verarbeitungsgrundsätzen zu generieren. Damit ging es auch darum, den für das Datenschutzrecht elementaren generalklauselartigen Vorgaben eine konkretisierende Struktur zu geben. Die Analyse der einzelnen Verarbeitungsgrundsätze förderte zu Tage, inwiefern sich in ihnen systemrelative Ansätze finden. Als ergiebig stellten sich die Analyse des Zweckbindungsgrundsatzes und in diesem Zusammenhang die Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil heraus. Das Urteil gilt als Magna Carta des Datenschutzrechts. Rezipiert wurden in erster Linie dessen subjektivrechtliche Dimension und das Grundrecht auf informationellen Subjektschutz. Das Urteil führt indes unmissverständlich den Systemschutz durch das Datenschutzrecht vor Augen: Nur wenn die Bürgerinnen und Bürger auf das Statistikgeheimnis vertrauen dürfen und Personendaten, die zum Zweck der Volkszählung erfasst werden, nicht zur Erfüllung anderer Verwaltungsaufgaben genützt werden, könne die Integrität der Statistik gewährleistet werden. Wenn die Bürgerinnen und Bürger dagegen befürchten müssten, dass von ihnen zum Zweck der Volkszählung erteilte Informationen z. B. zu Konsequenzen im Steuer- oder Migrationsbereich führen, wäre nicht mit wahrheitsgemässen und vollständigen Informationen zu rechnen. Verwaltungssanktionen könnten dies nicht verhindern. Nur eine strenge Zweckbindung, das Statistikgeheimnis sowie organisatorische Massnahmen würden das Funktionieren der statistischen Erhebung sicherstellen. Die Analyse der weiteren Verarbeitungsgrundsätze bestätigte die Bedeutung des Systemschutzes. 2048

Im *sechsten Kapitel* verengte sich der Fokus auf die Normierung des Datenschutzgesetzes für den privaten Bereich. Titelgebend für das dritte Strukturmerkmal war der «Persönlichkeitsschutz». Schutzobjekt der Normen des DSG für den privaten Bereich ist die Persönlichkeit, anknüpfend an Art. 28 ff. ZGB. In diesem Kapitel wurden die konkretisierenden Normen des DSG, Art. 12 ff. DSG resp. 30 ff. nDSG vertiefend dargestellt. Gezeigt wurde, dass die prinzipielle Verarbeitungsfreiheit in erster Linie durch die generalklauselartigen Grundsätze limitiert wird. Der Wille des Datensubjektes wird als Widerspruch oder als Rechtfertigungsgrund integriert. Das Regime wurde als Missbrauchsgesetzgebung taxiert, eine Qualifikation als Recht auf informationelle Selbstbestimmung verworfen. Diese Beurteilung wurde durch einen Blick auf das Recht am eigenen Bild und dessen Funktionsweise sowie durch eine Untersuchung der Einwilligungskonstruktionen im Biomedizinrecht erhärtet. Das DSG dagegen lehnt sich eng an die 2049

Mechanik von Art. 28 ff. ZGB an. Folglich ist das DSG vom *Subjektschutz,* dem *Persönlichkeitsschutz* geprägt. Damit handelt es sich um eine deliktsrechtliche und abwehrrechtliche Konstruktion.

2050 Der **dritte Teil** dieser Arbeit stand unter dem Titel «Vom Recht auf informationellen Subjektschutz zum Recht auf informationellen Systemschutz».

2051 Das *siebte Kapitel* knüpfte unter der Überschrift «Datenschutz auf dem Prüfstand» an die im zweiten Teil beschriebenen Strukturmerkmale an und analysierte, wie funktionstüchtig die Normierung durch das DSG ist. Das Ergebnis lautete, dass auch für die Schweiz zunächst von einem eigentlichen *Vollzugsdefizit* ausgegangen werden muss. Mit anderen Worten blieb und bleibt das DSG weitgehend toter Buchstabe, die faktische Verwirklichung und Umsetzung ist ungenügend. Die schwache Einhaltung des Gesetzes wurde im privaten Bereich insb. mit dem geringen Risiko von Konsequenzen begründet. Interventionen vonseiten des EDÖB oder individualrechtliche Klagen vonseiten der Subjekte sind nicht ernsthaft zu befürchten. Es folgte eine Auseinandersetzung mit den – wenigen – Urteilen zum Datenschutzrecht. Problematisiert wurde die *inkonsequente Definierung des Schutzobjektes* in datenschutzrechtlichen Fällen durch die Schweizer Gerichte. Ein Gesetz, in dessen Zentrum Generalklauseln stehen, ist auf eine strukturierende und konkretisierende Rechtsprechung angewiesen. Diese vermisst man in der Schweiz. Immerhin haben in den letzten Jahren Interventionen des EDÖB aufgrund von sog. Systemfehlern dem Datenschutzrecht Nachdruck verliehen. Auch wenn dieses Instrument zur Rechtsdurchsetzung des Datenschutzrechts mit der Totalrevision des DSG fallengelassen wurde, zeigte sich in ihrer Analyse erneut die systemische Dimension des Datenschutzrechts. Mit ihr wird anerkannt, dass ein ausschliesslich individualrechtlicher Ansatz im Datenschutzrecht, auch was die Durchsetzung desselben bei Verstössen anbelangt, ungenügend ist. Zudem wurde festgestellt, dass mit den jüngsten Urteilen, die einer Intervention des EDÖB vorangingen, das Datenschutzrecht und die Rechtsprechung hierzu eine Aufwertung erfahren haben. Gleichwohl ist zu attestieren, dass die Wichtigkeit des Datenschutzrechts in der Praxis von den Unternehmen ungenügend beachtet wurde. Wie intensiv das Thema die Informationsgesellschaft beschäftigt, zeigte sich anhand eines Schlaglichts auf die *mediale Berichterstattung* und die *politischen Debatten.* Hier wurde deutlich, dass der Datenschutz und das Datenschutzrecht gerade auch spezifisch für bestimmte Gesellschaftsbereiche verhandelt werden. Den Abschluss des Kapitels bildete ein Blick auf die Ursachenforschung bezüglich der Defizite des aktuellen Datenschutzrechts. Genannt wurden die ungenügenden Sanktionsrisiken sowie die mangelnde strukturierende Wirkung eines generalklauselartigen Datenschutzrechts. Ein zentrales Begründungsmuster wurde, in Einklang mit dem subjektivrechtlichen Ansatz des zeitgenössischen Rechts, in der Achtlosigkeit der Da-

tensubjekte verortet, denen angelastet wird, für Rabatte und die Nutzung von vermeintlichen Gratisdiensten ihre Personendaten zu kommerzialisieren. Sodann wurde gezeigt, dass für Schwächen des Datenschutzrechts pauschal der rasante technologische Fortschritt verantwortlich gemacht wird. Eine Evaluation dieser *Erklärungsmuster* ist von hoher Bedeutung. Nur wenn die Defizite in zutreffender und hinreichend präziser Weise identifiziert werden, sind Fortschritte zu ihrer Beseitigung im und durch das Recht denkbar. Folglich wurden in diesem Kapitel zwei Herausforderungen, die faktischer Natur sind, präziser dargestellt: erstens die *neuen Informationstechnologien* und zweitens die *Kommerzialisierungstendenzen*. Die *neuen Technologien* wurden anhand dreier Potenzen beschrieben: Tracking und Monitoring, Aggregierung und Analyse sowie Verteilung und Veröffentlichung resp. umgekehrt: Aufgreifen und Zugreifen. Diese drei Potenzen werden regelmässig miteinander kombiniert. Mit diesen Ausführungen konnte ein besseres und genaueres Verständnis der Funktionsweisen und Gefährdungspotentiale neuer Informationsverarbeitungstechnologien gewonnen werden. Unübersehbar wurde, dass allein das Bild von Informationsflüssen in Netzwerkstrukturen Ausgangspunkt datenschutzrechtlicher Analysen sein kann. Es ist deutlich besser geeignet, datenschutzrechtliche Herausforderungen abzubilden, als eine Vorstellung, die einem Datensubjekt Personendaten als Quasi-Objekte gegenüberstellt. Ähnlich wie die Chiffre des rasanten technischen Fortschritts wurde diejenige von «Daten sind das Gold des 21. Jahrhunderts» dekodiert. Bewusst wurde darauf verzichtet, einen weiteren zivilrechtlichen Beitrag zur Kommerzialisierung des Persönlichkeitsrechts zu leisten. Stattdessen wurde anhand einer *Stufenfolge* herausgearbeitet, inwiefern im Zusammenhang mit Personendaten *expandierende wirtschaftliche Begehrlichkeiten* zur Erosion anderer gesellschaftlicher Bereiche führen. Die Praxis von Kreditauskunfteien bildete eines der Illustrationsbeispiele.

Es folgte im *achten Kapitel* eine Analyse der «jüngsten Lösungsstrategien». Im 2052
Vordergrund stand hier die Präsentation der *legislativen Neuerungen*, namentlich der DSGVO, zudem der Totalrevision des DSG. Nachgezeichnet wurden die wichtigsten Entwicklungstrends: der lange Arm der DSGVO, aber auch des DSG in territorialer Hinsicht, der Ansatz diversifizierter Schutzziele trotz des Übergangs zu einem Monismus, der Ansatz der Stärkung der Rechtsposition des Datensubjektes, der Ansatz der faktischen Verwirklichung des Datenschutzrechts, der Compliance-, Governance- und Accountability-Ansatz, der risikobasierte Ansatz sowie der Ansatz der starken Behördenhand. Im DSG bedeutet die Integration mehrerer neuer Ansätze durch die Totalrevision, dass die drei Strukturmerkmale des bisherigen DSG eine neue Einbettung und damit eine neue Bedeutung finden werden. Es folgte eine Auseinandersetzung mit den wichtigsten der in der *Lehre diskutierten Ansätze*. Wie sich zeigte, kommt vorrangige

Bedeutung den im Subjektschutz basierten *Einwilligungskonstruktionen* zu. Sie werden sowohl *persönlichkeitsrechtlich* wie *eigentumsrechtlich* diskutiert, wobei die Begründung eines eigentlichen Herrschaftsrechts der Datensubjekte im Vordergrund steht. In die Gegenrichtung weist der *Anonymisierungsansatz*, bei dem das Band zwischen Datensubjekt und Personendaten nicht gestärkt, stattdessen gekappt wird. Bezüglich beider Lösungsansätze wurden *Einwände* diskutiert, denen zufolge beide Ansätze sowohl konzeptionell wie faktisch an ihre Grenzen stossen. Basierend auch auf diesen kritischen Einwänden wurde die Entwicklung eines neuen Paradigmas möglich.

2053 Das *neunte Kapitel* widmete sich der Theoriebildung für ein «Recht auf informationellen Systemschutz». Ausgangspunkt war eine Fallkonstellation zur geheimen Observation im (öffentlich-rechtlichen) Versicherungskontext. Die Analyse des Sachverhaltes, des Bundesgerichtsurteils sowie des anschliessenden Urteils des EMGR, EGMR Nr. 61838/10 – Vukato-Bojić/Schweiz, Urteil vom 18. Oktober 2016, zeigte, dass sich die rechtliche Konfliktlage nicht in einem bipolaren und individualrechtlichen Konflikt erschöpft. Rechtlich problematisch ist nicht erst eine konkret durchgeführte Observation des Privatlebens einer IV-Beziehenden, getragen von wirtschaftlichen Motiven der IV-Versicherung. Vielmehr erodiert die Praxis – ungeachtet der Frage, ob sie gesetzlich vorgesehen ist oder nicht – bereits aufgrund der potentiellen Möglichkeit die Integrität des Privatlebens des Kollektivs der IV-Beziehenden, zudem die Integrität des Sozialversicherungskontextes und, im Zusammenhang mit der IV, die Integrität des Gesundheitsbereichs. Wenn Versicherungen aus wirtschaftlichen Motiven selbst bei nicht erhärtetem Betrugsverdacht die Expertisen des medizinisch zuständigen Personals systematisch in Frage stellen und medizinisch nicht geschulte Personen – in diesem Fall Detektive – mittels geheimer Observation eine Invalidität beurteilen sollen, wird nicht nur der Gesellschaftsbereich des Privatlebens erodiert. Die Praxis unterminiert zugleich die Integrität des Gesundheits- und Sozialversicherungsbereichs, indem sie die dort geltenden Ziele, Logiken und Rationalitäten durchkreuzt. Anhand des konkreten Falles wurde die *kollektive Dimension des Rechtskonfliktes* herausgearbeitet, wobei sich die Untersuchung systemtheoretische Ansätze zunutze machte.

2054 Das *Recht auf informationellen Systemschutz* ist ein *neues Paradigma* zur Gestaltung des Datenschutzes und des Datenschutzrechts der Zukunft. Seine Aufgabe wird sein, Flüsse von Personendaten ausdifferenziert so zu gestalten, dass die Robustheit von etablierten Teilsystemen unserer Gesellschaft garantiert wird. Das Datenschutzrecht der Zukunft kann nur ein systemadäquates Recht sein. Die systemische Dimension des Datenschutzrechts war zwar seit jeher in diesem angelegt; ihre Bedeutung wurde bisher aber nicht erkannt und folglich auch nicht anerkannt. Mit dem Recht auf informationellen Systemschutz wird das Da-

tenschutzrecht zum Garanten für die Integrität stabilisierter und stabilisierender gesellschaftlicher Bereiche. Es leistet einen Beitrag zum Schutz der Demokratie, des privaten und freiheitlichen Lebens, der Gesundheit, der Wissenschaft und Forschung, des Sozialstaats, des Arbeitskontextes usf. Indem das künftige Datenschutzrecht auf den Schutz gesellschaftlicher Systeme abzielt, wird es auch seinen Schutzauftrag gegenüber dem einzelnen Subjekt wahrnehmen können. Denn das *Recht auf informationellen Systemschutz inkludiert den informationellen Subjektschutz*. Erst damit wird das Datenschutzrecht all seinen Bedeutungsdimensionen gerecht. Erst damit wird das Datenschutzrecht seinen Schutzzielen – dem Schutz des Subjektes, aber auch dem Schutz etablierter Institutionen – wirksam Nachachtung verschaffen.

Literaturverzeichnis

A

Aebi-Müller Regina E., Die Privatsphäre des Arbeitnehmers, in: Girsberger Daniel/Schmid Jörg (Hrsg.), Neue Rechtsfragen rund um die KMU: Erb-, Steuer-, Sozialversicherungs- und Arbeitsrecht, Zürich 2006, S. 13 ff.

Dies., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes. Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Habil. Bern 2005

Ahn Byung Ha, Der vermögensrechtliche Zuweisungsgehalt des Persönlichkeitsrechts, Diss. Berlin 2009

Ahrens Claus, Die Verwertung persönlichkeitsrechtlicher Positionen, Habil. Würzburg 2002

Albers Marion, Informationelle Selbstbestimmung, Habil. Baden-Baden 2005

Allen Anita L., Privacy Law. Positive Theory and Normative Practice, Harv. L. Rev. Forum 2013, S. 241 ff.

Althaus Stämpfli Annette, Personendaten von Bankkunden. Ihre Weiterleitung im Finanzkonzern und an dritte Dienstleister, Bern 2004

Amelung Ulrich, Der Schutz der Privatheit im Zivilrecht: Schadensersatz und Gewinnabschöpfung bei Verletzung des Rechts auf Selbstbestimmung über personenbezogene Informationen im deutschen, englischen und US-amerikanischen Recht, Diss. Tübingen 2002

Amman Martin, Datenschutz im Bank- und Kreditbereich. Eine Studie zu einem Schweizer Datenschutzgesetz unter Berücksichtigung ausländischer Erfahrungen, insbesondere in der BRD und in den USA, Diss. Zürich 1987

Ders., Unternehmen im neuen gesetzlichen Umfeld. Problemreiche Beurteilung der Kreditwürdigkeit, NZZ vom 28. März 1990

Amstutz Marc, Dateneigentum: Eckstein der kommenden Digitalordnung, NZZ vom 5. September 2018, S. 10

Ders., Dateneigentum: Funktion und Form, AcP 2018, S. 438 ff.

Ders., Der Text des Gesetzes: Genealogie und Evolution von Art. 1 ZGB, Schweizerischer Juristentag 2007, 100 Jahre ZGB, ZSR 2007, S. 237 ff.

Angwin Julia, The web's new gold mine: Your secrets, WSJ vom 30. Juli 2010

Aries Philippe/Duby Georges/Veyne Paul (Hrsg.), Geschichte des privaten Lebens, Frankfurt a. M. 1989

Arnold Jörg, Daten aus dem Auto – Digitale Spuren im Strassenverkehr, Jusletter IT vom 24. November 2016

Arter Oliver/Jörg Florian S. (Hrsg.), Entertainment Law, Bern 2006

Auer Marietta, Der privatrechtliche Diskurs der Moderne, Habil. Tübingen 2014 (zit. Diskurs)

Dies., Digitale Leistungen, ZfPW 2019, S. 130 ff.

Dies., Eigentum, Familie, Erbrecht. Drei Lehrstücke zur Bedeutung der Rechtsphilosophie im Privatrecht, AcP 2016, S. 239 ff.

Dies., Materialisierung, Flexibilisierung, Richterfreiheit, Diss. Tübingen 2004 (zit. Materialisierung)

Auf der Mauer Rolf/Fehr-Bossard Delia, Personalisierte Werbung, in: Thouvenin Florent/Weber Rolf H. (Hrsg.), Werbung – Online, ITSL 2017, S. 23 ff.

Aulehner Josef, 10 Jahre «Volkszählungs»-Urteil. Rechtsgut und Schutzbereich des Rechts auf informationelle Selbstbestimmung in der Rechtsprechung, CR 1993, S. 446 ff.

B

Baer Susanne, Rechtssoziologie. Eine Einführung in die interdisziplinäre Rechtsforschung. 3. Aufl., Baden-Baden 2017

Baeriswyl Bruno, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber Rolf/Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, ZIK 2014, S. 45 ff.

Ders., Daten als Medizin – das neue Paradigma, digma 2014, S. 52 ff.

Ders., Datennutzung und Datensouveränität. Bringen Individualrechte an Daten den Ausgleich zwischen den Datenbearbeitern und den betroffenen Personen?, digma 2019, S. 156 f.

Ders., Der «grosse Bruder» DSGVO und das revDSG: Ein vergleichender Überblick, SZW 2021, S. 8 ff.

Ders., Der Schatten über der Anonymität. Anonymität ist Teil der informationellen Selbstbestimmung, technisch aber schwierig umzusetzen, digma 2008, S. 4 f.

Ders., Geschichten aus dem Wilden Westen. Der Datenschutz im privatrechtlichen Bereich geht seine eigenen Wege: Der Grundrechtsschutz bleibt auf der Strecke, digma 2010, S. 140 ff.

Ders., Kleingedrucktes unter der Lupe – Die Allgemeinen Geschäftsbedingungen (AGB) von Sozialen Netzwerken versprechen keinen Datenschutz, digma 2010, S. 56 ff.

Ders., Mehr Transparenz im neuen DSG, digma 2020, S. 6 ff.

Ders., Vom eindimensionalen zum mehrdimensionalen Datenschutz – Tendenzen der Rechtsentwicklung, in: Baeriswyl Bruno/Rudin Beat (Hrsg.), Perspektive Datenschutz. Praxis und Entwicklungen in Recht und Technik, Zürich/Baden-Baden/Wien 2002, S. 47 ff.

Ders., Wie weiter mit dem Datenschutz? Eine Bilanz nach zehn Jahren eidgenössisches Datenschutzgesetz, digma 2003, S. 48 ff.

Baeriswyl Bruno/Rudin Beat, Moderner Datenschutz – auch eine Wachstumschance für die Wirtschaft, Jusletter vom 28. Juni 2004

Ballenegger Sarah, Kommentar zu Art. 17 DSG, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG)

Balthasar Alexander, Datenschutz im Internet. Faktische und damit rechtliche Grenzen auch für den demokratischen Gesetzgeber?, Jusletter IT vom 20. Februar 2014

Balthasar Stephan, Der Schutz der Privatsphäre im Zivilrecht. Eine historisch-vergleichende Untersuchung zum deutschen, französischen und englischen Recht vom ius commune bis heute, Diss. Tübingen 2006

Barocas Solon/Nissenbaum Helen, Big Data's End Run around Anonymity and Consent, in: Lane Julia/Stodden Victoria/Bender Stefan/Nissenbaum Helen (ed.), Privacy, Big Data, and the Public Good, Cambridge 2016, S. 44 ff.

Dies., Big Data's End Run around Procedural Privacy Protections, Communications of the ACM 2014, S. 31 ff.

Dies., On Notice. The Trouble with Notice and Consent, Proceedings of the Engaging Data Forum, The First International Forum on the Application and Management of Personal Electronic Information, October 2009

Bartsch Michael, Eine kurze Geschichte der Privatheit, in: Bartsch Michael/Briner Robert G. (Hrsg.), DGRI Jahrbuch 2010, Berlin 2011, S. 31 ff.

Bartsch Verena, Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte, Berlin 2004

Bartuschka Wolfram, Künstliche Intelligenz, Chatbots, Robot Process Automation – neue Technologien als Fluch oder Segen für gute Compliance?, CB 2019, S. 340 ff.

Basho Kalinda, The Licencing of Our Personal Information. Is It a Solution to Internet Privacy?, Calif. L. Rev. 2000, S. 1507 ff.

Bauer Andreas/Günzel Holger (Hrsg.), Data-Warehouse-System: Architektur, Entwicklung, Anwendung, 3. Aufl., Heidelberg 2009

Baumann Robert, Der nummerierte Bürger, SJZ 2006, S. 1 ff.

Bächli Marc, Das Recht am eigenen Bild. Die Verwendung von Personenbildern in den Medien, in der Kunst, der Wissenschaft und in der Werbung aus der Sicht der abgebildeten Person, Diss. Basel/Genf/München 2002

Bäumler Helmut, Marktwirtschaftlicher Datenschutz, digma 2003, S. 30 ff.

Bechtold Stefan, Vom Urheber zum Informationsrecht. Implikationen des Digital Rights Management, Schriftreihe Information und Recht, Bd. 33, München 2002

Becker Jürgen/Hilty Reto M./Stöckli Jean-Fritz/Würtenberger Thomas (Hrsg.), Recht im Wandel seines sozialen und technologischen Umfeldes. Festschrift für Manfred Rehbinder, München 2002

Belser Eva M., Zur rechtlichen Tragweite des Grundrechts auf Datenschutz: Missbrauchsschutz oder Schutz der informationellen Selbstbestimmung?, in: Epiney Astrid/Fasnacht Tobias/Blaser Gaëtan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung/Instruments de mise en œuvre du droit à l'autodétermination informationnelle, Bern 2013, S. 19 ff.

Belser Eva M./Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011

Belser Eva M./Noureddine Hussein, Kommentar zu §§ 7–8, in: Belser Eva M./Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011

Belser Urs, Das Datenschutzgütesiegel GoodPriv@cy® – Blaupause für den Artikel 11 DSG? in: Weber Rolf H./Thouvenin Florent, Datenschutz-Managementsysteme im Aufwind? ZIK 2016, S. 143 ff.

Ders., Das Recht auf Auskunft, die Transparenz der Datenbearbeitung und das Auskunftsverfahren, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 55 ff.

Ders., Die Technikneutralität des Datenschutzgesetzes, ein strategisch richtiger Entscheid des Gesetzgebers?, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing: 20 Jahre Datenschutz in der Schweiz, Zürich 2012, S. 1 ff.

Benhamou Yaniv/Tran Laurent, Circulation des biens numériques : de la commercialisation à la portabilité, sic! 2016, S. 571 ff.

Bennett Coin J., Regulating Privacy – Data Protection and Public Policy in Europe and the United States, New York 1992

Beranek Zanon Nicole, Big Data und Datensicherheit, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, S. 86 ff.

Bergelson Vera, It's Personal But is it Mine? Toward Property Rights in Personal Information, UC Davis L. Rev. 2003, S. 379 ff.

Berger Kurzen Brigitte, E-Health und Datenschutz, Diss. Zürich 2004

Bergmann Susanne, Publicity Rights in the United States and in Germany. A Comparative Analysis, Loyola of Los Angeles ELR 1999, S. 479 ff.

Bergt Matthias, Sanktionierungen von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, S. 555 ff.

Bernard Andreas, Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur, Frankfurt a. M. 2017

Beurskens Michael, Vom Sacheigentum zum „virtuellen Eigentum"? – Absolute Rechte an „Daten", in: Domej Tanja/Dörr Bianka S./Hoffmann-Nowotny u. a. (Hrsg.), Einheit des Privatrechts, komplexe Welt: Herausforderungen durch fortschreitende Spezialisierung und Interdisziplinarität. Jahrbuch Junger Zivilrechtswissenschaftler 2008, Stuttgart 2009, S. 443 ff.

Beuter Claudia, Die Kommerzialisierung des Persönlichkeitsrechts, Diss. Konstanz 2000, abrufbar unter: <http://w3.ub.uni-konstanz.de/kops/volltexte/2000/406/>

Beuthien Volker, Schützt das allgemeine Persönlichkeitsrecht auch kommerzielle Interessen der Person?, in: Beuthien Volker (Hrsg.), Persönlichkeitsgüterschutz vor und nach dem Tode, in: Marburger Medienschriften, Bd. 4, Baden-Baden 2002, S. 9 ff.

Ders., Was ist vermögenswert, die Persönlichkeit oder ihr Image?, NJW 2003, S. 1220 ff.

Beuthien Volker/Hieke Marion, Unerlaubte Werbung mit dem Abbild prominenter Personen, AfP 2001, S. 353 ff.

Beuthien Volker/Schmölz Anton Sebastian, Persönlichkeitsschutz durch Persönlichkeitsgüterrechte, München 1999

Bibas Stephanos, A Contractual Approach to Data Privacy, Harv. J.L. & Pub. Pol'y 1994, S. 591 ff.

Biene Daniel, Starkult, Individuum und Persönlichkeit. Überlegungen zur interessengerechten rechtlichen Gestaltung der wirtschaftlichen Nutzung von Persönlichkeitsaspekten, Diss. Zürich/Bern 2004

Bieri Adrian/Powell Julian, Die Totalrevision des Bundesgesetzes über den Datenschutz. Übersicht der wichtigsten Neuerungen für Unternehmen, Jusletter vom 16. November 2020

Bijok Alexander, Kommerzialisierungsfester Datenschutz. Rechtliche Problemlagen der Datennutzung in der Informationswirtschaft, Baden-Baden 2020

Birnhack Michael D., The EU Data Protection Directive: An Engine of a Global Regime, CLSR 2008, S. 508 ff.

Bischof Severin/Schweizer Rainer J., Der Begriff der Personendaten, digma 2011, S. 152 ff.

Blauert Andreas/Wiebel Eva, Gauner- und Diebslisten, Frankfurt a. M. 2001

Blechta Gabor, Kommentar zu Art. 3 und Art. 4 DSG, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG)

Blonski Dominika, Aus den Datenschutzbehörden, digma 2019, S. 100 f.

Dies., Aus den Datenschutzbehörden, digma 2018, S. 154 ff.

Boehm Franziska, Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-Level, Heidelberg u. a. 2012

Bohnet François/Melcarne Luca, Le secret professionnel du médecin, de l'avocat, du notaire et de l'agent d'affaires dans la poursuite pour dettes : recouvrement des créances, devoir de renseigner et de remettre, JdT 2020 II, S. 31 ff.

Boll Jürg, Die Entbindung vom Arzt- und Anwaltsgeheimnis, Diss. Zürich 1983

Bolliger Christian/Féraud Marius/Epiney Astrid/Hänni Julia, Evaluation des Bundesgesetzes über den Datenschutz, Schlussbericht, Bern 2011

Bondallaz Stéphane, La protection des personnes et de leurs données dans les télécommunications. Analyse critique et plaidoyer pour un système en droit suisse, Diss. Zürich 2007

Borges Georg, Die Datenschutz-Grundverordnung. Potentiale für praxisgerechten Datenschutz, Jusletter IT vom 23. Februar 2017

Bossardt Matthias, § 21 Organisatorische und technische Datenschutzmassnahmen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, 557 ff.

Bosse Christian K./Dietrich Aljoscha/Kelbert Patricia u. a., Beschäftigtendatenschutz: Rechtliche Anforderungen und technische Lösungskonzepte, Jusletter IT vom 28. Februar 2020

Böckenförde Thomas, Auf dem Weg zu einer elektronischen Privatsphäre. Zugleich eine Besprechung von BVerfG, Urteil vom 27. Februar 2008 – „Online-Durchsuchung", JZ 2008, S. 925 ff.

Brant sebastian, Sebastian Brants Narrenschiff: Ein Hausschatz zur Ergetzung und Erbauung, erneuert von Karl Simrock, Verlag Franz Lipperheide, Berlin 1872

Breitenmoser Stephan/Schweizer Rainer J., Kommentar zu Art. 13 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die Schweizerische Bundesverfassung: St. Galler Kommentar, Zürich/St. Gallen 2014, S. 306 ff.

Breitschmid Peter, Kommentar zu Art. 11 ff. ZGB, in: Breitschmid Peter/Jungo Alexandra (Hrsg.), Handkommentar zum Schweizer Privatrecht, Art. 1–456 ZGB, 3. Aufl., Zürich 2016

Breitschmid Peter/Jungo Alexandra (Hrsg.), Handkommentar zum Schweizer Privatrecht, Art. 1–456 ZGB, 3. Aufl., Zürich 2016

Briner Robert G., Big Data und Sachenrecht, Jusletter IT vom 21. Mai 2015

Broger Urban, Ist der gläserne Steuerpflichtige bereits Realität? Möglichkeiten der schweizerischen Steuerbehörden im Bereich der Datenbearbeitung, zsis Monatsflash 2009

Brosette Josef, Der Wert der Wahrheit im Schatten des Rechts auf informationelle Selbstbestimmung. Schriften zum Recht des Informationsverkehrs und der Informationstechnik, Bd. 1, Berlin 1991

Browe Peter S.J., Das Beichtgeheimnis im Altertum und Mittelalter, Scholastik 1934, S. 1 ff.

Brunner Stephan C., Das revidierte Datenschutzgesetz und seine Auswirkungen im Gesundheits- und Versicherungswesen, in: Schaffhauser René/Horschik Matthias (Hrsg.), Datenschutz im Gesundheits- und Versicherungswesen, St. Gallen 2008, S. 142 ff.

Ders., Mit rostiger Flinte unterwegs in virtuellen Welten? Leitgedanken zur künftigen Entwicklung des schweizerischen Datenschutzrechts, Jusletter vom 4. April 2011

Brunton Finn/Nissenbaum Helen, Obfuscation. A User's Guide for Privacy and Protest, MIT Press 2015

Brunton Finn/Nissenbaum Helen, Political and ethical perspectives on data obfuscation, in: Hildebrandt Mireille/Bries Katja (ed.), Privacy, Due Process and the Computational Turns, New York 2013, S. 164 ff.

Brunton Finn/Nissenbaum Helen, Vernacular Resistance to Data Collection and Analysis. A Political Theory of Obfuscation, First Monday 2011

Brühwiler-Frésey Lukas, Medizinischer Behandlungsvertrag und Datenrecht, Zürich 1996

Bründler Rolf, Das erste schweizerische Datenschutzgesetz im Überblick, SJZ 1993, S. 129 ff.

Bucher Eugen, «Drittwirkung» der Grundrechte? – Überlegungen zu «Streikrecht» und «Drittwirkung» i. S. v. BGE 111 II 245–259, SJZ 1987, S. 37 ff.

Ders., Urteilsanmerkung: Das Horror-Konstrukt der «Zwangsmedikation»: zweimal (ohne Zuständigkeit) ein Ausflug ins juristische Nirwana. Zu BGE 126 I 112–121 und BGE 127 I 6–30, ZBJV 2001, S. 764 ff.

Ders., Vertrauenshaftung: Was? Woher? Wohin?, in: Forstmoser Peter/Honsell Heinrich/Wiegand Wolfgang (Hrsg.), Richterliche Rechtsfortbildung in Theorie und Praxis: Methodenlehre und Privatrecht, Zivilprozess- und Wettbewerbsrecht. Festschrift für Hans Peter Walter, Bern 2004, S. 231 ff.

Bucher Manuel, Spyware: Rechtliche Würdigung ausgewählter Fragen sowie Empfehlungen an die Praxis unter besonderer Berücksichtigung des Eidgenössischen Datenschutzgesetzes, Zürich/Basel/Genf 2010

Buchner, Benedikt, Der gläserne Sportler, DuD 2009, S. 475 ff.

Ders., Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument, DuD 2010, S. 39 ff.

Ders., Formularmässige Einwilligung, DuD 2010, S. 52

Ders., Informationelle Selbstbestimmung im Privatrecht, Habil. Tübingen 2006

Ders., Kommentar zu Art. 22 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, München 2017 (zit. Beck-Komm.-DSGVO)

Buchner Benedikt/Kühling Jürgen, Kommentar zu Art. 4 Nr. 11, Art. 7 und Art. 8 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, München 2017 (zit. Beck-Komm.-DSGVO)

Buchner Benedikt/Petri Thomas, Kommentar zu Art. 6 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, München 2017 (zit. Beck-Komm.-DSGVO)

Bull Hans Peter, Datenschutz oder die Angst vor dem Computer, München 1984 (zit. Computer)

Ders., Informationelle Selbstbestimmung – Vision oder Illusion, 2. Aufl., Tübingen 2011 (zit. Vision)

Ders., Neue Bewegung im Datenschutz – Missbrauchsbekämpfung oder Ausbau bereichsspezifischer Regelungen?, ZRP 2008, S. 233 ff.

Ders., Persönlichkeitsschutz im Internet: Reformeifer mit neuen Ansätzen, NVwZ 2011, S. 257 ff.

Ders., Vom Datenschutz zum Informationsrecht – Hoffnungen und Enttäuschungen, in: Hohmann Harald (Hrsg.), Freiheitssicherung durch Datenschutz, Frankfurt a. M. 1987, S. 173 ff.

Bungart Frederik, Dingliche Lizenzen an Persönlichkeitsrechten, Baden-Baden 2005

Bunneberg Stefan, Namensmerchandising: Die Kommerzialisierung und Monopolisierung der Persönlichkeit ausgehend vom Familiennamen als Marke. Schriften zum Persönlichkeitsrecht, Bd. 1, Hamburg 2007

Burghardt Thorben/Böhm Klemens/Buchmann Erik/Kuhling Jurgen/Sivridis Anastasios, A Study on the Lack of Enforcement of Data Protection Act, in: Sivridis Alexander/Patrikakis Cahralampos, Proceedings of the 3rd International Conference on e-Democracy, Athen 2009, S. 3 ff.

Burkert Herbert, Aktuelle Herausforderungen des Datenschutzrechts im Kontext nationaler und internationaler Entwicklungen, in: Epiney Astrid/Fasnacht Tobias/Blaser Gaëtan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2013, S. 1 ff.

Ders., Datenschutz, in: Jung Reinhard/Winter Robert (Hrsg.), Data Warehousing Strategie: Erfahrungen, Methoden, Visionen, St. Gallen 2000, S. 117 ff.

Ders., Internet und Recht. Ansätze zu einem Versuch einer etwas allgemeineren Betrachtung mit ungewissem Ausgang, in: Drossu Olga/van Haaren Kurt/Hensche Detlev et al. (Hrsg.), Machtfragen der Informationsgesellschaft, Marburg 1999, S. 385 ff.

Ders., Personendaten als Handelsware? Datenschutz und Kommerzialisierung von Verwaltungsinformationen, in: Fakten. Die Zeitschrift für Datenschutz des Kantons Zürich, Sondernummer 4/1996, S. 23 ff.

Ders., Von künftigen Aufgaben des Informationsrechts, in: Meier-Schatz Christian J./Schweizer Rainer J. (Hrsg.), Recht und Internationalisierung, Zürich 2000, S. 155 ff.

Busset Thomas, Zur Geschichte der eidgenössischen Volkszählung, in: Bundesamt für Statistik (Hrsg.), Statistik der Schweiz, Bern 1993, 15 ff.

Büchler Andrea, Die Kommerzialisierung von Persönlichkeitsgütern. Zur Dialektik von Ich und Mein, AcP 2006, S. 300 ff.

Dies., Persönlichkeitsgüter als Vertragsgegenstand? Von der Macht des Faktischen und der dogmatischen Ordnung, in: Honsell Heinrich/Portmann Wolfgang/Zäch Roger/Zobl Dieter (Hrsg.), Aktuelle Aspekte des Schuld- und Sachenrechts. Festschrift für Heinz Rey, Zürich 2003, S. 177 ff.

Büchler Andrea/Cottier Michelle, Legal Gender Studies. Rechtliche Geschlechterstudien. Eine kommentierte Quellensammlung, Zürich/St. Gallen 2012

Büchler Andrea/Jakob Dominique (Hrsg.), Kurzkommentar ZGB, 2. Aufl., Basel 2018 (zit. KuKo-ZGB)

Bühlmann Lukas/Lagler Marion, Informationspflichten und Auskunftsrecht nach dem neuen Datenschutzrecht, SZW 2021, S. 16 ff.

Bühlmann Lukas/Schüepp Michael, Information, Einwilligung und weitere Brennpunkte im (neuen) Schweizer Datenschutzrecht. Eine kritische Analyse anhand des Helsana+-Urteils, Jusletter vom 15. März 2021

Büllesbach Alfred/Dreier Thomas (Hrsg.), Wem gehört die Information im 21. Jahrhundert? Proprietäre versus nichtproprietäre Verwertung digitaler Informationen, Köln 2004

C

Cachelin Joël Luc, Offliner. Die Gegenkultur der Digitalisierung, Bern 2015

Caluori Corina, Der Verursacherbegriff im Altlastenrecht – eine kritische Analyse, URP 2011, S. 541 ff.

Camavdic Benjamin, Predictive Policing in der Schweiz, Jusletter IT vom 26. September 2019

Campbell Jody C., Who Owns Kim Basinger? The Right of Publicity's Place in the Bankruptcy System, J. Intell. Prop. L. 2005, S. 179 ff.

Cavoukian Ann, Der Schutz der Privatheit in der Wolke. Plädoyer für ein flexibles und nutzerzentriertes Identitätsmanagement als Erfolgsvoraussetzung für Cloud Computing, digma 2009, S. 20 ff.

Dies., Privacy by Design in Law, Policy and Practice, Ontario 2011

Cavoukian Ann/Chibba Michelle/Williams Graham/Ferguso Andrew, The Importance of ABAC to Big Data: Privacy and Context, Jusletter IT vom 21. Mai 2015

Cellina Eva/Geissbühler Grégoire, Collecte et transmission de données relatives au crédit : cadre légal, validité et limites, Jusletter vom 13. Juli 2014

Ceregato Mirco, Der Vorentwurf zur Revision der Schweizerischen Zivilprozessordnung – Übersicht und Würdigung, Jusletter vom 10. September 2018

Chappuis Guy/Hardegger Andreas, Observation Versicherter: Allheilmittel oder Schreckgespenst? HAVE 2018, S. 204 f.

Christensen Arthur/Spies Otto (Hrsg.), Persische Märchen. Die Märchen der Weltliteratur, Bd. 1, Düsseldorf 1984

Chu Wesley W. (ed.), Data Mining and Knowledge Discovery for Big Data. Methodologies, Challenges and Opportunities, Berlin/Heidelberg 2014

Cicchini Marco, A new 'inquisition'? Police reform, urban transparency and house numbering in eighteenth-century Geneva, Urban Hist. 2012, S. 614 ff.

Cichocki Michal, Big Data und Datenschutz: Ausgewählte Aspekte, Jusletter IT vom 21. Mai 2015

Ders., Erste Überlegungen zur klar zustimmenden Handlung sowie Freiwilligkeit bei der Einwilligung, Jusletter IT Flash vom 21. Januar 2016

Coen Adam, Social Media: Legal Risk and Corporate, New York 2013

Coll Sami, Big Data, Big Troubles? Enjeux éthiques et sociaux du big data, in: Epiney Astrid/Nüesch Daniela (Hrsg.), Big Data und Datenschutzrecht/Big Data et droit de la protection des données, Zürich 2016 (Separatum), S. 1 ff.

Conley Amanda/Datta Anupam/Nissenbaum Helen/Sharma Divya, Sustaining Privacy and Open Justice in the Transition to Online Court Records. A Multidisciplinary Inquiry, Md. L. Rev. 2012, S. 772 ff.

Cottier Bertil, L'ère numérique et le principe de légalité – Frictions et possibilités d'adaptions, Forum Europarecht 2018, Digitalisierung und Schutz der Privatsphäre/L'ère numérique et la protection de la sphère privée, S. 25 ff.

Ders., Gouvernance d'Internet : Protection de la vie privée et des données personnelles, SRIEL 2016, S. 255 ff.

Ders., La révision de la loi fédérale sur la protection des données : mieux vaut tard que jamais, Jusletter vom 17. Dezember 2007

Ders., Le droit d'accès aux documents officiels, in : Métille Sylvain (ed.), Le droit d'accès, Bern 2021, S. 139 ff.

Cottier Michelle, Kommentar zu Vor Art. 307 ff. ZGB, in: Büchler Andrea/Jakob Dominique (Hrsg.), Kurzkommentar ZGB, 2. Auflage, Basel 2018 (zit. KuKo-ZGB)

D

Danioth Hans, Ziele und Grundanliegen des Datenschutzes im öffentlichen Bereich, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 9 ff.

Datenschutz-forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing: 20 Jahre Datenschutz in der Schweiz, Zürich 2012

De Montjoye Yves-Alexandre/Radaelli Laura/Singh Vivek Kumar et al. (ed.), Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata, Science 2015, S. 536 ff.

De Werra Jacques, Entreprises et Big Data : peut-on forcer les entreprises à partager leurs données non-personnelles (par des licences obligatoires ou des licences „FRAND"), RSDA 2020, S. 365 ff.

Dejung Christof/Dommann Monika/Speich Chassé Daniel (Hrsg.), Auf der Suche nach der Ökonomie. Historische Annäherungen, Tübingen 2014

Derleder Peter, Die uneingelöste Grundrechtsbindung des Privatrechts, in: Jestaedt Matthias/Lepsius Oliver (Hrsg.), Verhältnismässigkeit. Zur Tragfähigkeit eines verfassungsrechtlichen Schlüsselkonzepts, Tübingen 2015, S. 234 ff.

Dickenson David L./Osaca Ronald L., Statistical Discrimination in Labor Markets: An Experimental Analysis, Digital Commons@USU, Economic Research Institute, Study Papers Economics and Finance, Utah State University 2004

Diercks Nina, Big Data-Analysen und Scoring in der (HR-)Praxis. Dürfen aus allgemein zugänglichen personenbezogenen (Arbeitnehmer-)Daten Score-Werte erstellt und genutzt werden?, PinG 2016, S. 30 ff.

Diethelm Dominique, Der strafrechtliche Schutz der Geheim- und Privatsphäre in der Pflege, in: Landolt Hardy/Blum-Schneider Brigitte/Breitschmid Peter u. a., Pflege in Politik, Wissenschaft und Ökonomie, S. 9 ff.

Dittrich Klaus R./Vavouras Athanasios, Data Warehousing aus technischer Sicht – Aufbau und Einsatz von Datenbanksystemen für die Verwaltung von mehrfachbenutzbaren Daten, digma 2001, S. 116 ff.

Dix Alexander, Kommentar zu § 41 BDSG, in: Simitis Spiros (Hrsg.), Bundesdatenschutzgesetz, NomosKommentar, 8. Aufl., Baden-Baden 2014

do Canto Philipp, Gesundheitsdaten in der digitalen Welt, sic! 2020, S. 177 ff.

Dolata Ulrich, Soziotechnischer Wandel als graduelle Transformation, Berl J Soziol 2011, S. 265 ff.

Domanig Andrea, Revision der ZPO. Aktueller Stand der Vorlage und Überblick über die geplanten Änderungen, Jusletter vom 17. Juni 2019

Dommann Monika, Autoren und Apparate. Die Geschichte des Copyrights im Medienwandel, Habil. Frankfurt a. M. 2014

Dies., Lost in tradition? Reconsidering the history of folklore and its legal protection since 1800, in: Graber Beat/Burri-Nenova Mira (ed.), Intellectual Property and Traditional Cultural Expressions in a Digital Environment, Cheltenham/Northampton 2008, S. 3 ff.

Dies., Mobile Medien, reguliertes Eigentum, in: Joly Jean-Baptiste/Visman Cornelia/Weitin Thomas (Hrsg.), Bildregime des Rechts, Stuttgart 2007, S. 249 ff.

Dies., Rechtsinstrumente. Die Übersetzung von Technik in Recht, SZG 2005, S. 17 ff.

Dies., Recording Prints, Reading Films – Mikrofilme, amerikanische Kosmopoliten und die Entdeckung des Copyrightproblems in den 1930erJahren, ZfM 2010, S. 73 ff.

Donos Pelopidas K., Datenschutz – Prinzipien und Ziele. Unter besonderer Berücksichtigung der Entwicklung der Kommunikations- und Systemtheorie, Diss. Frankfurt a. M./Baden-Baden 1998

Dougoud Maya/Pfaffinger Monika, «Das wahre Problem mit den Schüler-Masken», Inside Paradeplatz vom 25. Januar 2021

Dörflinger Tim, Das Private auf dem globalen Präsentierteller. Chancen und Risiken moderner Kommunikationstechnologien aus der Sicht der deutschen Bürger, Berlin 2009

Drallé Lutz, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Diss. Kiel 2010

Drechsler Christian, Die Revision des Datenschutzrechts, AJP 2007, S. 1471 ff.

Dreier Thomas, Creative Commons, Science Commons. Ein Paradigmenwechsel im Urheberrecht?, in: Ohly Ansgar/Bodewig Theo/Dreier Thomas/Götting Horst-Peter/Haedicke Maximilian/Lehmann Michael (Hrsg.), Perspektiven des Geistigen Eigentums und Wettbewerbsrechts. Festschrift für Gerhard Schricker, München 2005, S. 283 ff.

Ders., Erinnern Sie sich, als … sein Opfer S. erschlug? Löschung von Berichten aus Online-Archiven aus Gründen des Persönlichkeitsrechts?, in: Hilty Reto M./Drexl Josef/Nordemann Wilhelm (Hrsg.), Schutz von Kreativität und Wettbewerb. Festschrift für Ulrich Loewenheim, München 2009, S. 67 ff.

Ders., Informationsrecht in der Informationsgesellschaft, in: Bizer Johann/Lutterbeck Bernd/Riess Joachim (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft. Freundesgabe für Alfred Büllesbach, Stuttgart 2002, S. 65 ff.

Drossu Olga/van Haaren Kurt/Hensche Detlev et al. (Hrsg.), Machtfragen der Informationsgesellschaft, Marburg 1999

Druey Jean Nicolas, „Daten-Schmutz" – Rechtliche Ansatzpunkte zum Problem der Über-Information, in: Brem Ernst/Druey Jean Nicolas/Kramer Ernst A./Schwander Ivo (Hrsg.), Festschrift für Mario M. Pedrazzini, Bern 1990, S. 379 ff.

Ders., Der Informations-Fetischismus, in: Kramer Ernst A./Nobel Peter/Waldburger Robert (Hrsg.), Festschrift für Peter Böckli, Zürich 2006, S. 589 ff.

Ders., Information als Gegenstand des Rechts, Zürich/Baden-Baden 1995

Ders., Ist Geheimhaltung schützenswert?, BJM 2005, S. 57 ff.

Ders., Ist Wissen delegierbar? Oder: Das Recht, nicht zu wissen, in: Waldburger Robert/Baer Charlotte M./Nobel Ursula/Bernet Benno (Hrsg.), Wirtschaftsrecht zu Beginn des 21. Jahrhunderts. Festschrift für Peter Nobel, Bern 2005, S. 877 ff.

Ders., Schutz der Information, in: Weber Rolf H./Hilty Reto (Hrsg.), Daten und Datenbanken, Rechtsfragen zu Schutz und Nutzung, Zürich 1999, S. 7 ff.

Ders., Vertrauen durch Recht?, in: Rechtswissenschaftliche Abteilung der Universität St. Gallen (Hrsg.), Rechtliche Rahmenbedingungen des Wirtschaftsstandortes Schweiz, Zürich/St. Gallen 2007, S. 525 ff.

Ders., Verträge auf Informationsleistung, in: Forstmoser Peter/Tercier Pierre/Zäch Roger (Hrsg.), Innominatverträge: Festgabe zum 60. Geburtstag von Walter R. Schluep, Zürich 1988, S. 147 ff.

Dworkin Ronald, Gerechtigkeit für Igel, Berlin 2014 (zit. Gerechtigkeit)

Ders., Was ist Gleichheit?, 2. Aufl., Berlin 2014 (zit. Gleichheit)

E

Eberle Carl-Eugen, Informationsrechte – Der grosse Wurf? Zur Notwendigkeit bereichsspezifischer Regelungen, in: Wilhelm Rudolf (Hrsg.), Information – Technik – Recht. Rechtsgüterschutz in der Informationsgesellschaft, Darmstadt 1983, S. 113 ff.

Ebert Nico/Widmer Michael, Datenschutz in Schweizer Unternehmen 2018. Eine Studie des Instituts für Wirtschaftsinformatik und des Zentrums für Sozialrecht, ZHAW Winterthur, 2018

Eckert Martin, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, SJZ 2016, S. 265 ff.

Ders., Digitale Daten als Wirtschaftsgut: Digitale Daten als Sache, SJZ 2016, S. 245 ff.

Eckhardt Anne/Fattebert Sylvain/Keel Alois/Meyer Patrick, Der gläserne Kunde. Elektronische Erfassung und Auswertung von Kundendaten, Schweizerischer Wissenschafts- und Technologierat, Bern 2000

Eggen Mirjam, Home Smart Home. Eine privatrechtliche Einordnung von Lösungen für intelligentes Wohnen, AJP 2016, S. 1131 ff.

Egli Patricia/Rechsteiner David, Social Bots und Meinungsbildung in der Demokratie, AJP 2017, S. 249 ff.

Ehmann Horst, Das Persönlichkeitsrecht als Wert, als Grundrecht und als absolut-subjektives Recht, in: Stathopoulos Michael/Beys Kostas/Philippos Doris/Karakostas Ionannis (Hrsg.), Festschrift für Apostolos Georgiades zum 70. Geburtstag, Zürich 2006

Ders., Zum kommerziellen Interesse an Politikerpersönlichkeiten, AfP 2007, S. 81 ff.

Ders., Zur Struktur des Allgemeinen Persönlichkeitsrechts, Juristische Schulung, Zeitschrift für Studium und praktische Ausbildung 1997, S. 193 ff.

Eifert Martin, Informationelle Selbstbestimmung im Internet. Das Bundesverfassungsgericht und die Online-Durchsuchungen, NVwZ 2008, S. 521 ff.

Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019

Emmenegger Susan, Die Informationspflichten der Bank bei Anlagegeschäften. Tout devient du droit public?, in: Kunz Peter V./Herren Dorothea/Cottier Thomas/Matteotti René (Hrsg.), Wirtschaftsrecht in Theorie und Praxis. Festschrift für Roland von Büren, Basel 2009, S. 643 ff

Dies., Le devoir d'information du banquier, in: Chappuis Christine/Winiger Bénédict (Hrsg.), La responsabilité pour l'information fournie à titre professionnel, Genf/Zürich/Basel 2009, S. 67 ff.

Dies., Marlene und die «Ich-AG». Geburt einer neuen Rechtsfigur?, in: Gauch Peter/Pichonnaz Pascal (Hrsg.), Figures juridiques/Rechtsfiguren. Mélanges dissociés pour Pierre Tercier/Festschrift für Pierre Tercier, Zürich 2003, S. 209 ff.

Emmenegger Susan/Reber Martina, Biometrische Daten im Bankkundenverkehr am Beispiel der Stimmauthentifizierung, in: Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 162 ff.

Emmenegger Susan/Zbinden Andrea, Die Standards zur Aufhebung des Bankgeheimnisses, in: Susan Emmenegger (Hrsg.), Cross-Border Banking, Basel 2009, S. 193 ff.

Engert Andreas, Digitale Plattformen, AcP 2018, S. 304 ff.

Engi Lorenz/Hungerbühler Francis, E-Voting – Stand und Entwicklung in der Schweiz, medialex 2006, S. 17 ff.

Ennöckl Daniel, Kommentar zu Art. 2, 3, 4 Nr. 6 DSGVO, in: Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. Nomos-Kommentar Baden-Baden 2017 (zit. NomosKomm-DSGVO)

Epiney Astrid, Besonders schützenswerte Personendaten – Zu den Anforderungen an die Rechtmässigkeit der Bearbeitung durch öffentliche Organe im Fall des Fehlens einer gesetzlichen Grundlage, in: Rumo-Jungo Alexandra/Pichonnaz Pascal/Hürlimann-Kaup Bettina/Fountoulakis Christina (Hrsg.), Une empreinte sur le Code Civil – Mélanges en l'honneur de Paul-Henri Steinauer, Bern 2013, S. 97 ff.

Dies., Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?, Jusletter IT vom 21. Mai 2015

Dies., Zu ausgewählten Herausforderungen des Datenschutzrechts, in: Epiney Astrid/Theuerkauf Sarah (Hrsg.), Datenschutz in Europa und die Schweiz, Zürich/Basel/Genf 2006, S. 1 ff.

Epiney Astrid/Civitella Tamara/Zbinden Patricia, Datenschutzrecht in der Schweiz. Eine Einführung in das Datenschutzgesetz des Bundes mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Institut für Europarecht, Fribourg 2009

Epiney Astrid/Fasnacht Tobias, Zu den datenschutzrechtlichen Vorgaben für Errichtung und Betrieb von Informationssystemen. Unter besonderer Berücksichtigung der Bearbeitung besonders schützenswerter Personendaten und der Zugriffsberechtigung und am Beispiel des Klienten-Informationssystems für Sozialarbeit (KiSS), Jusletter vom 24. Februar 2014

Epiney Astrid/Fasnacht Tobias/Blaser Gaëtan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich/Basel/Genf 2013

Epiney Astrid/Hobi Patrick (Hrsg.), Die Revision des Datenschutzgesetzes/La révision de la loi sur la protection des données, Zürich 2009

Epiney Astrid/Hofstötter Bernhard/Meier Annekathrin/Theuerkauf Sarah, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen, Zürich 2007

Epiney Astrid/Theuerkauf Sarah (Hrsg.), Datenschutz in Europa und die Schweiz/La protection des données en Europe et la Suisse, Zürich/Basel/Genf 2006

Evans A.C., European Data Protection Law, Am. J. Comp. L. 1981, S. 571 ff.

F

Fankhauser Roland/Fischer Nadja, Kinderfotos auf Facebook oder wenn Eltern die Persönlichkeitsrechte ihrer Kinder verletzen, in: Fankhauser Roland/Reusser Ruth/Schwander Yvo (Hrsg.), Brennpunkt Familienrecht. Festschrift für Thomas Geiser, Dike Zürich/St. Gallen 2017, S. 193 ff.

Fasel Daniel, Fuzzy Data Warehousing for Performance Measurement: Concept and Implementation, Cham/Heidelberg 2014

Fasel Daniel/Meier Andreas (Hrsg.), Big Data – Grundlagen, Systeme und Nutzungspotenziale, Wiesbaden 2016

Fasel Daniel/Meier Andreas, Was versteht man unter Big Data und NoSQL?, in: Fasel Daniel/Meier Andreas (Hrsg.), Big Data – Grundlagen, Systeme und Nutzungspotenziale, Wiesbaden 2016, S. 3 ff.

Fasnacht Tobias, Die Einwilligung im Datenschutzrecht. Vorgaben einer völker- und verfassungsrechtlich konformen Ausgestaltung der datenschutzrechtlichen Einwilligung im schweizerischen Recht, Diss. Zürich/Basel/Genf 2017

Fateh-Moghadam Bijan, Selbstbestimmung im biotechnischen Zeitalter, BJM 2018, S. 205 ff.

Fellmann Walter, Anwaltsrecht, 2. Aufl., 2017

Fiedler Herbert, Datenschutz und Gesellschaft, in: Podlech Adalbert/Steinmüller Wolfgang (Hrsg.), Informationsrecht und Informationspolitik, München 1976, S. 179 ff.

Flaherty David H., Protecting Privacy in Surveillance Societies. The Federal Republic of Germany, Sweden, France, Canada, and the United States, North Carolina 1989

Flückiger Alexandre, L'autodétermination en matière de données personnelles : un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété ?, PJA 2013, S. 837 ff.

Flückiger Alexandre/Auer Andreas, La vidéosurveillance dans l'œil de la Constitution, AJP 2006, S. 924 ff.

Fontane Theodor, Effie Briest, Stuttgart 2019

Forkel Hans, Das Problem der vertraglichen Einräumung von Berechtigungen an Persönlichkeitsrechten, GRUR 1988, S. 491 ff.

Forstmoser Peter, Datenbanken und Persönlichkeitsschutz, SJZ 1974, S. 217 ff.

Ders., 10 Jahre Gesetz – 30 Jahre Diskussion. Von den Anfängen des Datenschutzes in der Schweiz, digma 2003, S. 50 ff.

Foucault Michel, Analytik der Macht, 6. Aufl., Frankfurt a. M. 2015

Ders., Überwachen und Strafen. Die Geburt des Gefängnisses, 15. Aufl., Frankfurt a. M. 2015

Fountoulakis Christiana, „Digital Natives" – Kinder, Smartphones und die KESB, in: Arnet Ruth/Eitel Paul/Jungo Alexandra/Künzle Hans Rainer (Hrsg.), Mensch als Mass. Festschrift für Peter Breitschmid, Zürich 2019, S. 145 ff.

Franke Gloria, The Right of Publicity vs. The First Amendment: Will One Test Ever Capture the Starring Role?, S. Cal. L. Rev. 2006, S. 958 ff.

Frei Nula, Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, Jusletter vom 17. September 2018

Freitag Andreas, Kommerzialisierung von Darbietungen des ausübenden Künstlers, Diss. Baden-Baden 1993

Fried Charles, Privacy, Yale L.J. 1968, S. 475 ff.

Friedman Lawrence M., Changing Times: Technology and Law in the Modern Era, in: Becker Jürgen/Hilty Reto M./Stöckli Jean-Fritz/Würtenberger Thomas (Hrsg.), Recht im Wandel seines sozialen und technologischen Umfeldes. Festschrift für Manfred Rehbinder, München 2002, S. 501 ff.

Fröhlich-Bleuler Gianni, Eigentum an Daten?, Jusletter vom 6. März 2017

Früh Alfred, Datenzuordnung und Datenzugang, digma 2019, S. 172 ff.

Funke Michael, Dogmatik und Voraussetzungen der datenschutzrechtlichen Einwilligung im Zivilrecht. Unter besonderer Berücksichtigung der Datenschutz-Grundverordnung, Diss. Baden-Baden 2017

Füller Jens Thomas, Eigenständiges Sachenrecht?, Habil. Tübingen 2006

G

Gabriel Kasper, People Analytics in privatrechtlichen Arbeitsverhältnissen: Vorschläge zur wirksameren Durchsetzung des Datenschutzrechts, Diss. St. Gallen 2021

Gallagher William T., Strategic Intellectual Property Litigation, the Right of Publicity, and the Attenuation of Free Speech. Lessons From the Schwarzenegger Bobblehead Doll War (and Peace), Santa Clara L. Rev. 2005, S. 581 ff.

Gallwas Hans Ulrich, Der allgemeine Konflikt zwischen dem Recht auf informationelle Selbstbestimmung und der Informationsfreiheit, NJW 1992, S. 2785 ff.

Gamper Lothar, Datenschutz – von Geheimhaltung, Geheimniskrämerei und Transparenz, Jusletter IT vom 22. Februar 2011

Gareis Karl, Die Privatrechtssphären im modernen Kulturstaate, insbesondere im Deutschen Reiche, Zeitschrift für Gesetzgebung und Praxis auf dem Gebiete des deutschen öffentlichen Rechtes 1877, S. 137 ff.

Garstka Hansjürgen, Das Selbstbestimmungsrecht und das Recht auf informationelle Selbstbestimmung, in: Götting Horst-Peter/Schertz Christian/Seitz Walter (Hrsg.), Handbuch des Persönlichkeitsrechts, München 2008, S. 392 ff.

Garstka Hansjürgen, Informationelle Selbstbestimmung und Datenschutz. Das Recht auf Privatsphäre, in: Schulzki-Haddouti Christiane (Hrsg.), Bürgerrechte im Netz, Wiesbaden 2003, S. 48 ff.

Gasser Urs, Kausalität und Zurechnung von Information als Rechtsproblem, Diss. München 2001

Gauch Peter, Der vernünftige Mensch. Ein Bild aus dem Obligationenrecht, in: Steinauer Paul-Henri (Hrsg.), Das Menschenbild im Recht. Festgabe der Rechtswissenschaftlichen Fakultät zur Hundertjahrfeier der Universität Freiburg, Freiburg 1990, S. 177 ff.

Gächter Thomas/Egli Philipp, Informationsaustausch im Umfeld der Sozialhilfe, Jusletter vom 6. September 2010

Gächter Thomas/Werder Gregori, Einbettung ausgewählter Konzepte in das schweizerische Datenschutzrecht, in: Epiney Astrid/Fasnacht Tobias/Blaser Gaëtan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich 2013, S. 87 ff.

Geiger Andreas, Die Einwilligung in die Verarbeitung von personenbezogenen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung, NVwZ 1979, S. 35 ff.

Geiser Thomas, Darf die Arbeitgeberin den Bewerber googlen?, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus u. a. (Hrsg.), Recht im digitalen Zeitalter. Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 373 ff.

Gerling Rainer W., Einwilligung und Datenweitergabe in der Forschung, DuD 2008, S. 733 ff.

Gesmann-Nuissl Dagmar, Rechtsprechungsreport «Innovations- und Technikrecht», InTeR 2018, 201 ff.

Geuss Raymond, Public Goods, Private Goods, Princeton Monographs in Philosophy, Bd. 22, Princeton 2009

Gierke Otto von, Deutsches Privatrecht, Bd. 1, Allgemeiner Teil und Personenrecht, Leipzig 1895

Giesen Thomas, Das Grundrecht auf Datenverarbeitung, JZ 2007, S. 918 ff.

Gilomen Hans-Jörg, Der Kleinkredit in mittelalterlichen Städten. Basel und Zürich im Vergleich, in: Holbach Rudolf/Pauly Michel (Hrsg.), Städtische Wirtschaft im Mittelalter. Festschrift für Franz Irsigler zum 70. Geburtstag, Köln/Weimar/Wien 2011, S. 109 ff.

Glass Philip, Die rechtsstaatliche Bearbeitung von Personendaten in der Schweiz. Regelungs- und Begründungsstrategien des Datenschutzrechts mit Hinweisen zu den Bereichen Polizei, Staatsschutz, Sozialhilfe und elektronische Informationsverarbeitung, Diss. Zürich/St. Gallen 2017

Glatthaar Matthias, Robot Recruiting, SZW 2020 S. 43 ff.

Ders., The Good, the Bad and the Ugly: Gedanken zum neuen Datenschutzgesetz, 16. März 2021, abrufbar unter: <https://datenrecht.ch/the-good-the-bad-and-the-ugly-gedanken-zum-neuen-datenschutzgesetz/>

Glaus Bruno, Das Recht am eigenen Wort. Informationelle Selbstbestimmung als Schranke der Medienfreiheit – mit allgemeinen Geschäftsbedingungen für das Mediengespräch, Diss. Bern 1997

Godt Christine, Eigentum an Information: Patentschutz und allgemeine Eigentumstheorie am Beispiel genetischer Information, Tübingen 2007

Gogniat Yves, Datenschutz in Spitälern, Jusletter vom 20. Juni 2016

Gonin Luc/Bigler Olivier, Commentaire du Art. 8 CEDH, Convention européenne des droits de l'homme (CEDH), Stämpflis Handkommentar, Bern 2018

Goodhart Arthur L., Restatement of the Law of Torts, Volume IV: A Comparison Between American and English Law, U. Pa. L. Rev. 1943, S. 487 ff.

Göpfert Burkard/Wilke Elena, Recherchen des Arbeitgebers in Sozialen Netzwerken nach dem geplanten Beschäftigtendatenschutzgesetz, NZA 2010, S. 1329 ff.

Götting Horst-Peter, Die Vererblichkeit der vermögenswerten Bestandteile des Persönlichkeitsrechts – ein Meilenstein in der Rechtsprechung des BGH, NJW 2001, S. 585 ff.

Ders., Persönlichkeitsrechte als Vermögensrechte, Tübingen 1995

Ders., Vom Right of Privacy zum Right of Publicity. Die Anerkennung eines Immaterialgüterrechts an der eigenen Persönlichkeit im amerikanischen Recht, GRUR Int. 1995, S. 656 ff.

Götting Horst-Peter/Schertz Christian/Seitz Walter, Handbuch des Persönlichkeitsrechts, München 2008

Götz Staehelin Claudia/Bertschi Manuel, Grenzen der Mitarbeiterüberwachung, RR-VR 2020 S. 5 ff.

Graber Christoph Beat/Teubner Gunther, Art and Money: Constitutional Rights in the Private Sphere?, Oxf. J. Leg. Stud. 1998, S. 61 ff.

Gregoritza Anna, Die Kommerzialisierung von Persönlichkeitsrechten Verstorbener, Diss. Berlin 2003

Greter Jean-Pierre, Die Akteneinsicht im schweizerischen Strafverfahren, Diss. Zürich 2012

Griesinger Marcel, Der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DSGVO, Jusletter vom 20. Januar 2020

Grimm Jacob und Wilhelm, Kinder- und Hausmärchen, 7. Aufl., Franz Duncker Verlag, Berlin 1857

Groebner Valentin, Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Mittelalter, München 2004

Ders., Nach der Megabit-Bombe: Wissenschaftliches Publizieren im Zeitalter des Internets, historisch gesehen, Mittelweg 36 2013, S. 29 ff.

Gruber Malte-Christian, Bioinformationsrecht. Zur Persönlichkeitsentfaltung des Menschen in technisierter Verfassung, Habil. Tübingen 2015

Grünberger Michael, Verträge über digitale Güter, AcP 2018, S. 213 ff.

Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Isabelle Wildhaber (Hrsg.), Recht im digitalen Zeitalter. Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015

Gugerli David, Suchmaschinen. Die Welt als Datenbank, Frankfurt a. M. 2009

Guntern Odilo, Erste Erfahrungen mit dem Datenschutzgesetz, in: Weber Rolf H./Thürer Daniel/Zäch Roger (Hrsg.), Datenschutz im europäischen Umfeld, Zürich 1995, S. 49 ff.

Gusy Christoph, Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, DuD 2009, S. 33 ff.

Günter Paul, Datenschutz im Gesundheitsbereich, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 151 ff.

Güntner Joachim, Privatsphäre. Schriftenreihe der Vontobelstiftung, Zürich 2011

H

Haas Raphaël, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Diss. Zürich 2007

Habermas Jürgen, Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft, Habil. Frankfurt a. M. 1990

Hagemeier Stefanie, Das Google WLAN-Scanning aus straf- und datenschutzrechtlicher Sicht, HRRS 2011, S. 72 ff.

Hannich Frank/Jenni Claudia/Beerli Beata/Mandl Teresa Valérie, Swiss CRM 2012. Einsatz und Trends in Schweizer Unternehmen. Von der Transaktion zur Beziehung. Crossing Borders, in: Zürcher Hochschule für Angewandte Wissenschaften (ZHAW), School of Management and Law, Zentrum für Marketing Management (Hrsg.), Winterthur 2012

Hansen Lene/Nissenbaum Helen, Digital Disaster, Cyber security, and the Copenhagen School, Int. Stud. Q. 2009, S. 1155 ff.

Hartung Jürgen, Kommentar zu Art. 24 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, München 2017 (zit. Beck-Komm.-DSGVO)

Harvey Michael G., Confidentiality: A Measured Response of the Failure of Privacy, U. Pa. L. Rev. 1992, S. 2385 ff.

Haslbauer Harald, Eigentum und Person. Begriff, Notwendigkeit und Folgen bürgerlicher Subjektivierung, Münster 2010

Hassemer Winfried, Prognosen zum Datenschutz, in: Simon Dieter/Weiss Manfred (Hrsg.), Zur Autonomie des Individuums. Liber Amicorum Spiros Simitis, Baden-Baden 2000, S. 121 ff.

Hauck Ernst, Wirtschaftsgeheimnisse – Informationseigentum kraft richterlicher Rechtsfortbildung?, Berlin 1987

Hauser Marc Thomas, Informationsbeschaffung als Rechtsproblem, Zürich 1978

Häusermann Daniel Markus, Vertraulichkeit als Schranke von Informationsansprüchen, Diss. Zürich/St. Gallen 2009

Heinzmann Peter/Bänziger Michael, Rechte für Fremde auf Ihrem Rechner?, digma 2001, S. 134 ff.

Heinz-Mohr Gerd/Sommer Volker, Die Rose. Entfaltung eines Symbols, Köln 1988

Helbing Thomas, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 2015, S. 145 ff.

Held Susann, Eigentum und Herrschaft bei John Locke und Immanuel Kant. Ein ideengeschichtlicher Vergleich, Berlin 2006

Helfrich Marcus, Kreditscoring und Scorewertbildung der SCHUFA. Datenschutzrechtliche Zulässigkeit im Rahmen der praktischen Anwendung, Diss. Baden-Baden 2010

Helle Jürgen, Besondere Persönlichkeitsrechte im Privatrecht. Das Recht am eigenen Bild, am gesprochenen Wort und der Schutz des geschriebenen Wortes, Tübingen 1991

Heller Lydia/Nuss Sabine, Open Source im Kapitalismus. Gute Idee – falsches System?, in: Gehring Robert A./Lutterbeck Bernd (Hrsg.), Open-Source-Jahrbuch 2004. Zwischen Softwareentwicklung und Gesellschaftsmodell, Berlin 2004, S. 385 ff.

Hellwege Phillip/Soniewicke Marta (Hrsg.), Die Einheit der Rechtsordnung, Tübingen 2020

Henke Ferdinand, Die Datenschutzkonvention des Europarates, Diss. Frankfurt a. M./Bern/New York 1986

Hensel Isabell/Teubner Gunther, Matrix Reloaded. Kritik der staatszentrierten Drittwirkung am Beispiel des Publication Bias, KritJ 2014, S. 150 ff.

Herbst Tobias, Kommentar zu Art. 5 DGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, München 2017 (zit. Beck-Komm.-DSGVO)

Herdes Daniela, Datenschutzrechtliche Herausforderungen beim Einsatz von KI im Bewerbungsverfahren, CB 2020, S. 95 ff.

Hermerschmidt Sven, Adresshandel durch die GEZ? Zur Befugnis der GEZ, Anschriften beim kommerziellen Adresshandel zu erheben, MMR 2005, S. 155 ff.

Herwig Jana/Tantner Anton, Zu den historischen Wurzeln der Kontrollgesellschaft, Wien 2014

Herzfeld Michael, The Social Production of Indifference. Exploring the Symbolic Roots of Western Bureaucracy, Chicago/London 1993

Hess-Odoni Urs, Die Herrschaftsrechte an Daten, Jusletter vom 17. Mai 2004

Heuberger Olivier, Profiling im Persönlichkeits- und Datenschutzrecht der Schweiz, Diss. Zürich/Luzern 2020

Hildebrandt Mireille/Gutwirth Serge (Hrsg.), Profiling the European Citizen. Cross-Disciplinary Perspectives, Belgien/Holland 2008

Hilty Reto M., Eine erste Analyse des Datenschutzrechts, NZZ vom 19. März 1994, S. 22

Ders., Rechtsfragen kommerzieller Nutzung von Daten, in: Weber Rolf H./Hilty Reto M. (Hrsg.), Daten und Datenbanken. Rechtsfragen zu Schutz und Nutzung, Zürich 1991, S. 81 ff.

Hirsch Célian/Jacot-Guillarmod Emilie, Les données bancaires pseudonymisées – Du secret bancaire à la protection des données, RSDA 2020, S. 151 ff.

Hoeren Thomas, Big data and the legal framework for data quality, Int. J. Law Inf. Technol. 2017, 26 ff.

Ders., «Das Pferd frisst keinen Gurkensalat!». Eine Einführung in das Informationsrecht, Paderborn 2008

Ders., Dateneigentum, MMR 2013, S. 486 ff.

Ders., Information als Gegenstand des Rechtsverkehrs. Prolegomena zu einer Theorie des Informationsrechts, MMR 1998, Beilage, S. 6 ff.

Ders., Internet- und Kommunikationsrecht, Köln 2008

Ders., Zu Datenschutz- und Werbeklauseln bei Kundenbindungssystemen. Anmerkungen zum BGH vom 16. Juli 2008, LMK 2008, S. 65 f.

Hofer Christian, § 16 Datenschutz im Handel mit Bonitätsdaten, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 557 ff.

Hoffmann-Riem Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 1998, S. 513 ff.

Hofmann Susanne/Meyer Michael Adrian, Datenschutz in der Schweiz, Expert Focus 2017, S. 422 ff.

Hohmann Harald (Hrsg.), Freiheitssicherung durch Datenschutz, Frankfurt a. M. 1987

Holbach Rudolf/Pauly Michel (Hrsg.), Städtische Wirtschaft im Mittelalter. Festschrift für Franz Irsigler zum 70. Geburtstag, Köln/Weimar/Wien 2011

Honsell Heinrich, Der Geheimnisschutz im Zivilrecht, in: Ruppe Hans Georg (Hrsg.), Geheimnisschutz im Wirtschaftsleben, Wien 1980, S. 45 ff.

Hoppe Tilman, Campbell v Mirror Ltd. – das «Modell»-Urteil zu Privacy?, ZUM 2005, S. 41 ff.

Ders., Privatleben in der Öffentlichkeit. Entscheidung des Europäischen Gerichtshofs für Menschenrechte vom 24. Juni 2004 mit Anmerkungen, ZEuP 2005, S. 656 ff.

Hotter Maximilian, Privatsphäre. Der Wandel eines liberalen Rechts im Zeitalter des Internets, Frankfurt a. M./New York 2011

Howe Daniel C./Nissenbaum Helen, TrackMeNot: Resisting Surveillance in Web Search, in: Kerr Ian/Steeves Valerie/Lucock Carole (ed.), Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society, Oxford 2009, S. 417 ff.

Hrubesch-Millauer Stephanie, Der Billigkeitsentscheid nach Art. 4 ZGB, ZBJV 2013, S. 469 ff.

Höning Nina, Das Recht am eigenen Bild und der Schutz prominenter Persönlichkeiten im deutschen und US-amerikanischen Recht, Diss. Hamburg 2012

Huber René, Kommentar zu Art. 27 DSG, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG)

Ders., Die Teilrevision des Eidg. Datenschutzgesetzes – ungenügende Pinselrenovation, recht 2006, S. 205 ff.

Hufen Friedhelm, Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbstbestimmung. Eine juristische Antwort auf „1984"?, JZ 1984, S. 1072 ff.

Hunter Rosemary/Cowan Sharon (ed.), Choice and Consent: Feminist Engagements with Law and Subjectivity, Oxford 2007

Hunziger Sven, Das Löschen im Datenschutzrecht, Frankfurt/Baden-Baden 2018

Husi-Stämpfli Sandra, Kinderrechte in der digitalen Welt, digma 2019, S. 84 ff.

Husi-Stämpfli Sandra/Gisler Katrin, Persönlichkeitsrechte und Archivierung: Alte und neue Herausforderungen, in: Epiney Astrid/Nüesch Daniela (Hrsg.), Big Data und Datenschutzrecht/Big Data et droit de la protection des données, Zürich 2016, S. 103 ff.

Hussein Noureddine, § 3 Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 98 ff.

Hürlimann Daniel, Publikationen von Urteilen durch Gerichte, sui generis 2014, S. 82 ff.

Hürlimann Daniel/Kettiger Daniel, Zugänglichkeit zu Urteilen kantonaler Gerichte. Ergebnisse einer Befragung, Justice – Justiz – Giustizia 2018

Hürlimann Daniel/Zech Herbert, Rechte an Daten, sui generis 2016, S. 98 ff.

Hürlimann-Kaup Bettina/Schmid Jörg, Einleitungsartikel und Personenrecht des ZGB, 3., ergänzte, verbesserte und nachgeführte Aufl., Zürich 2016

I

Inderkum Matthias, Schadenersatz, Genugtuung und Gewinnherausgabe aus Persönlichkeitsverletzung, Diss. Zürich 2008

J

Jakob Dominique, Kommentar zu Art. 60 ff. ZGB, in: Büchler Andrea/Jakob Dominique (Hrsg.), Kurzkommentar ZGB, 2. Aufl., Basel 2018 (zit. KuKo-ZGB)

Jandt Silke, Datenschutz durch Technik in der DS-GVO, DuD 2017, S. 562 ff.

Dies., Kommentar zu Art. 4 Nr. 11 und Art. 35 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, München 2017 (zit. Beck-Komm.-DSGVO)

Janger Edward J., Privacy Property, Information Costs, and the Anticommons, Hastings L.J. 2003, S. 899 ff.

Jänich Volker, Geistiges Eigentum – eine Komplementärerscheinung zum Sachenrecht?, Habil. Tübingen 2002

Jöhri Yvonne, § 8 Aufgabe und Bedeutung der öffentlichen Datenschutzbeauftragten, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 245 ff.

K

Kahler Thomas/Werner Stefan, Electronic Banking und Datenschutz. Rechtsfragen und Praxis, Berlin/Heidelberg 2008

Kalyvas James/Overly Michael (ed.), Big Data: A Business and Legal Guide, Boca Raton 2015

Kamlah Wulf, Das SCHUFA-Verfahren und seine datenschutzrechtliche Zulässigkeit, MMR 1999, S. 395 ff.

Kamp Meike/Rost Martin, Kritik an der Einwilligung. Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen, DuD 2013, S. 80 ff.

Kamp Meike/Weichert Thilo, Scoringsysteme zur Beurteilung der Kreditwürdigkeit. Chancen und Risiken für Verbraucher, Forschungsprojekt des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) Schleswig-Holstein 2006, abrufbar unter: <https://www.datenschutzzentrum.de/uploads/projekte/scoring/2005-studie-scoringsysteme-uld-bmvel.pdf>

Kang Jerry/Buchner Benedikt, Privacy in Atlantis, Harv. J.L. & Tech. 2004, S. 229 ff.

Karavas Vagias, Das Computer-Grundrecht. Persönlichkeitsschutz unter informationstechnischen Bedingungen. Neue Risiken, neue Rechte, WestEnd 2010, S. 95 ff.

Ders., Digitale Grundrechte. Elemente einer Verfassung des Informationsflusses im Internet, Diss. Frankfurt a. M. 2006 (zit. Digitale Grundrechte)

Ders., Körperverfassungsrecht. Entwurf eines inklusiven Biomedizinrechts, Habil. Zürich/St. Gallen 2018 (zit. Körperverfassungsrecht)

Karavas Vagias/Burri Mira/Gruber Malte-C., Rechtlicher Kontext und Regulierung, in: Lang Alexander/Gschmeidler Brigitte/Gruber Malte-C./Wuketich Milena/Kinz Elena/Karavas Vagias/Winkler Florian/Schumann Simone/Burri Nina/Griessler Erich, Neue Anwendungen der DNA-Analyse: Chancen und Risiken. Interdisziplinäre Technikfolgenabschätzung, v/d/f Hochschulverlag AG an der ETH Zürich, TA-SWISS 2020, S. 251 ff.

Karg Moritz, Der Wert personenbezogener Daten, digma 2011, S. 146 ff.

Kaufmann Christine/Ghielmini Sabrina/Medici Gabriela/Pulver Fanny, Das Recht auf Privatsphäre im digitalen Zeitalter. Staatliche Schutzpflichten bei Aktivitäten von Unternehmen, Bern 2016

Kähler Lorenz, Raum für Masslosigkeit. Zu den Grenzen des Verhältnismässigkeitsgrundsatzes im Privatecht, in: Jestaedt Matthias/Lepsius Oliver (Hrsg.), Verhältnismässigkeit, Tübingen 2015,
S. 210 ff.

Kälin Oliver, Der Sachbegriff im schweizerischen ZGB, Diss. Zürich 2002

Kehr Thomas/Zapp Benjamin, DSGVO – Ein erster Überblick aus der Bußgeldpraxis der Aufsichtsbehörden, CB 2020, S. 100 ff.

Keist Ramona, Gesichtserkennung im zivilrechtlichen Persönlichkeitsschutz, Jusletter vom 20. Mai 2019

Dies., Künstliche Intelligenz: Quo Vadis?, CB 2020, S. 89 ff.

Kilian Wolfgang, Personenbezogene Daten als schuldrechtliche Gegenleistung, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, DatenDebatten – Bd. 3, Berlin 2018, S. 191 ff.

Ders., Strukturwandel der Privatheit, in: Garstka Hansjürgen/Coy Wolfgang (Hrsg.), Wovon – für wen – wozu? Systemdenken wider die Diktatur der Daten. Wilhelm Steinmüller zum Gedächtnis, Berlin 2014, S. 195 ff.

Klar Manuel, Kommentar zu Art. 3 und Art. 4 Nr. 1 DSGVO, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung Kommentar, München 2017 (zit. Beck-Komm.-DSGVO)

Kleiner Beat, Datenschutz und Bankgeschäft, in: Brem Ernst/Druey Jean Nicolas/Kramer Ernst A./Schwander Ivo (Hrsg.), Festschrift für Mario M. Pedrazzini, Bern 1990, S. 397 ff.

Klippel Diethelm, Historische Wurzeln und Funktionen von Immaterialgüter- und Persönlichkeitsrechten im 19. Jahrhundert, ZNR 1982, S. 132 ff.

Klüber Rüdiger, Persönlichkeitsschutz und Kommerzialisierung, Tübingen 2007

Koch, Christian, Scoring-Systeme in der Kreditwirtschaft – Einsatz unter datenschutzrechtlichen Aspekten, MMR 1998, S. 458 ff.

Kohte Wolfhard, Die rechtfertigende Einwilligung, AcP 1985, S. 105 ff.

Kollmann Tobias/Tanasic Julia, Herausforderung Online-Marketing. Neue Marketinginstrumente zur verbesserten Kundenansprache durch Personalisierung und Individualisierung, digma 2012, S. 98 ff.

Koops Bert-Jaap, The Trouble with European Data Protection Law, Tilburg Law School Legal Studies Research Paper Series 2015

Köhntopp Marit/Köhntopp Kristian, Datenspuren im Internet, CR 2000, S. 248 ff.

Körner Marita, Informierte Einwilligung als Schutzkonzept, in: Simon Dieter/Weiss Manfred (Hrsg.), Zur Autonomie des Individuums. Liber Amicorum Spiros Simitis, Baden-Baden 2000, S. 131 ff.

Krajewski Markus, Ask Jeeves. Der Diener als Informationszentrale, in: Brandstetter Thomas/Hübel Thomas/Tantner Anton (Hrsg.), Vor Google. Eine Mediengeschichte der Suchmaschine im analogen Zeitalter, Wien 2012, 151 ff.

Ders., Der Diener. Mediengeschichte einer Figur zwischen König und Klient, Frankfurt a. M. 2010

Kramer Ernst A., Juristische Methodenlehre, 5. Aufl., Bern 2016

Krähnke Uwe, Selbstbestimmung. Zur gesellschaftlichen Konstruktion einer normativen Leitidee, Göttingen 2006

Kreis Georg, Staatsschutz im Laufe der Zeit von der Skandalisierung zur Gleichgültigkeit. Ein Blick zurück auf die Fichenaffäre vor zwanzig Jahren, digma 2009, S. 54 ff.

Kren Kostkiewicz Jolanta/Wolf Stephan/Amstutz Marc/Fankhauser Roland (Hrsg.), ZGB Kommentar. Schweizerisches Zivilgesetzbuch, 3. Aufl., Zürich 2016

Kresse Bernhard, Kommentar zu Art. 97 DSGVO, in: Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. Nomos-Kommentar Baden-Baden 2017 (zit. NomosKomm-DSGVO)

Krüger Jochen/Vogelgesang Stephanie/Weller Michael, Datenschutz für Minderjährige nach der Europäischen Datenschutz-Grundverordnung (DSGVO) vom 27. April 2016, Jusletter IT vom 23. Februar 2017

Kube Hanno, Die Zugänge der Informationsgesellschaft und der Gegenstandsbezug des Rechts, JZ 2001, S. 944 ff.

Kuhlen Rainer, Wem gehört die Information im 21. Jahrhundert? – eine Skizze, in: Büllesbach Alfred/Dreier Thomas (Hrsg.), Wem gehört die Information im 21. Jahrhundert? Proprietäre versus nicht proprietäre Verwertung digitaler Inhalte, Köln 2004, S. 1 ff.

Kuhn Moritz/Poledna Tomas (Hrsg.), Arztrecht in der Praxis, Zürich 2007

Kuonen Nicolas, La responsabilité précontractuelle, Diss. Fribourg 2007

Kurz Contanze/Rieger Frank, Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber verlieren, Frankfurt a. M. 2011

Kübler Daniel, SDF – Schriften zur Demokratieforschung Bd./Nr. 14, Medien und direkte Demokratie, Zürich 2018, S. 1 ff.

Kühne Roland, Schutz der Verschwiegenheit von Rechtsanwälten, Steuerberatern und Notaren vor strafprozessualen Ermittlungsmassnahmen, Diss. Baden-Baden 2013

Künzle Hans Rainer, Digitaler Nachlass nach schweizerischem Recht, successio 2015, S. 39 ff.

L

Ladeur Karl-Heinz, Das Medienrecht und die Ökonomie der Aufmerksamkeit. In Sachen Dieter Bohlen, Maxim Biller, Caroline von Monaco u. a., Köln 2007 (zit. Ökonomie der Aufmerksamkeit)

Ders., Kritik der Abwägung in der Grundrechtsdogmatik, Tübingen 2004 (zit. Kritik)

Ders., Schutz von Prominenz als Eigentum. Zur Kritik der Caroline-Rechtsprechung des Bundesverfassungsgerichts, ZUM 2000, S. 879 ff.

Landes Joan B. (ed.), Feminism, the Public and the Private, Oxford 1998

Lang Alexander/Gschmeidler Brigitte/Gruber Malte-C./Wuketich Milena/Kinz Elena/Karavas Vagias/Winkler Florian/Schumann Simone/Burri Nina/Griessler Erich, Neue Anwendungen der DNA-Analyse: Chancen und Risiken. Interdisziplinäre Technikfolgenabschätzung, v/d/f Hochschulverlag AG an der ETH Zürich, TA-SWISS 2020

Langer Margit, Informationsfreiheit als Grenze informationeller Selbstbestimmung – Verfassungsrechtliche Vorgaben der privatrechtlichen Informationsordnung. Schriften zum Recht des Informationsverkehrs und der Informationstechnik, Bd. 2, Berlin 1992

Langhanke Carmen, Daten als Leistung. Eine rechtsvergleichende Untersuchung zu Deutschland, Österreich und der Schweiz, Tübingen 2018

Langheinrich Marc/Karjoth Günter, Eine Balance zwischen Nutzen und Schutz. Wie Internetnutzer sich der Beobachtung durch Werbetreibende entziehen können, digma 2012, S. 116 ff.

Laux Christian, Das Recht auf Datenportabilität, digma 2019, S. 166 ff.

Leebron David W., The Right to Privacy's Place in the Intellectual History of Tort Law, Case W. Res. L. Rev. 1991, S. 769 ff.

Lehmann Beat/Sauter Regine M., Datensicherung und Haftung aus Bearbeitungs- und Sicherungsfehlern, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 135 ff.

Lessig Lawrence, Code. Version 2.0, New York 2006

Ders., Privacy as Property, Soc. Res. 2002, S. 247 ff.

Leusser Wolfgang/Hippner Hajo/Wilde Klaus D., CRM – Grundlagen, Konzepte und Prozesse, in: Hippner Hajo/Hubrich Beate/Wilde Klaus D. (Hrsg.), Grundlagen des CRM. Strategie, Geschäftsprozesse und IT-Unterstützung, 3. Aufl., Wiesbaden 2011, S. 16 ff.

Lévy Vanessa, Le droit à l'image, Diss. Zürich 2002

Liedke Bernd, Die Einwilligung im Datenschutzrecht, Edewecht 2012

Lindner Eric, Die datenschutzrechtliche Einwilligung nach §§ 4 Abs. 1, 4a BDSG – ein zukunftsfähiges Institut? Hamburg 2013

Linoff Gordon S./Berry Michael J. A., Data Mining Techniques for Marketing, Sales, and Customer Support, 3rd ed., New York 2011

Litman Jessica, Information Privacy/Information Property, Stan. L. Rev. 2000, S. 1283 ff.

Loch Karen D./Conger Sue/Oz Effy, Ownership, Privacy and Monitoring in the Workplace. A Debate on Technology and Ethics, J. Bus. Ethics 1998, S. 653 ff.

London Economics (Hrsg.), Study on the economic benefits of privacy-enhancing technologies, London 2010, abrufbar unter: <https://londoneconomics.co.uk/wp-content/uploads/2011/09/17-Study-on-the-economic-benefits-of-privacy-enhancing-technologies-PETs.pdf>

Luhmann Niklas, Macht im System, 1. Aufl., Berlin 2013 (zit. Macht)

Ders., Soziale Systeme. Grundriss einer allgemeinen Theorie, 16. Aufl., Frankfurt a. M. 2015 (zit. Systeme)

Ders., Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität, 5. Aufl., Konstanz/München 2014 (zit. Vertrauen)

Lüthy Ellen, Zivilrechtliche Probleme der identifizierenden Berichterstattung am Beispiel der Presse, Diss. Zürich 1981

Lynskey Orla, The Foundations of EU Data Protection Law, Oxford 2015

M

Magnus Robert, Das Anwaltsprivileg und sein zivilprozessualer Schutz. Eine rechtsvergleichende Analyse des deutschen, französischen und englischen Rechts, Tübingen 2010

Maisch Michael Marc, Informationelle Selbstbestimmung in Netzwerken: Rechtsrahmen, Gefährdungslagen und Schutzkonzepte am Beispiel von Cloud Computing und Facebook, Diss. Berlin 2015

Mallmann Otto, Zielfunktionen des Datenschutzes. Schutz der Privatsphäre – korrekte Information, Frankfurt a. M. 1977

Mantz Reto, Kommentar zu Art. 32 DSGVO, in: Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. Nomos-Kommentar Baden-Baden 2017 (zit. NomosKomm-DSGVO)

Marsch Nikolaus, Das Europäische Datenschutzgrundrecht. Grundlagen – Dimensionen – Verflechtungen, Tübingen 2018

Martin Kirsten/Nissenbaum Helen, Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables, Colum. Sci. & Tech. L. Rev., Forthcoming

Mattern Friedemann, Acht Thesen zur Informatisierung des Alltags, in: Mattern Friedemann (Hrsg.), Die Informatisierung des Alltags. Leben in smarten Umgebungen, Berlin 2007, S. 11 ff.

Mattern Friedemann (Hrsg.), Die Informatisierung des Alltags. Leben in smarten Umgebungen, Berlin 2007

Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG)

Maurer-Lambrou Urs/Kunz Simon, Kommentar zu Art. 1 und Art. 2 DSG, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG)

Mayer-Schönberger Viktor, Delete. Die Tugend des Vergessens in digitalen Zeiten, Berlin 2010 (zit. Delete)

Ders., Demystifying Lessig, Wis. L. Rev. 2008, S. 713 ff.

Ders., In Search of the Story: Narratives of Intellectual Property, Va. J.L. & Tech. 2005, S. 1 ff.

Ders., Information und Recht. Vom Datenschutz bis zum Urheberrecht, Wien 2001 (zit. Information und Recht)

Ders., Informationsrecht als Gestaltungsaufgabe: Eine transatlantische Gestaltungsaufgabe, in: Schweizer Rainer J./Burkert Herbert/Gasser Urs (Hrsg.), Festschrift für Jean Nicolas Druey, Zürich 2002, S. 853 ff.

Ders., On the Future of Law in the Information Society, in: Gerfried Stocker/Christine Schöpf (Hrsg.), Goodbye Privacy, Ostfildern 2007, S. 102 ff. (Deutsche Version: Mayer-Schönberger Viktor, Recht im Wandel – Zur Zukunft des Rechts in der Informationsgesellschaft, in: Gerfried Stocker/Christine Schöpf (Hrsg.), Goodbye Privacy, Ostfildern 2007, S. 108 ff.)

Mayer-Schönberger Viktor/Cukier Kenneth, Big Data. A Revolution That Will Transform How We Live, Work and Think, London 2013

McCarthy J. Thomas, The Human Persona as Commercial Property: The Right of Publicity, Colum.-VLA J.L. & Arts 1995, S. 124 ff.

Meier Andreas, Datamanagement mit SQL und NoSQL, in: Meier Andreas/Fasel Daniel (Hrsg.), HMD 2014, S. 17 ff.

Meier Konrad, Bankaufsichtsrechtliche Relevanz des Datenschutzgesetzes, in: Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 1 ff.

Meier Philippe, A l'impossible nul n'est tenu ... sauf Google ?, medialex 2011, S. 69 f.

Ders., Protection des données. Fondements, principes généraux et droit privé, Bern 2011

Ders., 5ème révision de l'AI et détection précoce : que reste-t-il de la protection des données et du secret médical ?, in : Kahil-Wolff Bettina/Simonin Emmanuelle, La 5ème révision de l'AI, Bern 2009, 87 ff.

Meier-Schatz Christian J./Schweizer Rainer J. (Hrsg.), Recht und Internationalisierung, Zürich 2000

Meister Herbert, Datenschutz und Datensicherheit, DuD 1986, S. 173 ff.

Métille Sylvain, Jurisprudence actuelle en matière des données : Surveillance, infiltration et transmission de données à un tiers : quelques atteintes à la sphère privée qui ont occupée récemment les tribunaux, in : Epiney Astrid/Fasnacht Tobias/Blaser Gaëtan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung, Zürich 2013, S. 113 ff.

Meyer Caroline B., Privatrechtliche Persönlichkeitsrechte im kommerziellen Rechtsverkehr, Diss. Basel 2008 (zit. Meyer Caroline B.)

Meyer Roland, Operative Portraits. Eine Bildgeschichte der Identifizierbarkeit von Lavater bis Facebook, Konstanz 2019 (zit. Meyer Roland)

Meyer Sebastian, Datenschutz in Zeiten von Universal Analytics, Jusletter IT vom 25. Februar 2016

Michel Margot, Kommentar zu Art. 270 ff. ZGB, in: Büchler Andrea/Jakob Dominique (Hrsg.), Kurzkommentar ZGB, 2. Aufl., Basel 2018 (zit. KuKo-ZGB)

Michlig Matthias, Bankgeheimnisverletzung (Art. 47 BankG) unter dem Aspekt der Lieferung von Personendaten ans U.S. Department of Justice, AJP 2014, S. 1055 ff.

Miller Arthur Raphael, Der Einbruch in die Privatsphäre, Darmstadt 1973

Moore Adam D., Privacy Rights. Moral and Legal Foundations, Pennsylvania 2010

Morgan Richard/Boardman Ruth, Data Protection Strategy. Implementing Data Protection Compliance, 2. Ed., London 2012

Morscher Lukas, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, ZBJV 2011, S. 177 ff.

Moskalenko Kateryna, The right of publicity in the USA, the EU, and Ukraine, IJC 2015, S. 113 ff.

Möller Jan/Florax Björn-Christoph, Kreditwirtschaft Scoring-Verfahren. Datenschutzrechtliche Unbedenklichkeit des Scoring von Kreditrisiken?, MMR 2002, S. 806 ff.

Murphy Richard S., Property Rights in Personal Information. An Economic Defence of Privacy, Geo. L.J. 1996, S. 2381 ff.

Müller Christoph, Obligationenrecht. Allgemeine Bestimmungen: Art. 1–18 OR mit allgemeiner Einleitung in das Schweizerische Obligationenrecht, Berner Kommentar, Bern 2018 (zit. BK-OR)

Müller Georg, Mantelgesetze und Einheit der Materie, LeGes 2013, S. 507 ff.

Müller Lucien, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung von Straftaten, Zürich/St. Gallen 2011

N

Nadakavukaren Schefer Krista, Ein völkerrechtlicher Schutz der kollektiven Privatsphäre? Der Schutz der Privatsphäre und die Anonymität im Zeitalter kommerzieller Drohnen, ZSR 2014, S. 259 ff.

Nagenborg Michael/El-Faddagh Mahha, Genetische Informationen: Eigentumsansprüche und Verfügbarkeit, IRIE 2006, S. 40 ff.

Nassehi Armin, Muster. Theorie der digitalen Gesellschaft, München 2019

Nebel Maxi, Big Data und Datenschutz in der Arbeitswelt. Risiken der Digitalisierung und Abhilfemöglichkeiten, ZD 2018, S. 520 ff.

Neupert Michael, Rechtmäßigkeit und Zweckmäßigkeit. Das Rahmen-Bild-Modell der verwaltungsgerichtlichen Kontrolldichte bei der Eingriffsverwaltung, Diss. Tübingen 2011

Niemann Fabian/Scholz Philip, Privacy by Design und Privacy by Default – Wege zu einem funktionierenden Datenschutz in Sozialen Netzwerken, in: Peters Falk/Kersten Heinrich/Wolfenstetter Klaus-Dieter (Hrsg.), Innovativer Datenschutz, Berlin 2012, S. 109 ff.

Nissenbaum Helen, A Contextual Approach to Privacy Online, Dædalus 2011, S. 32 ff.

Dies., From Preemption to Circumvention. If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?, Berkeley Tech. L.J. 2011, S. 1367 ff.

Dies., Privacy in Context. Technology, Policy, and the Integrity of Social Life, Stanford 2010

Dies., Privatsphäre im Kontext. Technologie, Politik und die Unversehrtheit des Sozialen, in: Heinrich-Böll-Stiftung (Hrsg.), #public_life. Digitale Intimität, die Privatsphäre und das Netz, Berlin 2011, S. 53 ff.

Dies., Respecting Context to Protect Privacy. Why Meaning Matters, Sci. Eng. Ethics 2018, S. 831 ff.

Nobel Peter, Entwicklungen im Bank- und Kapitalmarktrecht/Le point sur le droit bancaire et des marchés des capitaux, SJZ 2018, S. 14 ff.

O

Oberholzer Niklaus, Datenschutz und Polizei, in: Brem Ernst/Druey Jean Nicolas/Kramer Ernst A./Schwander Ivo (Hrsg.), Festschrift für Mario M. Pedrazzini, Bern 1990, S. 427 ff.

Odlyzko Andrew, Privacy, Economics, and Price Discrimination on the Internet, CEC'03, Proceedings of the 5th International Conference on Electronic Commerce, Pittsburgh/Pennsylvania 2003, S. 355 ff.

Ders., The Volume and Value of Information, Int. J. Commun. 2012, S. 920 ff.

Ohly Ansgar, «Volenti non fit inuiria». Die Einwilligung im Privatrecht, Habil. Tübingen 2002

Opel Andrea, Lieferung von Bankmitarbeiterdaten an ausländische Steuerbehörden – wenn Amtshilfe ausartet, in: Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 77 ff.

Oppliger Damien, La carte de crédit – Étude droit suisse, ex/ante 2020, S. 32 ff.

Ortner Sherry B., Is Female to Male as Nature is to Culture?, in: Landes Joan B. (ed.), Feminism, the Public and the Private, Oxford 1998, S. 21 ff.

P

Paefgen Franziska, Der von Art. 8 EMRK gewährleistete Schutz vor staatlichen Eingriffen in die Persönlichkeitsrechte im Internet, Diss. Berlin 2017

Page Gérald, Le droit d'accès et de contestation dans le traitement des données personnelles : étude de base en droit privé suisse et américain, Diss. Zürich 1983

Papa Roberta/Pietruszak Thomas, § 17 Datenschutz im Personalwesen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 577 ff.

Passadelis Nicolas, § 6 Rechtsanwendung bei internationaler Datenbearbeitung durch Private, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 167 ff.

Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015

Passadelis Nicolas/Roth Simon, Weisser Rauch über Brüssel. Was Schweizer Unternehmen über die europäische Datenschutz-Grundverordnung wissen müssen, Jusletter vom 4. April 2016

Pärli Kurt, Datenaustausch zwischen Arbeitgeber und Versicherung. Probleme der Bearbeitung von Gesundheitsdaten bei der Begründung des privatrechtlichen Arbeitsverhältnisses, Diss. Bern 2003

Ders., Das Kreuz mit der Selbstverantwortung, SZS 2018, S. 107 ff.

Ders., Datenschutz durch Selbstregulierung?, digma 2011, S. 66 ff.

Ders., Die Bearbeitung von Arbeitnehmerpersonendaten durch den Arbeitgeber im Interesse von Sozial- und Privatversicherungen, in: Riemer-Kafka Gabriela (Hrsg.)., Sozialversicherung: Von der Wiege bis zur Bahre, Zürich/Luzern 2016, S. 52 ff.

Ders., Die EGMR-Rechtsprechung zum Schutz der Privatsphäre und vor Überwachung am Arbeitsplatz, EuZA 2020, S. 224 ff.

Ders., Observation von Arbeitnehmern/-innen durch die Arbeitgeberin, HAVE 2018, S. 228 ff.

Ders., Observation von Versicherten – Der Gesetzgeber auf Abwegen, recht 2018, 120 ff.

Ders., Schutz der Privatsphäre am Arbeitsplatz in digitalen Zeiten – eine menschenrechtliche Herausforderung, EuZA 2015, S. 48 ff.

Pedrazzini Mario M., Der Ausbau des Datenschutzes, in: Kaufmann Otto K./Koller Arnold/Riklin Alois (Hrsg.), Zur Zukunft von Staat und Wirtschaft in der Schweiz. Festschrift für Kurt Furgler, Zürich/Köln 1984, S. 316 ff.

Ders., Der Rechtsschutz der betroffenen Personen gegenüber privaten Bearbeitern. Klagen, vorsorgliche Massnahmen, Gerichtsstand, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 81 ff.

Ders., Die Grundlagen der schweizerischen Datenschutzgesetzgebung, Wirtschaft und Recht 1982, S. 27 ff.

Ders., Die Grundlagen des Datenschutzes im Privatbereich: die Grundzüge und der Geltungsbereich des Bundesgesetzes, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 19 ff.

Peter James Thomas, Das Datenschutzgesetz im Privatbereich: Unter besonderer Berücksichtigung seiner motivationalen Grundlage, Diss. Zürich 1994

Peters Falk/Kersten Heinrich/Wolfenstetter Klaus-Dieter (Hrsg.), Innovativer Datenschutz, Berlin 2012

Petri Thomas, Compliance und Datenschutz, Jusletter IT vom 1. September 2010

Ders., Das Scoringverfahren der SCHUFA, DuD 2001, S. 290 ff.

Peukert Alexander, «Sonstige Gegenstände» im Rechtsverkehr, in: Leible Stefan/Lehmann Stefan/Zech Herbert (Hrsg.), Unkörperliche Güter im Privatrecht, Tübingen 2011, S. 99 ff.

Ders., Güterzuordnung als Rechtsprinzip, Habil. Tübingen 2007

Pfaffinger Monika, DSGVO, Extraterritoriale Wirkung und konkrete Pflichten für die Banken, in: Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 17 ff.

Dies., Geheime und offene Formen der Adoption. Wirkungen von Information und Kontakt auf das Gleichgewicht im Adoptionsdreieck, Diss. Zürich 2008

Dies., Kommentar zu Art. 1 ff. und Art. 264 ff. ZGB, in: Büchler Andrea/Dominique Jakob (Hrsg.), Kurzkommentar ZGB, 2. Aufl., Basel 2018 (zit. KuKo-ZGB)

Dies., Polyvalentes Kindeswohl – methodische Reflexionen über das Wohl des (adoptierten) Kindes, ZSR 2011, S. 417 ff.

Dies., The Past Future of Adoption: The Impact of Biotechnologies on an Old Institution, Ancilla Iuris (anci.ch) 2016, S. 49 ff., abrufbar unter: <https://www.anci.ch/articles/ancilla2016_49_pfaffinger.pdf>

Dies., Vaterschaft auf dem Prüfstand. Das Recht des Ehemannes auf Kenntnis der eigenen Vaterschaft im Zeitalter der Genetik, FamPra.ch 2014, S. 604 ff.

Pfaffinger Monika/Balkanyi-Nordmann Nadine, Mit dem Datenschutz gilt es nun ernst, Private – Das Geld-Magazin 2019, S. 22 f.

Dies., Neues Datenschutzrecht. Europa macht Ernst mit Datenschutz, Schweizer Bank Mai 2018, S. 21 f.

Dies., Die Compliance-Organisation im digitalen Zeitalter, RR-CO 2019, S. 2 ff.

Pfeifer Karl-Nikolaus, Eigenheit oder Eigentum – was schützt das Persönlichkeitsrecht?, GRUR 2002, S. 495 ff.

Ders., Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, JZ 2012, S. 851 ff.

Pfeil Werner, Der Mensch steht höher als Technik und Maschine – Benötigen wir ein Grundrecht zum Schutz vor Künstlicher Intelligenz?, InTeR 2020, S. 82 ff.

Pisà Maria, Die Herausforderung der Datenlöschung meistern, RR-COMP 2019, S. 8 ff.

Placzek Thomas, Allgemeines Persönlichkeitsrecht und privatrechtlicher Informations- und Datenschutz. Eine schutzgutbezogene Untersuchung des Rechts auf informationelle Selbstbestimmung, Diss. Münster 2006

Pohle Jörg, Datenschutz und Technikgestaltung. Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, Diss. Berlin 2017

Porter Theodore M., Trust in Numbers. The Pursuit of Objectivity in Science and Public Life, Princeton 1995

Posner Richard A., Economic Analysis of Law, 7. Ed., Austin/Boston/Chicago a.o. 2007

Post Robert Charles, Rereading Warren & Brandeis: Privacy, Property, and Appropriation, Case W. Res. L. Rev. 1991, S. 647 ff.

Prieur Yvonne, Datenschutz durch «Big-Data-Geschäfte» auf dem Prüfstand, AJP 2015, S. 1643 ff.

Dies., § 13 Datenschutz im Sozialversicherungskontext, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 431 ff.

Probst Thomas, Die unbestimmte „Bestimmbarkeit" der von Daten betroffenen Person im Datenschutzrecht. Personendaten und anonymisierte Einzeldaten in der globalisierten Informationsgesellschaft – Quo vaditis?, AJP 2013, S. 1423 ff.

Ders., Digitalisierung und Vertragsrecht – Probleme des Schutzes der Privatsphäre aus vertragsrechtlicher Sicht, in: Epiney Astrid/Sangsue Déborah (Hrsg.), Digitalisierung und Schutz der Privatsphäre, Forum Europarecht Bd./Nr. 39, Zürich 2018, S. 41 ff.

Prosser William L., Privacy, Calif. L. Rev. 1960, S. 383 ff.

R

Radlanski Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Diss. Tübingen 2016

Rampini Corrado, Kommentar zu Art. 13 DSG, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BK-DSG)

Raschauer Nicolas, Kommentar zu Art. 24 und Art. 42 DSGVO, in: Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. Nomos-Kommentar Baden-Baden 2017 (zit. NomosKomm-DSGVO)

Räther Philipp, Die Anwendung der neuen EU-Datenschutz-Grundverordnung im Unternehmen, ZHR 2019, S. 94 ff.

Räuchle Christine, Online-Profiling. Die Erhebung und Nutzung personenbezogener Profile im Internet unter datenschutzrechtlichen Gesichtspunkten des internationalen, europäischen und deutschen Rechts, Diss. Tübingen 2006

Reber Martina, Privacy by Design & Privacy by Default – Relevanz für die Banken, in: Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 41 ff.

Rechsteiner Stefan/Steiner Thomas, Datenschutz bei intelligenten Mess- und Steuersystemen, Jusletter vom 11. Juni 2018

Regan P. M., Legislating Privacy, Technology, Social Values and Public Policy, Chapel Hill/London 1995

Reichman Jerome H./Samuelson Pamela, Intellectual Property Rights in Data, Vand. L. Rev. 1997, S. 52 ff.

Reimer Philipp, Kommentar zu Art. 5 DSGVO, in: Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. Nomos-Kommentar, Baden-Baden 2017 (zit. NomosKomm-DSGVO)

Rey Heinz, Die Grundlagen des Sachenrechts und das Eigentum, 3., ergänzte und überarbeitete Aufl., Bern 2007

Richards Neil M., The Puzzle of Brandeis, Privacy, and Speech, Vand. L. Rev. 2010, S. 1295 ff.

Richter Ingo, Die Digitalisierung des Alltags, in: Mehde Veith/Ramsauer Ulrich/Seckelmann Margrit (Hrsg.), Staat, Verwaltung, Information. Festschrift für Hans Peter Bull, Berlin 2011, S. 1041 ff.

Riemer Hans Michael, Die Einleitungsartikel des Schweizerischen Zivilgesetzbuches. Art. 1–10 ZGB. Eine Einführung, 2. Aufl., Bern 2003

Ders., Persönlichkeitsrechte und Persönlichkeitsschutz gemäss Art. 28 ff. ZGB im Verhältnis zum Datenschutz-, Immaterialgüter- und Wettbewerbsrecht, sic! 1999, S. 103 ff.

Rifkin Jeremy, Access. Das Verschwinden des Eigentums. Warum wir weniger besitzen und mehr ausgeben werden, Frankfurt a. M./New York 2000 (zit. Access)

Ders., Der Europäische Traum. Die Vision einer leisen Supermacht, Frankfurt a. M. 2004 (zit. Traum)

Ritter Martina, Die Dynamik der Privatheit und Öffentlichkeit in modernen Gesellschaften, Wiesbaden 2008

Rogosch Patricia Maria, Die Einwilligung im Datenschutzrecht, Baden-Baden 2013

Rohn Patrick, Zivilrechtliche Verantwortlichkeit der Internet Provider nach schweizerischem Recht, Diss. Zürich 2004

Rosa Hartmut, Unverfügbarkeit, 3. Aufl., Salzburg 2019

Rossnagel Alexander/Pfitzmann Andreas/Garstka Hansjürgen, in: Bundesministerium des Inneren (Hrsg.), Gutachten zur Modernisierung des Datenschutzrechts, Berlin 2001

Ronellenfitsch Michael/Denfeld Bastian, Die Vereinbarkeit von Zugangskontrollen für gewerbliche Spielstätten mit dem Grundrecht auf informationelle Selbstbestimmung, Hamburg 2009

Rosch Daniel/Wider Diana (Hrsg.), Zwischen Schutz und Selbstbestimmung. Festschrift für Christoph Häfeli zum 70. Geburtstag, Bern 2013

Rosenthal David, Das Bauchgefühl im Datenschutz, in: Datenschutz-forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing: 20 Jahre Datenschutz in der Schweiz, Zürich 2012, S. 69 ff.

Ders., Das neue Datenschutzgesetz, Jusletter vom 16. November 2020

Ders., Der Entwurf für ein neues Datenschutzgesetz. Was uns erwartet und was noch zu korrigieren ist, Jusletter vom 27. November 2017

Ders., Kommentar zu Art. 3, Art. 4, Art. 12 und Art. 13 DSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar DSG, Zürich 2008 (zit. HK-DSG)

Ders., Löschen und doch nicht löschen, digma 2019, S. 190 ff.

Ders., Wie sich Privatpersonen gegen die Verletzungen ihrer Persönlichkeitsrechte durch Dritte auf Social-Media-Plattformen wehren können, Anwaltsrevue 2014, S. 415 ff.

Ders., § 7 Sanktionierungen von Datenschutzverstössen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, 203 ff.

Rosenthal, David/Epprecht Barbara, Banken und ihre datenschutzrechtliche Verantwortlichkeit im Verkehr mit ihren Dienstleistern, in: Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 127 ff.

Rosenthal David/Gubler Seraina, Die Strafbestimmungen des neuen DSG, SZW 2021, S. 52 ff.

Rosenthal David/Jöhri Yvonne, Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, Zürich/Basel/Genf 2008 (zit. HK-DSG)

Rosenthal David/Vasella David, Erste Erfahrungen mit der DSGVO, digma 2018, S. 166 ff.

Rossnagel Alexander, Modernisierung des Datenschutzes, digma 2011, S. 160 ff.

Roth Gregor, Das einheitliche Recht auf Information. Ein Beitrag zur Institutionenbildung, Diss. Köln/Berlin/München 2006

Rössler Beate, Den Wert des Privaten ergründen – Philosophische Überlegungen zum Verhältnis zwischen Autonomie und Privatheit, digma 2002, S. 106 ff.

Dies., Der Wert des Privaten, Diss. Frankfurt a. M. 2001

Dies., What is there to lose? Privacy in offline and online friendships, Eurozine vom 27. Februar 2015, abrufbar unter: <https://www.eurozine.com/what-is-there-to-lose/>

Röthel Anne, Die Konkretisierung von Generalklauseln, in: Riesenhuber Karl (Hrsg.), Europäische Methodenlehre. Grundfragen der Methoden des Europäischen Privatrechts, 3. Aufl., Berlin 2015, S. 225 ff.

Röösli Martin, Gesundheitsgefährdungsabschätzung: Auswirkungen von nichtionisierender Strahlung auf den Menschen, URP 2021, S. 117 ff.

Ruch Alexander (Hrsg.), Recht und neue Technologien, Berlin/Zürich 2004

Rudin Beat, Datenschutzgesetze – wie weiter?, digma 2001, S. 126 ff.

Ders., Der neue Datenhunger der Verwaltung. Hält das Datenschutzkonzept den Herausforderungen stand?, BJM 1998, S. 113 ff.

Ders., Die Erosion der informationellen Privatheit – oder: Rechtsetzung als Risiko, in: Sutter-Somm Thomas/Hafner Felix/Schmid Gerhard/Seelmann Kurt (Hrsg.), Risiko und Recht. Festgabe zum schweizerischen Juristentag 2004, Basel/Genf/München/Bern 2004, S. 415 ff.

Ders., Erfolg – und Geld zurück. Vom «Return on Investment» von Datenschutz- und Informationssicherheitsmassnahmen, digma 2003, S. 4 f.

Ders., Facebook, Twitter & Co. am Arbeitsplatz. Soziale Netzwerke – Traum aller Marketingfachleute oder Albtraum für die Sicherheitsverantwortlichen?, digma 2010, S. 48 f.

Ders., Pay as you drive und Persönlichkeitsschutz. Neue Modelle der Mobilitätsversicherung und -besteuerung. Technische Möglichkeiten und rechtliche Grenzen, digma 2007, S. 88 f.

Ders., Scoring: Den Kunden «berechnen». Wenn das Individuum statistisch bewertet wird. Ausgewählte datenschutzrechtliche Aspekte des Kredit-Scorings, digma 2007, S. 50 ff.

Ders., Sperrrecht gegen Publikation im Auto-Index (Wiedergabe und Kommentierung des Urteils Nr. 15/01 der Eidgenössischen Datenschutzkommission vom 22. Mai 2003), digma 2004, S. 32 ff.

Ders., Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, SJZ 2009, S. 1 ff.

Ders., Videoüberwachung, Aufbewahrungsfrist (Kommentierung von BGE 133 I 77), digma 2007, S. 34 ff.

Ruegg Jean/Flückiger Alexandre/November Valérie/Klauser Francisco, Vidéosurveillance et risques dans l'espace à usage public : Représentations des risques, régulation sociale et liberté de mouvement, Genf 2006

Rule James/Hunter Lawrence, Towards Property Rights in Personal Data, in: Bennet Colin J./Grant Rebecca (ed.), Visions of Privacy. Policy Choices for the Digital Age, Toronto 1999, S. 168 ff.

Rusch Arnold/Kummer Miriam, Unfreiwilliges Outing Homosexueller, AJP 2015, S. 916 ff.

S

Sachs Ulrich, Marketing, Datenschutz und das Internet, Diss. Köln/München 2008

Samuelson Pamela, Privacy As Intellectual Property?, Stan. L. Rev. 2000, S. 1125 ff.

Sandri Sandra, Har-pa-chered (Harpokrates): Die Genese eines ägyptischen Götterkindes, Orientalia Lovaniensia Analecta, Bd. 151, Leuven/Paris/Dudley 2006

Sattler Andreas, Der Einfluss der Digitalisierung auf das Gesellschaftsrecht, BB 2018, S. 2243 ff.

Ders., Personenbezogene Daten als Leistungsgegenstand, SJZ 2017, S. 1036 ff.

Schaar Peter, Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft, München 2007

Schachtner Christina/Duller Nicole, Praktiken des Managements von Privatheit und Öffentlichkeit im Cyberspace. Performative Akte im Kontext des Zeigens und Nicht-Zeigens, ÖZS 2014, Sonderheft, S. 61 ff.

Schaffhauser René/Brunner Stephan C. (Hrsg.), Datenschutz im Gesundheits- und Versicherungswesen. Referate der Tagung vom 27. September 2007, St. Gallen 2008

Schäfer Marc-Frédéric, Über die Rechtfertigung von Persönlichkeitsverletzungen, medialex 2011, S. 142 ff.

Schefer Markus, Grundrechte in der Schweiz, Bern 2005

Scheja, Gregor, Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank. Eine Untersuchung unter besonderer Berücksichtigung der §§ 4b, 4c BDSG, Diss. Baden-Baden 2006

Schermer Bart W./Custers Bart/van der Hof Simone, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, Ethics Inf. Technol. 2014, S. 171 ff.

Schiedermair Stephanie, Der Schutz des Privaten als internationales Grundrecht, Habil. Tübingen 2012

Schindler Benjamin, Justizöffentlichkeit im digitalen Zeitalter, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus u. a. (Hrsg.), Recht im digitalen Zeitalter. Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 741 ff.

Schineis Michael, Marketing und Datenschutz. Probleme, Lösungsansätze, empirische Ergebnisse, Diss. Augsburg 1989

Schluep Walter R./Lüchinger Adolf, Über Sinn und Funktionen des Anwaltsgeheimnisses im Rechtsstaat, Zürich 1994

Schmid Alan/Schmidt Kirsten Johanna/Zech Herbert, Rechte an Daten – zum Stand der Diskussion, sic! 2018, S. 627 ff.

Schmid Jörg, KMU und Datenschutz: Der heikle Umgang mit Personendaten. Luzerner Beiträge zur Rechtswissenschaft, in: Schmid Jörg/Girsberger Daniel (Hrsg.), Rechtsfragen rund um die KMU, Zürich 2003, S. 151 ff.

Ders., Persönlichkeitsschutz bei der Bearbeitung von Personendaten durch Private, ZBJV 1995, S. 809 ff.

Schmidt Kirsten Johanna, Datenmärkte ohne «Dateneigentum», digma 2019, S. 178 ff.

Schmidt Walter, Die bedrohte Entscheidungsfreiheit, JZ 1974, S. 241 ff.

Schmitt Patrick, Adoption und Diffusion neuer Technologien am Beispiel der Radiofrequenz-Identifikation (RFID), Diss. Zürich 2008

Schnabl Wolfgang, Datenschutz und Informationssicherheit – ein natürlicher Gegensatz?, Jusletter IT vom 24. Mai 2018

Schoemann Ferdinand D. (ed.), Philosophical Dimensions of Privacy: An Anthology, Cambridge 1984

Schrepfer Thomas W., Datenschutz und Verfassung. Eine Untersuchung zur verfassungsrechtlichen Relevanz der Erfassung, Aufbewahrung und Weitergabe personenbezogener Daten, Diss. Bern/Frankfurt a. M./New York 1985

Schröder Annika Sophie, Best Practice im Data Mapping, digma 2020, S. 16 ff.

Schuler-Harms Margarete, Die kommerzielle Nutzung statistischer Persönlichkeitsprofile als Herausforderung für den Datenschutz, in: Sokol Bettina (Hrsg.), Living by Numbers. Leben zwischen Statistik und Wirklichkeit, Düsseldorf 2005, S. 5 ff.

Schunck Elia, Propertisierung von Personendaten?, digma 2013, S. 66 ff.

Schuppli Roman, Private Sicherheitsdienste im Spannungsfeld von Gewaltmonopol und Grundrechten, Sicherheit & Recht 2019, S. 49 ff.

Schwartz Paul M., Beyond Lessig's Code for Internet Privacy. Cyberspace Filters, Privacy-Control, and Fair Information Practices, Wis. L. Rev. 2000, S. 743 ff.

Ders., Property, Privacy, and Personal Data, Harv. L. Rev. 2004, S. 2055 ff.

Schwendenwein Hugo, Das neue Kirchenrecht, Graz/Wien/Köln 1983

Schweighofer Erich, Die neue EU-Datenschutz-Grundverordnung. Entstehung und Überblick, Jusletter IT vom 9. Februar 2016

Schweizer Alex, Customer Relationship Management, Diss. Bern u. a. 2007 (zit. CRM)

Ders., Data Mining, Data Warehousing: Datenschutzrechtliche Orientierungshilfen für Privatunternehmen, Zürich 1999 (zit. Data Warehousing)

Ders., Die Aufsicht über die privaten Datenbearbeitungen und die Beschwerdemöglichkeiten privater Bearbeiter und betroffener Personen gegen Aufsichtsentscheide, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 91 ff.

Ders., Die Informatik fordert das Recht heraus – Vermittlung des gesellschaftlichen und ökonomischen Wertes des informationellen Schutzes, digma 2003, S. 58 ff.

Ders., Falsche Personendaten und Analyseergebnisse. Die Bedeutung des Grundsatzes der Datenrichtigkeit wird in der Zukunft stark zunehmen, digma 2007, S. 64 ff.

Ders., Grundsatzfragen des Datenschutzes, Habil. Basel 1986

Ders., Kommentar zu Art. 10 und Art. 13 Abs. 2 BV, in: Ehrenzeller Bernhard/Schweizer Rainer/Schindler Benjamin/Vallander Klaus (Hrsg.), Die schweizerische Bundesverfassung. St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014

Ders., Privacy. Selbstbestimmung in der transparenten Gesellschaft, in: Schweizer Rainer J./Burkert Herbert/Gasser Urs (Hrsg.), Festschrift für Jean Nicolas Druey, Zürich 2002, S. 907 ff.

Ders., § 1 Geschichte und Zukunft des Datenschutzrechts, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 6 ff.

Schwenke Matthias Christoph, Individualisierung und Datenschutz: Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Individualisierung, Wiesbaden 2006

Schwenzer Ingeborg, Familie und Recht. Ausgewählte Beiträge aus 25 Jahren, Bern 2010

Dies., Familienrecht und gesellschaftliche Veränderungen. Gutachten zum Postulat 12.3607 Fehr 'Zeitgemässes kohärentes Zivilinsbesondere Familienrecht', FamPra.ch 2014, S. 966 ff.

Seemann Bruno, Prominenz als Eigentum. Parallele Rechtsentwicklungen einer Vermarktung der Persönlichkeit im amerikanischen, deutschen und schweizerischen Privatrecht, Diss. Baden-Baden 1996

Seethaler Frank, Entstehungsgeschichte des Datenschutzgesetzes, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG), 3 ff.

Seischab Lisa, Wettbewerbsrechtliche und datenschutzrechtliche Grundsatzfragen von Kundenbindungssystemen. Interdisziplinäre Zusammenhänge unter Einbeziehung ökonomischer Ansätze, Diss. Hamburg/Frankfurt a. M. 2009

Simitis Spiros, Datenschutz. Verteidigung der Privatsphäre, in: Schlemmer Johannes (Hrsg.), Der Verlust der Intimität, München 1976, S. 67 ff.

Ders., Datenschutz – Voraussetzung oder Ende der Kommunikation?, in: Horn Norbert/Luig Klaus/Söllner Alfred (Hrsg.), Europäisches Rechtsdenken in Geschichte und Gegenwart: Festschrift für Helmut Coing, München 1982, Bd. 2, S. 495 ff.

Ders., Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S. 394 ff.

Ders., Einleitung: Geschichte – Ziele – Prinzipien, in: Simitis Spiros (Hrsg.), Bundesdatenschutzgesetz. NomosKommentar, 8. Aufl., Baden-Baden 2014 (zit. NomosKomm-BDSG), S. 81 ff.

Ders., Hat der Datenschutz eine Zukunft? Symposium on Privacy and Security, ETH ZH, 15.–16. September 2004 (zit. Symposium)

Ders., Informationskrise des Rechts und Datenverarbeitung, Karlsruhe 1970

Ders., Kommentar zu §§ 1 und 4a BDSG, in: Simitis Spiros (Hrsg.), Bundesdatenschutzgesetz, NomosKommentar, 8. Aufl., Baden-Baden. 2014

Ders., Privacy – An Endless Debate?, Calif. L. Rev. 2010, S. 1989 ff.

Ders., «Sensitive Daten». Zur Geschichte und Wirkung einer Fiktion, in: Brem Ernst/Druey Jean Nicolas/Kramer Ernst A./Schwander Ivo (Hrsg.), Festschrift für Mario M. Pedrazzini, Bern 1990, S. 469 ff.

Simon Dieter/Weiss Manfred (Hrsg.), Zur Autonomie des Individuums. Liber Amicorum Spiros Simitis, Baden-Baden 2000

Solove Daniel J., Privacy and Power. Computer Databases and Metaphors for Information Privacy, Stan. L. Rev. 2001, S. 1393 ff.

Söbbing Thomas, Der Datenskandal bei Facebook und die rechtliche Zulässigkeit von künstlicher Intelligenz (KI) zur Beeinflussung der politischen Willensbildung (sog. Microtargeting), InTeR 2018, S. 182 ff.

Specht Louisa, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen. Eine Erläuterung des gegenwärtigen Meinungsstandes und Gedanken für eine zukünftige Ausgestaltung, CR 2016, S. 288 ff.

Dies., Konsequenzen der Ökonomisierung informationeller Selbstbestimmung. Die zivilrechtliche Erfassung des Datenhandels, Diss. Köln 2011

Specht Louisa/Rohmer Rebecca, Zur Rolle des informationellen Selbstbestimmungsrechts bei der Ausgestaltung eines möglichen Ausschließlichkeitsrechts an Daten, PinG 2016, abrufbar unter: <https://www.pingdigital.de/PinG.04.2016.127>

Spiecker genannt Döhmann Indra, Datenschutzrecht in der EU: Aktuelle Herausforderungen unter besonderer Berücksichtigung der Datenschutz-Grundverordnung, in: Epiney Astrid/Sangsue Déborah (Hrsg.), Digitalisierung und Schutz der Privatsphäre/L'ère numérique et la protection de la sphère privée, Zürich 2018, S. 1 ff.

Stamm-Pfister Christa, Kommentar zu Art. 7 DSG, in: Maurer-Lambrou Urs/Blechta Gabor (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014 (zit. BSK-DSG)

Stämpfli Sandra, Das Schengener Informationssystem und das Recht der informationellen Selbstbestimmung, Diss. Bern 2009

Steinauer Paul-Henri, Die Verletzung durch private Datenbearbeitung und die allfällige Rechtfertigung einer Verletzung. Einzelheiten der gesetzlichen Regelung, in: Schweizer Rainer J. (Hrsg.), Das neue Datenschutzgesetz des Bundes. Referate der Tagungen der Hochschule St. Gallen vom 15. Oktober und 13. November 1992, Zürich 1993, S. 43 ff.

Ders., Le droit d'accès, in : Universités de Berne, Fribourg, Genève, Lausanne et Neuchâtel (Hrsg.), Informatique et protection de la Personnalité, Fribourg 1981, S. 79 ff.

Ders., Le Titre préliminaire du Code civil, in: Schweizerisches Privatrecht, II/1, Basel 2009

Steinke Hubert, Der Hippokratische Eid: ein schwieriges Erbe, SAEZ 2016, S. 1699 ff.

Strasser Othmar, Datenschutz und Bankgeschäft am Beispiel der Bonitätsprüfung bei Krediten, SJZ 1997, S. 449 ff.

Studer Evelyne/de Werra Jacques, Regulating Cybersecurity, Expert Focus 2017, S. 511 ff.

Sunil Soares, The Chief Data Officer Handbook for Data Governance, Boise 2014

Sury Ursula, Neues Datenschutzgesetz und Dokumentation von Unternehmen, SJZ 2021, S. 458 ff.

Suter Stefan, Das Berufs- und Beichtgeheimnis kirchlicher Seelsorger, Art. 321 StGB und CIC, Zürich/St. Gallen 2009

Sutter Patrick (Hrsg.), Selbstbestimmung und Recht. Festschrift für Rainer J. Schweizer zum 60. Geburtstag, Zürich 2003

Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. Nomos-Kommentar Baden-Baden 2017 (zit. NomosKomm-DSGVO)

Ders., (Hrsg.), Kirchliches Datenschutzrecht. Datenschutzbestimmungen der katholischen Kirche. Handkommentar. Nomos-Kommentar Baden-Baden 2020

T

Tantner Anton, Die ersten Suchmaschinen. Adressbüros, Fragämter, Intelligenz-Comptoirs, Berlin 2015 (zit.: Suchmaschinen)

Ders., Ordnung der Häuser, Beschreibung der Seelen. Hausnummerierung und Seelenkonskription in der Habsburgermonarchie, Diss. Innsbruck 2007 (zit.: Ordnung der Häuser)

Taupitz Jochen (Hrsg.), Kommerzialisierung des menschlichen Körpers, Berlin/Heidelberg 2007

Teubner Gunther, Die anonyme Matrix: Zu Menschenrechtsverletzungen durch „private" transnationale Akteure, Der Staat 2006, S. 161 ff.

Ders., Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten, AcP 2018, S. 155 ff.

Ders., Expertise als soziale Institution. Die Internalisierung Dritter in den Vertrag, in: Brüggemeier Gert (Hrsg.), Festschrift für Eike Schmidt, Heidelberg 2005, S. 303 ff.

Ders., Ein Fall von struktureller Korruption? Die Familienbürgschaft in der Kollision unverträglicher Handlungslogiken (BVerfGE 89, 214 ff.), KritV 2000, S. 388 ff.

Ders., Standards und Direktiven in Generalklauseln. Möglichkeiten und Grenzen der empirischen Sozialforschung bei der Präzisierung der Gute-Sitten-Klauseln im Privatrecht, Diss. Frankfurt a. M. 1971

Thouvenin Florent, Datenschutz auf der Intensivstation, digma 2019, S. 206 ff.

Ders., Wem gehören meine Daten? Von Sinn und Nutzen der Erweiterung des Eigentumsbegriffs, SJZ 2017, S. 21 ff.

Thouvenin Florent/Früh Alfred/Lombard Alexandre, Eigentum an Sachdaten: Eine Standortbestimmung, SZW 2017, S. 25 ff.

Tiefenthal Jürg Marcel, Kommentar zu Art. 21 Ausweispflicht, in: Tiefenthal Jürg Marcel (Hrsg.), Kantonale Polizeihoheit. Eine systematische Darstellung des kantonalen Polizeirechts anhand des Schaffhauser Polizeigesetzes, Zürich/Basel/Genf 2016, S. 391 ff.

Tinnefeld Marie-Theres/Buchner Benedikt/Petri Thomas, Einführung in das Datenschutzrecht. Datenschutz und Informationssicherheit in europäischer Sicht, 5. Aufl., München 2012

Toubiana Vincent/Narayana Arvind/Boneh Dan/Nissenbaum Helen/Barocas Solon, Adnostic: Privacy Preserving Targeted Advertising, Proceedings Network and Distributed System Symposium, März 2010, abrufbar unter: <https://crypto.stanford.edu/adnostic/adnostic-ndss.pdf>

Toubiana Vincent/Nissenbaum Helen, An Analysis of Google Logs Retention Policies, J. Priv. Confid. 2011, S. 3 ff.

Trosch Daniel, Grenzen einer Kommerzialisierung von Informationen des öffentlichen Sektors, Baden-Baden 2008

Tuor Peter/Schnyder Bernhard/Schmid Jörg/Jungo Alexandra, ZGB. Das Schweizerische Zivilgesetzbuch, 14. Aufl., Zürich 2015

Turkington Richard, Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, N. Ill. U. L. Rev. 1990, S. 479 ff.

U

Ullmann Eike, Persönlichkeitsrechte in Lizenz?, AfP 1999, S. 209 ff.

Unseld Florian, Die Kommerzialisierung personenbezogener Daten, Diss. München 2010

Uttinger Ursula, § 10 Datenschutz im Gesundheitswesen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 427 ff.

V

van Spyk Benedikt, Das Recht der Selbstbestimmung in der Humanforschung. Zugleich eine Untersuchung der Grundlagen und Grenzen des «informed consent» im Handlungsbereich der Forschung am Menschen, Zürich/St. Gallen 2011

Vasella David, Profiling nach der DSGVO und dem E-DSG bei Banken, in: Emmenegger Susan (Hrsg.), Banken und Datenschutz, Basel 2019, S. 189 ff.

Ders., Zum Anwendungsbereich der DSGVO, digma 2017, S. 220 ff.

Ders., Zur Freiwilligkeit und Ausdrücklichkeit der Einwilligung im Datenschutzrecht, Jusletter vom 16. November 2015

Vasella David/Sievers Jaqueline, Der «Swiss Finish» im Vorentwurf des DSG, digma 2017, S. 44 ff.

Vasella David/Ziegler Noémi, Krankenversicherung und DSG-Revision, digma 2019, S. 80 ff.

Vec Miloš, Die Spur des Täters. Methoden der Identifikation in der Kriminalistik (1879–1933), Baden-Baden 2002

Vesting Thomas, Das Internet und die Notwendigkeit der Transformation des Datenschutzes, in: Karl Heinz Ladeur (Hrsg.), Innovationsoffene Regulierung des Internet, Baden-Baden 2003,
S. 155 ff.

Ders., 1. Teil. Grundlagen des Persönlichkeitsrechts, 2. Teil. Verfassungsrechtlicher Persönlichkeitsschutz, 3. Kapitel. Einführung, § 6 Verfassungsgeschichtliche und verfassungsdogmatische Grundlagen, in: Götting Horst-Peter/Schertz Christian/Seitz Walter (Hrsg.), Handbuch des Persönlichkeitsrechts, München 2008, S. 101 ff.

Vischer Daniel, Zwanzig Jahre Datenschutz: Staatsschutz und Datenschutz, in: Datenschutz-Forum Schweiz (Hrsg.), Von der Lochkarte zum Mobile Computing: 20 Jahre Datenschutz in der Schweiz, Zürich 2012, S. 109 ff.

Vismann Cornelia, Das Recht und seine Mittel. Ausgewählte Schriften, Krajewski Markus/Steinhauer Markus (Hrsg.), Frankfurt a. M. 2012

Vogt Hans-Ueli/Wiget Lukas, Aktuelle Fragen des Photorechts: Urheberrecht, Recht am eigenen Bild und Gegendarstellungsrecht, in: Arter Oliver/Jörg Florian S. (Hrsg.), Entertainment Law, Bern 2006, S. 129 ff.

Vokinger Kerstin Noëlle, Die digitale Bekämpfung von Covid-19 und die Rolle des Bundes(rates), SJZ 2020, S. 412 ff.

von Arnauld, Andreas, Zur Rhetorik der Verhältnismässigkeit, in: Jestaedt Matthias/Lepsius Oliver (Hrsg.), Verhältnismässigkeit, Tübingen, 2015, S. 276 ff.

von Lewinski Kai, Europäisierung des Datenschutzrechts. Umsetzungsspielraum des deutschen Gesetzgebers und Entscheidungskompetenz des BVerfG, DuD 2012, S. 564 ff.

Ders., Geschichte des Datenschutzrechts von 1900–1997, in: Arndt Felix/Augsberg Steffen (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit. 48. Assistententagung Öffentliches Recht, Heidelberg 2008, Baden-Baden 2009, S. 196 ff.

Ders., Kodifikationsstrategien im Datenschutzrecht, oder: Wann ist der Zeitpunkt der Unkodifizierbarkeit erreicht?, in: Kloepfer Michael (Hrsg.), Gesetzgebung als wissenschaftliche Herausforderung. Gedächtnisschrift Thilo Brandner, Baden-Baden 2011, S. 107 ff.

von Reden Armgard, Unternehmensweiter Datenschutz. Die Bedeutung von Privacy und der Aufbau von Vertrauen in Kundenbeziehungen am Beispiel der IBM, digma 2001, S. 124 f.

W

Wagner Alexander, Armenfürsorge in (Rechts-)Theorie und Rechtsordnungen der frühen Neuzeit, in: Schmidt Sebastian/Aspelmeier Jens (Hrsg.), Norm und Praxis der Armenfürsorge in Spätmittelalter und früher Neuzeit, Stuttgart 2006, S. 21 ff.

Waidner Michael/Karjoth Günter, Ist Anonymität praktisch realisierbar? Technische Überlegungen zu Möglichkeiten und Grenzen anonymisierter Transaktionen im Internet, digma 2004, S. 18 ff.

Walder Wyss AG (Isler Michael/Kunz Oliver M./Müller Thomas/Schneider Jürg/Vasella David), Zulässigkeit der Bekanntgabe von Bankkundendaten durch schweizerische Banken an Beauftragte im Ausland unter Art. 47 BankG

Waldmeier Stefanie-Daniela, Informationelle Selbstbestimmung – ein Grundrecht im Wandel?, Diss. Zürich 2015

Walzer Michael, Sphären der Gerechtigkeit. Ein Plädoyer für Pluralität und Gleichheit, Frankfurt a. M. 2006

Warren Samuel/Brandeis Louis, The Right to Privacy, Harv. L. Rev. 1890, S. 193 ff.

Wächter Michael, Falsifikation und Fortschritt im Datenschutz. Qualitätsmanagement und Haftung im privaten Datenschutzrecht, Diss. Berlin 2000

Weber Rolf H., Ali Baba oder das Risiko exklusiver Informationsinhaltsrechte, in: Schweizer Rainer J./Burkert Herbert/Gasser Urs (Hrsg.), Festschrift für Jean Nicolas Druey, Zürich 2002, S. 1009 ff.

Ders., Automatisierte Entscheidungen: Perspektive Grundrechte, SZW 2020, S. 18 ff.

Ders., EU-Datenschutz-Grundverordnung: Kernelemente und Ausstrahlungswirkung auf die Schweiz, Jusletter IT vom 24. September 2015

Ders., Geldentschädigung als Rechtsfolge von Persönlichkeitsverletzungen?, medialex 2000, S. 75 ff.

Ders., Kassandra oder Wissensbroker – Dilemma im «Global Village», in: Becker Jürgen/Hilty Reto M./Stöckli Jean-Fritz/Würtenberger Thomas (Hrsg.), Recht im Wandel seines sozialen und technologischen Umfeldes. Festschrift für Manfred Rehbinder, München 2002, S. 405 ff.

Ders., Online-Marketing und Datenschutz. Die Privatheit ist durch neue elektronische Werbeformen gefährdet, digma 2012, S. 110 ff.

Ders., Persönlichkeit als Immaterialgut?, in: Honsell Heinrich/Zäch Roger/Hasenböhler Franz/Harrer Friedrich/Rhinow René (Hrsg.), Privatrecht und Methode. Festschrift für Ernst A. Kramer, Basel 2004, S. 411 ff.

Weber Rolf H./Heinrich Ulrike I., Existiert ein Recht auf Anonymität im Internet?, ZSR 2013, S. 477 ff.

Weber Rolf H./Henseler Simon, Daten als Entgelt, SZW 2019, S. 335 ff.

Weber Rolf H./Hilty Reto (Hrsg.), Daten und Datenbanken. Rechtsfragen zu Schutz und Nutzung, Zürich 1999

Weber Rolf H./Staiger Dominic N., Vertragsgestaltung rund um Big Data, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, S. 151 ff.

Weber Rolf H./Thouvenin Florent, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 2018, S. 43 ff.

Weber Rolf H./Thürer Daniel/Zäch Roger (Hrsg.), Datenschutz im europäischen Umfeld, Zürich 1995

Wech Petra, Das Bankgeheimnis. Struktur, Inhalt und Grenzen einer zivilrechtlichen Schutzpflicht, Berlin 2008

Weichert Thilo, Datenschutzrechtliche Anforderungen an Verbraucher-Kredit-Scoring, DuD 2005, S. 582 ff.

Ders., Datenschutzrechtliche Probleme beim Adresshandel, wrp 1996, S. 522 ff.

Ders., Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, in: Bäumler Helmut (Hrsg.), E-Privacy. Datenschutz im Internet, Braunschweig/Wiesbaden 2000, S. 158 ff.

Ders., Kundenbindungssysteme – Verbraucherschutz oder der gläserne Konsument?, DuD 2003, S. 161 ff.

Ders., Scoring – die gesetzliche Erlaubnis zur wissenschaftlichen Diskriminierung von Verbrauchern, ver.di 2008, S. 12 ff.

Ders., Wem gehören die privaten Daten?, in: Taeger Jürgen/Wiebe Andreas (Hrsg.), Informatik – Wirtschaft – Recht: Regulierung in der Wissensgesellschaft, Baden-Baden 2004, S. 281 ff.

Welsing Ruth, Das Recht auf informationelle Selbstbestimmung im Rahmen der Terrorabwehr. Darstellung anhand einer Untersuchung der präventiven Rasterfahndung, Hamburg 2009

Wenhold Celine, Nutzerprofilbildung durch Webtracking: Zugleich eine Untersuchung zu den Defiziten des Datenschutzrechts im Zeitalter von Big Data-Anwendungen, Frankfurt a. M. 2018

Wente Jürgen, Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte, NJW 1984, S. 1446

Wermelinger Amédéo, Google Street View: On the road again?, digma 2012, S. 134 ff.

Wermelinger Amédéo/Schweri Daniel, Teilrevision des Eidgenössischen Datenschutzrechts. Es nützt nicht viel, schadet es etwas?, Jusletter vom 3. März 2008

Wersig Maria, Der unsichtbare Mehrwert: Unbezahlte Arbeit und ihr Lohn, in: Foljanty Lena/Lembke Ulrike (Hrsg.), Feministische Rechtswissenschaft. Ein Studienbuch, 2. Aufl., Baden-Baden 2012, S. 173 ff.

Wespi Andreas, Big Data: Technische Aspekte, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, S. 3 ff.

Westin Alan f., The origins of modern claims of privacy, in: Schoemann Ferdinand D. (ed.), Philosophical Dimensions of Privacy: An Anthology, Cambridge 1984, S. 56 ff.

Westkamp Guido, Privacy & Publicity. Schutz und Kommerzialisierung der Persönlichkeit im modernen britischen Common Law, Diss. Baden-Baden 2011

Weydner-Volkmann Sebastian/Feiten Linus, Vertrauensstiftende Videoüberwachung?, digma 2019, S. 218 ff.

Widmer Barbara, Der lange Weg der digitalen Grundbuchzugriffe: Die Aufsicht über die Plattform Terravis, AJP 2020, S. 30 ff.

Widmer Michael, § 4 Informations- und Meldepflichten bei der Bearbeitung von Personendaten und § 5 Rechte der Datensubjekte, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 121 ff. und S. 149 ff.

Wiegand Wolfgang, Numerus Clausus der dinglichen Rechte. Zur Entstehung und Bedeutung eines zentralen zivilrechtlichen Dogmas, in: Becker Hans-Jürgen/Brauneder Wilhelm/Caroni Pio u. a. (Hrsg.), Wege europäischer Rechtsgeschichte. Rechtsgeschichtliche Reihe, Bd. 60. Festschrift für Karl Kroeschell, Frankfurt a. M./Bern/New York/Paris 1987, S. 623 ff.

Wielsch Dan, Zugangsregeln. Die Rechtsverfassung der Wissensteilung, Habil. Tübingen 2008

Wildhaber Isabelle, Genetische und medizinische Informationen in der Arbeitswelt, Jusletter vom 6. Dezember 2010

Wildhaber, Isabelle/Lohmann, Melinda Florina/Kasper, Gabriel, Diskriminierung durch Algorithmen – Überlegungen zum schweizerischen Recht am Beispiel prädiktiver Analytik am Arbeitsplatz, ZSR 2019, S. 459 ff.

Wilhelm Rudolf (Hrsg.), Information – Technik – Recht. Rechtsgüterschutz in der Informationsgesellschaft, Darmstadt 1983

Woolf Virginia, A Room of One's Own, Wordsworth Classics (ed.), London 2012

Wu Tim, Blind Spot. The Attention Economy and the Law, Antitrust L.J. 2017, S. 34 ff.

Wuermeling Ulrich, Scoring von Kreditrisiken, NJW 2002, S. 3508

Z

Zech Herbert, Information als Schutzgegenstand, Habil. Tübingen 2012

Ders., Unkörperliche Güter im Zivilrecht – Einführung und Überblick, in: Leible Stefan/Lehmann Stefan/Zech Herbert (Hrsg.), Unkörperliche Güter im Privatrecht, Tübingen 2011, S. 1 ff.

Ziebarth Wolfgang, Kommentar zu Art. 4 A, B, Art. 4 Nr. 1, 3, 5, 10, 16–19, 21–23, Art. 31, 51–55, 57–59 DSGVO, in: Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar. Nomos-Kommentar Baden-Baden 2017 (zit. NomosKomm-DSGVO)

Ziegler Noémi/Vasella David, Informationelle Selbstbestimmung, digma 2019, S. 158 ff.

Zittel Niggi, § 12 Datenschutz in der Privatversicherung, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht. Beraten in Privatwirtschaft und öffentlicher Verwaltung. Handbücher für die Anwaltspraxis, Basel 2015, S. 427 ff.

Zulauf Rena/Sieber Maja, Die Person der Zeitgeschichte: Entstauben oder entsorgen?, medialex 2017, S. 20 ff.

Zulauf Rena/Sieber Maja, Social Media als privatsphärenfreier Raum? Das Konzept der Vorder- und Hinterbühne im Medienrecht, AJP 2017, S. 548 ff.

Verzeichnis der wichtigsten Materialien

Bayerisches Landesamt für Datenschutzaufsicht (BLD), FAQ zur DS-GVO, Auftragsverarbeitung, Abgrenzung, Stand 20. Juli 2018, abrufbar unter: <https://www.lda.bayern. de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf> (zit. BLD, FAQ Auftragsverarbeitung), S. 1 ff.

Bundesrat, Bericht über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, S. 335 ff. (zit. BR, Schlussbericht Evaluation 2011–1952)

Bundesrat, Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988 II S. 414 ff. (zit. BBl 1988 II 414 ff.)

Bundesrat, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017–1084, S. 6941 ff. (zit. BBl 2017–1084, 17.059)

Bundesrat, Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003, BBl 2002–2527, S. 2101 ff. (zit. BBl 2003)

Bundesamt für Justiz, Änderung von Art. 12 Abs. 2 lit. a DSG: Auslegungshilfe vom 10. Oktober 2006

Commission Nationale de l'Informatique et des Libertés (CNIL), Règlement européen sur la protection des données personnelles, Guide du sous-traitant, Stand September 2017, abrufbar unter: <https://www.cnil.fr/fr/reglement-europeen-sur-la-protectiondes-donnees-un-guide-pour-accompagner-les-sous-traitants> (zit. CNIL, Guide sous-traitant).

Eidgenössisches Finanzdepartement (EFD), Bericht der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit vom 17. August 2018, abrufbar unter: <https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-72083.html>, (zit. EFD, Bericht 2018)

Eidgenössisches Justiz- und Polizeidepartement (EJPD), Bundesamt für Justiz (BJ), Direktionsbereich Öffentliches Recht, Fachbereich Rechtsetzungsprojekte und -methodik (Hrsg.), Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, Bern 21. Dezember 2016, S. 1 ff. (zit. EJPD, Erläuternder Bericht)

Eidgenössisches Justiz- und Polizeidepartement (EJPD), Bundesamt für Justiz (BJ), Direktionsbereich Öffentliches Recht, Fachbereich Rechtsetzungsprojekte und -methodik (Hrsg.), Normkonzept zur Revision des Datenschutzgesetzes. Bericht der Begleitgruppe Revision DSG, Bern 29. Oktober 2014 (zit. EJPD, Bericht Begleitgruppe)

Eidgenössisches Justiz- und Polizeidepartement (EJPD), Bundesamt für Justiz (BJ), Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz. Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens, Bern 10. August 2017 (zit. EJPD, Zusammenfassung)

Eidgenössischer Öffentlichkeits- und Datenschutzbeauftragter (EDÖB), Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, Stand November 2018, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/rechtliche-grundlagen/Datenschutz%20-%20International/DSGVO.html> (zit. EDÖB, EU-DSGVO und die Schweiz), S. 1 ff.

European Data Protection Board (EDPD), diverse Guidelines

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European Data Protection Law, Luxemburg 2018

European Union Agency for Network and Information Security (Enisa), Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, 17. Dezember 2015, abrufbar unter: <https://www.enisa.europa.eu/publications/big-data-protection/at_download/fullReport>