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 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. 1056

Im Evaluationsbericht jedoch wird attestiert, dass der EDÖB nicht über genügend 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, 1057

> «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 eine Aussage des EDÖB selbst zitierwürdig: 1058

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 Ia 97; BGE 110 Ia 85; BGE 103 Ia 492; BGE 100 Ia 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 1086
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-

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 Schranken des Rechts: 1090

> «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 von Belser die *unsachgemässe Verwendung* «des Rechts auf informationelle Selbstbestimmung» ein, indem es festhält: 1091

> «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 wieder auf ihre Grundlagen zurück. Unter Bezug auf Biaggini weist es folglich hin: 1092

> «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 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

1121

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 Publikumsmedien 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. 1161

Indikativ dafür, dass die datenschutzrechtlichen Herausforderungen facettenreicher 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. 1162

Im Zusammenhang mit der Einschlägigkeit diverser Kontexte und ihrer Abgrenzung 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 1163

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]

1178 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]

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:

1209 *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.

1210 *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.

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 *Radiofrequenzsysteme* 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] 1212

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]

1222 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.

1223 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.

1224 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*.

1.1.2. Aggregierung und Auswertung

1225 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-

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»).

Optimierungen werden weiter im Verkehrs- resp. Transportkontext erreicht, in- 1267
dem 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.

Spätestens in dem Augenblick, in welchem personenbezogene Angaben, Analyse- 1268
ergebnisse 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.

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] 1272

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. 1273

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 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. 1283

Kundinnen und Kunden, die der Verarbeitung von Personendaten durch den 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. 1284

Mittels Generierung und Auswertung der gesammelten Angaben über das Konsumverhalten lassen sich in diverser Hinsicht *Effizienzsteigerungen* erreichen, 1285

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 abbildenden privacy policies, mit denen der Datenschutz gewährleistet werden soll. Kritische Worte hierzu in der New York Times: 1305

> «We read 150 privacy policies. They were an incomprehensible disaster.»[1760]

Dasselbe Medium, die New York Times, liefert mit ihrer privacy policy die Probe aufs Exempel, um die Strategie der (versuchten) Transparenz und deren Problematik zu illustrieren: 1306

> «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 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] 1307

Ein ähnliches Bild findet man bei der Zeit und deren Datenschutzerklärung. Hier ist unter dem Schlagwort «Werbedienste» zu lesen: 1308

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.

1317 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.

1318 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.

1319 *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

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-Verbraucher schuetzer-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.

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. 1409

2.3. *Kontextualisierende Schlussfolgerungen*

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, 1410

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.

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. 1444

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 1445

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 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] 1499

Welche *Folgerungen* aus der Formulierung gemäss DSGVO in ihrem Schutzzweckartikel 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. 1500

Unbestritten dürfte schon heute sein, dass die *systematische Auslegung* von besonderer 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. 1501

Anhand dieser Kurzanalyse wurde deutlich, dass das *Datenschutzrecht mehrdimensionalen und verschiedenen Schutzzwecken* dient. Namentlich eine systematische und kontextuelle Auslegung von Art. 1 DSGVO kann Entwicklungen 1502

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]

1505 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.

1506 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.

1507 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.

1508 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-

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.

1524 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-

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]

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. 1568

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. 1569

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] 1570

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]

1576 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.

1577 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

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. 1625
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.

Ansatzpunkte für die wissenschaftliche Analyse von datenschutzrechtlichen 1626
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.

Die Weiterentwicklung der für die analoge Welt etablierten Rechtskategorien 1627
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]

Lange war die *persönlichkeitsrechtliche Begründung des Privatheits- und Daten-* 1628
schutzes 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-

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.

1665 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]

1666 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

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 Erscheinungen 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. 1669

Gleichwohl zeige die Diskussion um die Kommerzialisierung von Persönlichkeitsrechten, 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] 1670

Nachdem er den Begriff des Gutes mit Bezug auf Information dargelegt hat, 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- 1671

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 f.; 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.

1755 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]

1756 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.

1757 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.

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.

Die jüngsten datenschutzrechtlichen Entwicklungen zeigen, dass Lösungen nicht 1793
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.

Ein Denken «out of the box» ist gefragt, gerade für ein Rechtsgebiet, das sich 1794
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.

Im nun folgenden IX. und letzten Kapitel geht es darum, für den Datenschutz 1795
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.

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. 1801

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. 1802

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- 1803

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.

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. 1827

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. 1828

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. 1829

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*.

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. 1930

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. 1931

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 1932

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]

1949 Bestätigt wird viertens, dass jede Technologie bezüglich ihrer Auswirkungen auf 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]

1950 Die US-amerikanischen Entscheide richten den Fokus punktuell zu stark auf die 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 Vertrauens 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: 1959

> «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 nicht nur der Gewährleistung individueller Entscheidungsfreiheit und politischer Meinungskundgabe. Sie nehmen zugleich eine *Garantenstellung für das demokratische System* an sich ein. 1960

Für den demokratischen und politischen Kontext ist der jüngste Facebook-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- 1961

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]

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] 1970

Im *Anstellungskontext* ist ein System, das keinerlei Restriktionen für die Erhebung von Informationen zu potentiellen Arbeitnehmenden vorsieht, zwar geeig- 1971

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.

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. 1985

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] 1986

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. 1987

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.