Bild und Recht – Studien zur Regulierung des Visuellen 7

Anne Steinbrück

Identitätsverwaltung in IKT-Systemen

Spieltheoretische Begründung eines Mediationsagenten zur Verhandlung personaler Identitäten

Nomos

Bild und Recht – Studien zur Regulierung des Visuellen

herausgegeben von

Prof. Dr. Thomas Dreier
PD Dr. Dr. Grischka Petri
Prof. Dr. Wolfgang Ullrich
Prof. Dr. Matthias Weller

Band 7

Anne Steinbrück

Identitätsverwaltung in IKT-Systemen

Spieltheoretische Begründung eines Mediationsagenten zur Verhandlung personaler Identitäten

Nomos

Dissertation an der rechtswissenschaftlichen Fakultät
der Albert-Ludwigs-Universität Freiburg,
Dekan: Prof. Dr. Jan von Hein
Mündliche Prüfung: 12./13.05.2020 in Karlsruhe
Erstgutachter: Prof. Dr. Thomas Dreier, M.C.J.
Zweitgutachter: Prof. Dr. Jens-Peter Schneider

Zum Buchcover:
© Deutscher Bundestag / Julia Nowak-Katz (Ausschnitt): Trichterförmiges Lichtumlenkelement (Konus), um das Tageslicht in den Plenarsaal zu lenken. Zudem werden die Besucher in verschiedenen Facetten abhängig vom Betrachtungswinkel sichtbar.

The book processing charge was funded by the Baden-Württemberg Ministry of Science, Research and Arts in the funding programme Open Access Publishing and the University of Freiburg.

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

Zugl.: Freiburg i. Br., Univ., Diss., 2020

1. Auflage 2020

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

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

ISBN (Print): 978-3-8487-6873-8
ISBN (ePDF): 978-3-7489-0969-9

DOI: https://doi.org/10.5771/9783748909699

Onlineversion
Nomos eLibrary

Für Regine Lindner

und diejenigen Menschen, die für mich identitätsbildend waren, sind und es noch sein werden.

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2020 als Dissertation an der rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg angenommen. Der Stand der Arbeit ist Juni 2020. Sie untersucht den Schutz personaler Identitäten in Zeiten von *Big Data*. Es wird dafür ein ethisch-technischer Mediationsagent begründet, der einen Schutzmechanismus gegen diskriminierende Algorithmen bei der Profilbildung darstellt. Ein solcher Mediationsagent soll den Einfluss auf die Bilder personaler Identitäten steigern und der freien Persönlichkeitsentwicklung im online-Kontext dienen.

Diese Arbeit entstand im Rahmen meiner Forschungen im Kompetenzzentrum KASTEL (BMBF) am Zentrum für Angewandte Rechtswissenschaft (ZAR) des Karlsruher Instituts für Technologie (KIT). Dabei gilt mein größter Dank Herrn Prof. Dr. Thomas Dreier, M.C.J., der mir nicht nur die Promotion ermöglichte, sondern mich auch zur Interdisziplinarität dieser Arbeit ermutigte. Ebenso bin ich Herrn Prof. Dr. Jens-Peter Schneider für die schnelle Zweitbegutachtung ausgesprochen dankbar. Für den größtmöglichen Forschungsfreiraum in der Forschungsgruppe Informationsrecht für technische Systeme und Rechtsinformatik (ITR) danke ich Herrn apl. Prof. Dr. Oliver Raabe sehr. Schließlich danke ich Herrn Prof. Dr. Thomas Dreier und den Herausgebern der Reihe „Bild und Recht“ für die Aufnahme dieser identitätsbezogenen Arbeit.

Meinem Lebensgefährten Artur Andrzejak danke ich in besonderem Maße für seine kontinuierliche Unterstützung, seine Offenheit und für seinen Humor. Damit hat er die Entstehung dieser Arbeit maßgeblich beeinflusst.

Heidelberg, Juni 2020 *Anne Steinbrück*

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
ACM	„Association for Computing Machinery“
a. E.	am Ende
a. F.	alte Fassung
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeine Gleichbehandlungsgesetz
Art.	Artikel
AöR	Archiv des öffentlichen Rechts
Az.	Aktenzeichen
BaaS	„Blockchain as a Service“
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMWi	Bundesministerium für Wirtschaft und Energie
BRD	Bundesrepublik Deutschland
BSIG	BSI-Gesetz
BT-Drucks.	Deutscher Bundestag Drucksachen
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BZRG	Bundeszentralregistergesetz
B2B	„Business to Business“
B2C	„Business to Consumer“
ca.	circa
Cal. Law Review	„California Law Review“
CLSR	„Computer Law & Security Review“
COM	„Commission“
Cornell Int’l LJ	„Cornell International Law Journal“
CR	Computer und Recht

CRi	„Computer Law Review International“
C2C	„Consumer to Consumer“
DCFR	„Draft Common Frame of Reference“
De-Mail-G	De-Mail-Gesetz
Ders.	Derselbe
Dies.	Dieselbe
DSGVO	Datenschutzgrundverordnung
DSGVO-E	Datenschutzgrundverordnung – Entwurf
DSRI	Deutsche Stiftung für Recht und Informatik
DuD	Datenschutz und Datensicherheit
Duke L. & Tech.	„Duke Law & Technology Review“
EDPL	„European Data protection Law Review“
EDPS	„European Data Protection Supervisor“
EG	Europäische Gemeinschaft
eIDAS-VO	Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt
Einf	Einführung
EJRR	„European Journal of Risk Regulation“
EPrivacy-VO-E	Verordnung über Privatsphäre und elektronische Kommunikation – Entwurf
ERCL	„European Review of Contract Law“
EU	Europäische Union
EuGRZ	Europäische Grundrechte-Zeitschrift
EuGH	Europäischer Gerichtshof
EWG	Erwägungsgrund
f./ff.	Folgende/ Fortfolgende
FAS	Frankfurter Allgemeine Sonntagszeitung
FAZ	Frankfurter Allgemeine Zeitung
Fn.	Fußnote
GG	Grundgesetz
GPS	„Global Positioning System“
GRC	Charta der Grundrechte der Europäischen Union
GWB	Gesetz gegen Wettbewerbsbeschränkungen
Harv. L. R.	„Harvard Law Review“
Hrsg.	Herausgeber

IDPL	„International Data Privacy Law“
IEEE	„Institute of Electrical and Electronics Engineers“
IKT	Informations- und Kommunikationstechnik
IP-Adresse	Internetprotokoll-Adresse
i. V. m.	in Verbindung mit
IWRZ	Zeitschrift für internationales Wirtschaftsrecht
JIPITEC	„Journal of Intellectual Property, Information Technology and Electronic Commerce Law”
JTHTL	„Journal on Telecommunications and High Technology Law“
JZ	JuristenZeitung
KASTEL	Kompetenzzentrum für angewandte Sicherheitstechnologie
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie-KunstUrhG
K&R	Kommunikation & Recht
LG	Landgericht
MedG	Mediationsgesetz
MMR	Multimedia und Recht
mwN	mit weiteren Nachweisen
NamÄndG	Gesetz über die Änderung von Familiennamen und Vorname
NIS-Richtlinie	Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
N&R	Netzwirtschaften & Recht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZZ	Neue Züricher Zeitung
OSI-Modell	„Open Systems Interconnection model“
OTT-Dienste	„Over the Top“-Dienste
PAuswG	Personalausweisgesetz
PassG	Passgesetz
PinG	„Privacy in Germany“
PKI	„Public-Key-Infrastructure“
PR	„Public Relations“

ProdHG	Produkthaftungsgesetz
PStG	Personenstandsgesetz
P2C	„Public to Consumer“
RDV	Recht der Datenverarbeitung
Rn.	Randnummer
S.	Satz/ Seite
sog.	sogenannt
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVO	Straßenverkehrsordnung
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TSG	Transsexuellengesetz
u. a.	und andere
U.S.	„United States of America“
U. Chi. Legal F.	„University of Chicago Legal Forum“
Urt.	Urteil
UWG-E	Gesetz gegen den unlauteren Wettbewerb-Entwurf
v.	vom
VergabeR	Zeitschrift für das gesamte Vergaberecht
Vgl.	Vergleiche
Vor	Vorbemerkung
VSBG	Verbraucherstreitbeilegungsgesetz
VwZG	Verwaltungszustellungsgesetz
Wash. L. Rev.	„Washington law review“
WRV	Weimarer Reichsverfassung
Yale L. J.	„Yale Law Journal“
ZaörRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZKM	Zeitschrift für Konflikt-Management
ZRP	Zeitschrift für Rechtspolitik
ZSHG	Zeugenschutz-Harmonisierungsgesetz

1.Teil: Einleitung

A. Motivation

Der Schutz personenbezogener Daten aus Art. 8 der europäischen Grundrechtecharta (GRC) und in der sekundärrechtlichen Datenschutzgrundverordnung (DSGVO) ist in digitalen Kontexten allgegenwärtig. Anders verhält es sich hingegen mit zusammengefassten personenbezogenen Daten in Gestalt der personalen Identität, die ebenfalls in ihren Entwicklungsbedingungen als schutzwürdig gilt. Der titelgebende Begriff der Identität ist insofern vielschichtig. Bedingt durch die Bedeutung des Vergleichens und der Zuschreibung einer Identität, steht die inhaltliche Ausgestaltung der personalen Identität aber im Zusammenhang mit dem Individuum. Somit wird keine datenzentrierte Perspektive eingenommen, sondern die Perspektive verschiebt sich auf die entstandene personale Identität.

Als Motivation der Untersuchung wird angenommen, dass sich die personale Identität im online-Kontext anders realisiert als im offline-Kontext und sich dies auf die Wahrnehmbarkeit der Identität in der Interaktion auswirkt. Denn die gesteigerten Interaktionsmöglichkeiten im online-Kontext, die nahezu zeitgleich über die Ländergrenzen hinweg möglich sind, lassen sich im offline-Kontext kaum abbilden. Danach ist die parallele Kommunikation mit Freunden etwa in einem Browser-Fenster möglich, in dem nächsten Browser-Fenster erfolgt die Kommunikation im beruflichen Netzwerk, in einem weiteren Browser-Fenster wird die Bewertung des letzten Restaurantbesuches getätigt und parallel lässt sich in der Applikation im Mobilfunkgerät der Verbrauch des „digitalen Hausrates“[1] beim Dienstanbieter einsehen. Diese im online-Kontext parallelen Handlungsmöglichkeiten finden mit der zeitlichen Dichte und Interaktionsvielfalt schwerlich eine Entsprechung im offline-Kontext. Darin kommt eine von dem Medienwissenschaftler *Pörksen* beschriebene Annahme der *„unerträgliche(n) Gleichzeitigkeit des Seins“*[2] zum Ausdruck, die zwar auf die Sofortvergleichbarkeit eines weiten Nachrichtenspektrums zwischen voyeuristischen Nachrichten der Boulevardpresse und schrecklichen Kriegsnachrichten ab-

1 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 25–38.
2 *Pörksen*, NZZ vom 12.07.2018, 37.

zielt, aber ebenso die gesteigerte Parallelität von Interaktionen und Identitätsrealisierung des Individuums verdeutlicht.

Weiter werden im online-Kontext vom Nutzer beim Aufrufen der Webseiten, dem Bewerten von Produkten oder Kommentieren von Nachrichten solche Informationsspuren hinterlassen, die Erkenntnisse über die personale Identität ermöglichen. Gleichwohl bleiben diese Informationsspuren etwa in Gestalt von Cookies und Profilen in ihrem inhaltlichen Erkenntniswert intransparent, so dass für den Nutzer eine Ungewissheit über die Folgen seines Nutzungsverhalten verbleibt. Denn einerseits können die Erkenntnisse in der Datenmenge untergehen, andererseits besteht das Risiko, dass sich Rückkoppelungswirkungen auf den Nutzer in Gestalt von zielgerichteter Werbung oder zielgerichteten Nachrichten entfalten. Dahinter stehen Algorithmen, mit denen die Profile für nutzerspezifische Einblendungen erstellt werden, die verhaltensbeeinflussenden Charakter haben können. Eine derart gezielte individuelle Ansprache der Nutzerinteressen im online-Kontext ist im offline-Kontext nicht erkennbar, was die Erforderlichkeit eines differenzierten Schutzregimes für die personale Identität im online-Kontext deutlich macht. Dabei bedarf es einer realen Kontrollmöglichkeit über die entstandenen personalen Identitäten, damit in Kenntnis dieser das Individuum seine Selbstbestimmung ausüben kann. Die Ungewissheit über die entstandenen Profile der personalen Identität im online-Kontext verlangt zunächst deren Transparenz, damit das Individuum auf die Fragen, „Wer bin ich im sozialen Netzwerk?“, „Wer wird erkennbar bei der Bewertung des Restaurants?“ und „Wer ist aus dem Benutzungsverhalten über den digitalen Hausrat erkennbar?“ auch Antworten bekommt. Erst wenn diese Fragen beantwortet werden können, besteht eine reale Selbstbestimmungsmöglichkeit. Gleichwohl ist unklar, wie sich die personale Identität im online-Kontext zusammensetzt und welchen Einfluss die Interaktionen auf die Darstellung der personalen Identität haben, was die Frage nach dem Identitätsbegriff aufwirft. Die mögliche Antwort kann in der Beschreibung aus *Alice im Wunderland* liegen, in der sich Alice fragt, ob sie am Morgen beim Aufstehen dieselbe wie immer sei und sie dabei glaubt, sich ein bisschen anders gefühlt zu haben,[3] was ein dynamisches Identitätsverständnis nahelegt.

Entsprechend lässt sich ein dynamisches Identitätsverständnis, welches sich an den verschiedenen Ausprägungen eines Individuums orientiert, für ein Identitätsverwaltungsmodell heranziehen, was sich auch in der Legal-

3 *Carroll*, Alice im Wunderland, 1993, S. 22.

definition zu personenbezogenen Daten gemäß Art. 4 Nr. 1 DSGVO[4] widerspiegelt. Danach kann etwa die online-Kennung *Ausdruck* der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen *Identitäten* einer natürlichen Person sein. Damit erkennt das Schutzregime der DSGVO neben dem Schutz der personenbezogenen Daten die Ausprägungen der Identitäten im offline- und im online-Kontext gleichermaßen an. Dazu gehört, dass die Einfluss- und Selbstbestimmungsmöglichkeit über personenbezogene Daten und die damit verbundenen personalen Identitäten gewährleistet wird. Dies umfasst auch die Kontrolle des Individuums über die personale Identität, die dem Schutzregime der informationellen Selbstbestimmung aus Art. 7, 8 GRC[5] unterliegt.

Dieses grundrechtliche Postulat der Selbstbestimmung gilt für die Identitätsverwaltung in informations- und kommunikationstechnischen (IKT)-Systemen und erwächst aus den Phänomenen der personalen Identitäten im online-Kontext in einem Zeitalter ubiquitärer Datenverarbeitungen. Neben dem rechtlichen Schutzregime wirkt das politische und wirtschaftliche *Konzept der digitalen Souveränität* zum Schutz der personalen Identität. Denn die digitale Souveränität beschreibt die selbstbestimmte Kontrolle über Daten und ihre Löschung in einer freiheitlichen Gesellschaft und funktionierenden Wirtschaft in komplexen und vernetzten Systemen.[6] Gleichzeitig kann aus dem Konzept der digitalen Souveränität der Bedarf nach rechtlichen Rahmenbedingungen für die generelle Stärkung der Entscheidungssouveränität und Transparenz über die Funktionsweise von Algorithmen gegenüber Individuen abgeleitet werden.[7]

Demnach wirkt die digitale Souveränität auf individueller Ebene als Datensouveränität über die personenbezogenen Daten und stellt zugleich das Postulat der Verwirklichung des Schutzes der informationellen Selbstbe-

4 Ebenso in Art. 2 a) der Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

5 Für das Kombinationsgrundrecht gemäß Art. 7, 8 GRC wird die Begrifflichkeit der informationellen Selbstbestimmung gewählt, um die Information als maßgebliche Anknüpfung für die Überschneidung zwischen dem Schutz der personenbezogenen Daten und dem Schutz des Privatlebens hervorzuheben. Gleichwohl wird das divergierende Schutzniveau zwischen dem europäischem Datenschutzgrundrecht und dem Recht auf informationelle Selbstbestimmung in dieser Untersuchung dargestellt.

6 *Beyerer/Müller-Quade/Reussner*, DuD 2018, 277.

7 *Dies.*, DuD 2018, 277 (278).

stimmung dar. Dies gilt verstärkt, wenn die Verarbeitung personenbezogener Daten von international agierenden Intermediären über die Ländergrenzen hinweg erfolgt und die Profile von Nutzern in sozialen oder beruflichen Netzwerken international abrufbar sind. In diesen Konstellationen drängt sich die Frage nach der Wirksamkeit des nationalen Regelungsregimes auf, wenn personale Identitäten intransparent und kaum bestimmbar sind. Neben regulatorischen Maßnahmen kommt daher die Identitätsverwaltung als ein im „Schatten des Rechts" wirkender Schutzmechanismus in Betracht.

B. Phänomene im online-Kontext

Der online-Kontext zeichnet sich, wie dargelegt, auch durch die gesteigerte Gleichzeitigkeit des Seins von Identitäten aus. Diese Identitäten sind für das Individuum mit der gleichzeitigen Nutzbarkeit zwar wahrnehmbar, die mit der Nutzung einhergehenden Erkenntnismöglichkeiten bleiben aber für das Individuum verborgen. Dieses online-Phänomen steigert sich, wenn das Nutzungsverhalten in den geschützten privaten Räumen stattfindet, aber die Eingaben etwa in einem sozialen Netzwerk einer breiten Öffentlichkeit zugänglich gemacht werden und die damit verbundenen Erkenntnismöglichkeiten kaum vorhersehbar sind. Dabei wird das Nutzungsverhalten im online-Kontext von dem Eindruck der Privatsphäre und Ortlosigkeit geprägt, was die Offenlegung privater Informationen erleichtert. Das Nutzungsverhalten ist geprägt von digital unbewussten Verhaltensweisen („*Digital unconscious*"[8]), was von den Darstellungen der Programme begünstigt wird.[9] Ebenso können im online-Kontext leichter fiktive Selbstbilder präsentiert werden, da die unmittelbaren Auswirkungen verfälschender Selbstdarstellungen im online-Kontext von der Wahrnehmbarkeit der handelnden Person zunächst ausgeschlossen sind oder die Wahrnehmbarkeit nur zeitlich verzögert erfolgt. Somit lässt sich eine Erosion der bewährten Sphäreneinteilung zwischen privater und öffentlicher Sphäre feststellen. Denn in den privaten Räumlichkeiten entsteht eine gesteigerte Offenlegungsbereitschaft über öffentlich sichtbare Äußerungen und die möglichen Folgen stehen im Widerspruch zu der empfundenen Privatsphäre.

---

8 *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 65.
9 *Turkle*, Leben im Netz – Identität in Zeiten des Internet, 1999, S. 264 f.

Mit der Ubiquität von Datenverarbeitungsprozessen geht das *Big Data*-Phänomen einher, dass neben der Verarbeitung personenbezogener Daten die Wertschöpfung und die Innovationsmöglichkeiten aus diesen betrieben werden, was einen weitergehenden Schutzbedarf gegenüber dem Individuum auslöst.[10] Denn weitreichende Datenverarbeitungen ermöglichen das Entstehen von Datenreservoirs[11], aus denen umfangreiche Erkenntnisse ableitbar sind, die nicht nur das Risiko der Re-Identifizierbarkeit steigern, sondern aufgrund der Kombination und *Dekontextualisierung der Datensätze* den Schutz der informationellen Selbstbestimmung gefährden. Diese möglichen Erkenntnisse ergeben sich neben der Verarbeitung personenbezogener Daten aus der Einbeziehung von Metadaten, die aus den Interaktionen und dem Standortwechsel eines Individuums entstehen und zusammengeführt einen umfassenden Erkenntnisgehalt ermöglichen. Die 1983 im Volkszählungsurteil postulierten Feststellungen, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum"[12] gäbe und die gewandelten technologischen Bedingungen umfassende und detaillierte Bilder einer Person ermöglichen[13], bleiben damit aktuell und finden in den jüngeren Entscheidungen „Recht auf Vergessen I & II"[14] eine weitere Konkretisierung für den online-Kontext.

Neben dem Phänomen der Datenverarbeitung gehört die Informations- und Wissenserlangung zum Geschäftsmodell von Intermediären, was personenbezogene Daten zu einem Rohstoff[15] macht. Den Intermediären kommt als Plattformbetreiber eine Schlüsselfunktion zu, da sie Akteure im Binnenmarkt der Datenökonomie und gleichzeitig Wärter über den Schutz der personenbezogenen Daten sind. Insofern kommt ihnen gegenüber dem Nutzer die Funktion eines Mediators[16] zu. Daher bildet das Konzept der digitalen Souveräntität zur Sicherstellung der individuellen Selbstbestimmung in seiner wirtschaftlichen Dimension ein Gegengewicht in der europäischen Datenökonomie. Dies gilt umso mehr, wenn die Trennung von Kontexten offline möglich ist, aber im online-Kontext die Grenzen der Kontexte faktisch aufgehoben sind.

---

10 *Smart Data Begleitforschung*, Smart Data - Smart Privacy?, 2015, S. 2 f.
11 *Solove*, Harv. L. R. 2013, 1880 (1889).
12 BVerfGE 65, 1 (45).
13 BVerfGE 65, 1 (17).
14 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I; BVerfG, Urt. v. 06.11.2019 – 1 BvR 276/17, Recht auf Vergessen II.
15 *Smart Data Begleitforschung*, Smart Data - Smart Privacy?, 2015, S. 3
16 *European Data Protection Supervisor, EDPS*, Opinion 8/2016 on coherent enforcement of fundamental right in the age of big data, S. 6.

Die kontextspezifische Datenverarbeitung und Trennung der Erkenntnismöglichkeiten über die personale Identität stößt in Anbetracht der *Ubiquität von Datenverarbeitungen* auf Umsetzungsschwierigkeiten. Denn zu Beginn der Datenverarbeitung sind die hinzukommenden Kontexte und das damit verbundene Risiko erweiterter Erkenntnismöglichkeiten über die personale Identität noch unbekannt. Dies wird in der Konstellation eines smarten Arbeitsplatzes deutlich, bei dem intelligente Assistenzsysteme eingesetzt werden, die umfangreiche Erkenntnisse über das Nutzungsverhalten des Arbeitnehmers ermöglichen und aus denen sich nach einer gewissen Zeit möglicherweise gesundheitsrelevante Informationen ableiten lassen. Ebenso wird dies bei einem im Haushalt einer Familie lebenden Kindermädchen deutlich, das einer Beschäftigung nachgeht und gleichzeitig private Tätigkeiten vornimmt. Dabei ist der datenschutzrechtliche Anwendungsbereich für die private Tätigkeit gemäß Art. 2 Abs. 2 c) DSGVO ausgeschlossen und es hängt von der Erscheinung des Verhaltens ab, wann der Beschäftigtendatenschutz gilt. Weiter lassen sich in sozialen Medien persönliche Informationen austauschen, die zunächst vom Anwendungsbereich ausgeschlossen sind, aber zu einem späteren Zeitpunkt im Datenzyklus von dem Anwendungsbereich der DSGVO erfasst werden. Dies kann bei privat geteilten Informationen unter „Freunden", die in den Sozial- und Beschäftigungsbereich gelangen, erfolgen.

In diesen Konstellationen gelten unterschiedliche rechtliche Schutzregime, die aber ineinander übergehen und gemeinsam zu vielfältigen Erkenntnismöglichkeiten führen. Gesteigert wird die Aufhebung der kontextbezogenen Grenzen, wenn Endgeräte von Sprachassistenten oder gedankenlesenden Technologien mit einem sog. „*Machine-Interface*"[17] verdrängt werden und über eine Schnittstelle sämtliche Informationen aus dem Leben einer Person verarbeitet werden. Hiermit wird die Schwierigkeit einer eindeutigen Trennung der Kontexte besonders deutlich und kann kontextspezifische Schutzmechanismen erheblich erschweren. Dies gilt besonders, wenn die Erkenntnismöglichkeiten sich im Lebenszyklus einer personalen Identität von der urprünglichen Datenverarbeitung etwa im sozialen Netzwerk unvorhersehbar erweitern lassen. Demnach gilt es, das Risiko der kontextübergreifenden Erkenntniserlangung und Dekontextualisierung von personenbezogenen Daten in die grundrechtliche Selbstbestimmungsvorgabe einzubeziehen. Denn das interdependente und kontextübergreifende Gefüge von Datenverarbeitungen erfasse sämtliche Lebensbereiche, welches das spezifische Risiko der „systemischen Digitali-

17 *Budras*, FAS vom 14.10.2018, 21.

sierung“[18] darstelle und ein Schutzregime als Antwort verlangt. Dafür erscheint die Identitätsverwaltung mit der kontextbezogenen Transparenz über personale Identitäten und die Einräumung einer Kontrollmöglichkeit als eine mögliche Lösung. Folglich soll die personale Identität in IKT-Systemen eingeordnet und das IKT-Recht als Grundlage für die *Modellbildung der Identitätsverwaltung* herangezogen werden. Dafür sollen die Phänomene der personalen Identität im offline-Kontext mit dem online-Kontext verglichen werden, um daraus die spezifischen Anforderungen an die Identitätsverwaltung im online-Kontext ableiten zu können.

Mit der Transparenz kann ein Überblick über die Verantwortung des Nutzers hinsichtlich seiner personalen Identitäten im online-Kontext hergestellt werden. Die Notwendigkeit für eine gesteigerte Transparenz lässt sich aus den Speichermöglichkeiten über eine personale Identität ableiten, die im offline-Kontext in dem Maße nicht ersichtlich sind. Gleichwohl sei der Übergang zwischen personaler Identität im offline- und online-Kontext fließend und eine Trennung erscheine künstlich (sog. „*onlife*“),[19] so dass eine strikte Zuordnung der personalen Identität in den Kontexten als erschwert gilt. Dies steigert den Bedarf nach einem differenzierten Schutzmechanismus. Demnach müsste ein Identitätsverwaltungsmodell die Komplexität der personalen Identitäten im online- und offline-Kontext gleichermaßen erfassen und die Kontrollierbarkeit der personalen Identitäten fördern, was wiederum mit dem hier untersuchungsgegenständlichen Modell der Identitätsverwaltung ermöglicht werden soll.

C. Untersuchungsgegenstand

Für die Untersuchung der Rahmenbedingungen einer solchen Identitätsverwaltung in IKT-Systemen bedarf es zunächst der Einordnung in das *Konzept des Selbstdatenschutzes*. Mit dieser Einordnung geht die Annahme einher, dass das Individuum zunehmend in der Verantwortung steht, seine Schutzbedarfe und Rechte selbst zu verfolgen. Denn mit der ubiquitären Datenverarbeitung gehen neue Gefährdungen der informationellen Selbstbestimmung einher, die eines effektiven rechtlichen Schutzregimes bedürfen. Dieses Schutzregime bestand ursprünglich in dem ordnungsrechtlichen Datenschutz des BDSG a. F., der aber nur ineffektiv die neuen Phänomene ubiquitärer Datenverarbeitung lösen konnte. Damit wurde der

18 *Spiecker gen. Döhmann*, CR 2016, 698.
19 *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 42, 50.

Bedarf eines neuen Datenschutzes formuliert, der über die Datenschutzprinzipien hinaus ein Schutzregime mit der Selbstregulierung durch Technikgestaltung ermöglicht.[20] Diese Selbstregulierung betrifft den Verantwortlichen und Betroffenen gleichermaßen, wenn es einerseits um die Implementierung von „*privacy by design*"-Lösungen geht und andererseits der Betroffene im Rahmen des Selbstdatenschutzes jederzeit seine Selbstbestimmung ausüben können soll.[21]

Diese gesteigerte Selbstbestimmung soll mit der Identitätsverwaltung umgesetzt werden und als eine technische Lösung für die Realisierung des Selbstdatenschutzes dienen (I.). Dabei bedarf es für die Eingrenzung der Identitätsverwaltung innerhalb eines Konzeptes des Selbstdatenschutzes der Bestimmung des zentralen Begriffs der Identität. Dieser soll in seinen rechtlichen Ausprägungen dargestellt werden und daneben die fachübergreifenden Perspektiven in den Untersuchungsgegenstand einbezogen werden (II.). Die konkrete Umsetzung der Identitätsverwaltung kann dabei eine dynamische Realisierung voraussetzen, um einen wirksamen und effektiven Schutz zu gewährleisten, was mit einem Regulationskonzept der mediativen Identitätsverwaltung erfolgen könnte (III.).

I. Selbstdatenschutz durch Identitätsverwaltung

Der Selbstdatenschutz als rechtliche Annahme aus der DSGVO bietet eine Lösung zur Realisierung der informationellen Selbstbestimmung und dient der Kompensation des datenschutzrechtlichen Vollzugsdefizits, mit dem der Betroffene gegen das Risiko eines „gläsernen Konsumenten" vorgehen könne.[22] Denn bei dem Phänomen der ubiquitären Datenverarbeitung wird besonders deutlich, dass die datenschutzrechtlichen Prinzipien der Transparenz, der Zweckbindung und Datenminimierung an ihre Grenzen stoßen. Die Transparenz komplexer Datenverarbeitungen und der Erkenntnismöglichkeiten lässt sich kaum für den Laien nachvollziehbar darstellen. Ferner ist eine weite Auslegung des Datenverarbeitungszwecks und eine Änderung dessen zu einem späteren Zeitpunkt der Datenverarbeitung möglich, so dass umfangreiche und unvorhersehbare Datenverarbeitungen vorgenommen werden können. Ebenso wird die Datenminimierung nur begrenzt umgesetzt, wenn Geschäftsmodelle darauf ausge-

20 *Roßnagel*, MMR 2005, 71 (74).
21 *Ders.*, MMR 2005, 71.
22 *Forum Privatheit*, White Paper – Selbstdatenschutz, 2014 S. 3 f.

richtet sind, möglichst umfassend Zugang zu personenbezogenen Daten zu erlangen. Daraus ergibt sich, dass der datenschutzrechtliche Vorfeldschutz gegenüber den Realphänomenen nur unzureichenden Schutz bietet und die Identitätsverwaltung als Konzept des Selbstdatenschutzes als Lösungsmechanismus heranzuziehen ist.

Der Lösungsmechanismus im Rahmen des Selbstdatenschutzes ist aus dem IKT-Recht in Gestalt der Transparenz, der Einwilligung, der Betroffenenrechte und dem Einsatz von technischen und organisatorischen Maßnahmen abzuleiten. Hinsichtlich der technischen Maßnahmen könnte für den Selbstdatenschutz ein Mechanismus in Frage kommen, mit dem der Nutzer sich selbst schützt. Damit würde der Selbstdatenschutz aus dem IKT-Recht mit einem technischen Konzept erweitert werden, welches über eine technische Normierung realisiert und zu einer Umsetzungsaufgabe der Hersteller werden könnte. Weiter müsste ein Konzept des Selbstdatenschutzes in einem Gesamtgefüge zum Schutz der personenbezogenen Daten stehen, welches zudem aus aufsichtsrechtlichen und strukturellen Schutzmaßnahmen bestehen kann. Mit einem in diesem Gesamtgefüge bestehenden Konzept des Selbstdatenschutzes würde die natürliche Person wieder zum Steuerungsadressaten „ihrer" Daten werden und es könnten zusätzliche Anreizmechanismen zur expliziten Steuerung der personenbezogenen Daten und der damit verbundenen personalen Identitäten eingesetzt werden.

Demnach soll ein *Modell zur Identitätsverwaltung* begründet werden, mit dem der bestehende Schutz im IKT-Recht um eine Schutzebene erweitert und als Grundlage für die Identitätsverwaltung herangezogen wird. Dabei soll der zentrale Schutzgegenstand der informationellen Selbstbestimmung über den Lebenszyklus einer personalen Identität hinweg gewahrt bleiben können und einen möglichen kompensatorischen Mechanismus enthalten, der einen Ausgleich gegenüber dem datenschutzrechtlichen Vollzugsdefizit darstellt. Für diesen Mechanismus könnte die Transparenz der Risiken von Datenverarbeitungsvorgängen über personale Identitäten erforderlich sein, um einen wirksamen Schutz der informationellen Selbstbestimmung herbeiführen zu können. Mit der Identitätsverwaltung als Möglichkeit der Selbstkontrolle könnte ein Gegengewicht zu den Phänomenen der ubiquitären Datenverarbeitung von Intermediären und der damit verbundenen Fremdkontrolle begründet werden. Sobald das „Risiko der Fremdbestimmung"[23] steige, bedarf es eines wirksamen Selbstdaten-

23 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 2.

schutzes gegen die entstandenen Informationsasymmetrien und algorithmusgesteuerten Erkenntisverfahren. Denn neben den Kräften des demokratischen Gesetzgebers wirkt der Markt auf die Phänomene in online-Kontexten und dieser Markt hat das Potential, den Bürger mit seinen Schutzmöglichkeiten zu verdrängen. Folglich könnte mit der Identitätsverwaltung und einem angemessenen regulatorischen Rahmen ein Gegengewicht geschaffen werden, welches den Selbstdatenschutz der natürlichen Person stärkt. Denn das Individuum verbleibt als „einziger plausibler Akteur“[24], der im Mittelpunkt des grundrechtlichen und IKT-rechtlichen Schutzes steht und seine Schutzwürdigkeit mit der fortschreitenden ubiquitären Datenverarbeitung beibehalten sollte.

II. Begriff der Identität

Der Begriff der Identität wird in der Rechtsordnung vielfach verwendet und es können in ihm aufgrund der rechtswissenschaftlichen Perspektive, welche als „disziplinäres Cluster“[25] verstanden werden kann, verschiedene fachliche Ausprägungen zum Ausdruck kommen. Dafür soll der Begriff zunächst überblicksartig im Recht eingeordnet (1.) und anschließend aus der philosophischen Perspektive (2.) beleuchtet werden. Mit der philosophischen Betrachtung wird die inhaltliche Grundlage für den Bedeutungsgehalt des Begriffs der personalen Identität geprägt werden. Die herausgearbeiteten Phänomene der personalen Identitäten sollen für die untersuchungsgegenständliche Modellbildung der Identitätsverwaltung herangezogen werden.

1. Identität im Recht

Unter dem Begriff der Identität wird zunächst die rechtliche Anerkennung einer staatlichen Zugehörigkeit verstanden. Diese Ausprägung der Identität entspricht einem Menschenrecht und wird von den Vereinten Nationen als solches in Ziffer 16.9 aus der „*2030 Agenda for Sustainable Develop-*

24 *Teubner*, Zeitschrift für Rechtssoziologie 2006, 5 (6).
25 *Jestaedt*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, S. 110.

ment" festgeschrieben, wonach bis 2030 jeder über eine rechtliche Identität, einschließlich der Eintragung im Geburtenregister, verfügen soll.[26]

In nationaler Hinsicht lassen sich unter dem Identitätsbegriff der Name, die Eintragung im Geburtenregister und die Informationen im Personalausweis einordnen. Dahingehend wurde die „digitale Identität"[27] spiegelbildlich zur offline-Welt im elektronischen Personalausweis gemäß § 18 PAuswG anerkannt. Diese digitale Identität kann im online-Kontext eingesetzt werden, indem mit einem Passwort eine Authentifizierung ermöglicht und die digitale Identität einem Individuum zugewiesen wird. Mit der Zuweisung von Passwörtern könnte im privatrechtlichen Kontext die sog. „*Single Sign-On*"-Lösung mit nur einem Passwort als Konzept der Identitätsverwaltung umgesetzt werden, wie es bereits von Intermediären zum erleichterten Registrieren und Anmelden angeboten wird.

Neben dem Konzept der Identitätsverwaltung als Berechtigungsverwaltung mit Passwörtern,[28] soll der Begriff der personalen Identität mit seinen Ausprägungen aus Art. 4 Nr. 1 DSGVO herangezogen werden. Damit soll die Identitätsverwaltung im Sinne eines Passwortmanagers um die datenschutzrechtlich anerkannten Ausprägungen der personalen Identität erweitert werden. Dies ist der erste zentrale Beitrag, der in dieser Untersuchung geleistet werden soll, um das Schutzregime im Rahmen des Selbstdatenschutzes in der DSGVO konkretisieren zu können. Für die Veranschaulichung dieser Pluralität an Phänomenen der personalen Identitäten, die gerade in online-Kontexten sichtbar werden, soll der einfachrechtliche Bezug zur Identität über das Namensrecht hinaus einbezogen werden. Dafür werden neben den Ausprägungen der „physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität"

26 www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E (zuletzt aufgerufen 20.06.2020). Ebenso ist in der UNCITRAL, *Working Group IV – Electronic Commerce*, ein internationalisiertes Konzept der Identitätsverwaltung der Gegenstand von Konsultationen. Bei der Findung von gemeinsamen Regelungen wird die eIDAS-VO als Regelungsbeispiel mit einbezogen. Gleichwohl sind die rechtskulturellen Unterschiede der Mitgliedstaaten über den Schutz der Privatheit derart differenziert, dass ein internationales datenschutzrechtliches Identitätsverwaltungsmodell nur schwer realisierbar sein wird. Damit würde sich eine mögliche Regelung der Identitätsverwaltung auf die internationale Nutzung von Signaturen und elektronischen Identitäten beziehen (Gespräch am 04.02.2019 mit zuständigem Referat im BMWi).

27 *Hornung*, Die digitale Identität, 2005.

28 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 68.

gemäß Art. 4 Nr. 1 DSGVO die personalen Teilidentitäten im IKT-Recht für die Modellbildung herangezogen.

Aus diesen Dimensionen der personalen Identität wird ein *stipulatives Modell zur personalen Identität und der Identitätsverwaltung* begründet. Damit könnte eine Entsprechung der personalen Identität mit ihren pluralen Ausprägungen von dem offline- in den online-Kontext übertragen und ein gleichwertiger Schutzmechanismus begründet werden.

2. Identität aus der philosophischen Perspektive

a) Identität von der Ununterscheidbarkeit zum Handlungsergebnis

Der Identitätsbegriff aus der philosophischen Perspektive lässt sich zunächst mathematisch nach *G. W. Leibniz* als Prinzip der Identität des Ununterscheidbaren umschreiben.[29] Darin komme die Bedeutung der Identität als „*idem*" also Gleichheit zum Ausdruck, womit ein Zuordnungszustand von absoluter Identität beschrieben wird, der eine qualitative Differenz zweier Objekte ausschließt.[30] Dem folgend erscheint die Identität in der Natur zweifelhaft, da etwa kein Eichenblatt oder kein Lebewesen dem anderen gleichen könne.[31] Mit dem Begriff der Identität geht daher die Singularität einher, die jedoch nur dann feststellbar ist, wenn der Vergleich zweier Objekte in einem Kontext vorgenommen wird. Darin kommt zum Ausdruck, dass die Identität der Klarstellung eines absolut Gleichen dient und gleichzeitig die Beschreibung der Operation des Vergleichens ist.

Da in der Biographie eines Individuums der Lebende von Kindesbeinen an immer derselbe sei, auch wenn er das Alter erreicht habe, befinde sich das Individuum in seiner Biographie immer in einem System von Beziehungen.[32] In diesem werde sich das Individuum immer wieder in seiner Physiologie über die Haare und das Blut erneuern und in seinen Beziehungen über die Freuden, Befürchtungen, Meinungen und Gewohnheiten niemals gleich bleiben im Sinne einer mathematischen Gleichheit.[33] Folglich

29 *Brockhaus Enzyklopädie,* 2006, Bd. 13, zu „Identität".
30 *Meuter*, in: Kolmer/Wildfeuer/Krings u.a. (Hrsg.), Neues Handbuch philosophischer Grundbegriffe, 2011, Bd. 2, S. 1203; *Siegwart*, in: Sandkühler (Hrsg.), Enzyklopädie Philosophie, 2010, Bd. 2, S. 1067.
31 *Brockhaus Enzyklopädie,* 2006, Bd. 13, zu „Identität".
32 *Platon*, Symposion, 2008, 207 D.
33 *Ders.*, Symposion, 2008, 207 E.

kann die Realisierung von Identität und ihre kontextbedingte Abhängigkeit festgestellt werden, worin der Begriff der Identität eine inhaltliche Ausgestaltung erfährt.[34] Die personale Identität knüpft demnach an die Physis und das Verhalten der Person an und wird relational bestimmt.

Nach *Koorsgard* wird die Handlung als Zweck der personalen Identität beschrieben und als Ergebnis des inneren Entscheidungsprozesses, der in eine äußerlich wahrnehmbare und vorübergehende („*contingent*") Handlung münde.[35] Die personale Identität setze sich zusammen aus den inneren Entscheidungen und äußeren Handlungen, worin eine „Konzeption von praktischer Identität" als Beschreibung und Selbstdarstellung des eigenen Selbst liege.[36] Schließlich führt *Korsgaard* aus, dass eine Giraffe nur dann eine sei, wenn sie das Prinzip verfolge, sich wie eine Giraffe zu verhalten.[37] Demnach sei die Handlung als Konstituierung und Konstruktion der Persönlichkeit und Identität einzuordnen.[38] Für den Begriff der personalen Identität lässt sich daraus zum einen der Name als Gleichheit und zum anderen die Handlung als konstitutives Element über die Biographie hinweg einordnen.

b) Identität nach *Ricœur*

Aus der philosophischen Perspektive bezieht der Identitätsbegriff nach *Ricœur* drei Ebenen in das Modell ein. Diese bestehen aus der Identität im Sinne der Gleichheit, der Identität als Selbst und der Identität als Realisierung einer Handlung in einer kommunikativen Beziehung. Folglich handelt es sich bei *Ricœur* um eine zusammengesetzte Identität, die einen numerischen Teil der Gleichheit *(Idem)* umfasst, welcher auf die Frage des „*Wer?*" zugeordnet werden könne, und einem sprechenden Teil als Selbstheit *(Ipse)*, der sich über die Handlung dynamisch realisiere.[39] Beide Ausprägungen der Identität stehen dialektisch zueinander und begründen den

34 *Meuter*, in: Kolmer/Wildfeuer/Krings u.a. (Hrsg.), Neues Handbuch philosophischer Grundbegriffe, 2011, Bd. 2, S. 1202; *Luhmann*, in: Marquard/Stierle (Hrsg.), Identität, 1979, S. 322 ff.
35 *Korsgaard*, Self-Constitution, 2009, S. 12.
36 *Dies.*, Self-Constitution, 2009, S. 19 f.
37 *Dies.*, Self-Constitution, 2009, S. 35–37.
38 *Dies.*, Self-Constitution, 2009, S. 42 f.
39 *Ricœur*, Oneself as another, 1994, S. 116; ebenso auf *Ricœur* abstellend, vgl. *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 81 f.

Charakter, der mediativ zwischen *Idem* und *Ipse* der Identität steht.[40] Mit dem dialektischen Verhältnis zwischen *Idem* und *Ipse* wird der bestehende Widerspruch zwischen statischer Gleichheit und dynamischer Selbstheit innerhalb einer personalen Identität aufgelöst.[41] Darin kommt die temporäre Dimension der personalen Identität zum Ausdruck, die sich dialektisch zwischen *Idem* und *Ipse* als Charakter bildet, und als temporäre Aktion der narrativen Identität in der kommunikativen Beziehung zur Außenwelt sichtbar wird.[42]

Mit der kommunikativen Beziehung wird ein *Agent als Bild der erscheinenden personalen Identität* begründet und für den Empfänger als eingegangenen Nachrichtengehalt erkennbar. Somit wird mit dem Agenten ein Zuschreibungsgegenstand geschaffen, der aus der Handlung und dem *Idem-Ipse*-Dialog besteht, womit im Rahmen der kommunikativen Beziehung eine Eigendynamik ausgelöst wird. Daraus können durch Zuschreibungen über die personale Identität weitere Attribute entstehen, die wiederum in das dialektische Verhältnis zwischen *Idem* und *Ipse* als Selbst und Ergebnis der reflexiven Äußerungen in Gestalt von Handlungen einfließen (Abbildung 1).[43]

Diese Annahmen dienen als philosophische Grundlage für die Modellbildung der Identitätsverwaltung, weshalb die Differenzierung zwischen dem *Idem-* und *Ipse*-Anteil einer personalen Identität im IKT-Recht eingeordnet werden soll. Denn mit einem Identitätsbegriff, der sich aus einer statischen und einer dynamischen Dimension zusammensetzt, lässt sich die Orientierung in den Regelungsbereichen zur Identität und des IKT-Rechts herstellen. Damit soll das grundrechtliche Schutzregime zur Identität herausgearbeitet und in die Modellbildung die differenzierten Ausprägungen des Identitätsbegriffs einbezogen werden.

40 *Ders.*, Oneself as another, 1994, S. 124.
41 *Ders.*, Oneself as another, 1994, S. 113 f.
42 *Ders.*, Oneself as another, 1994, S. 143.
43 *Ders.*, Oneself as another, 1994, S. 88, 122.

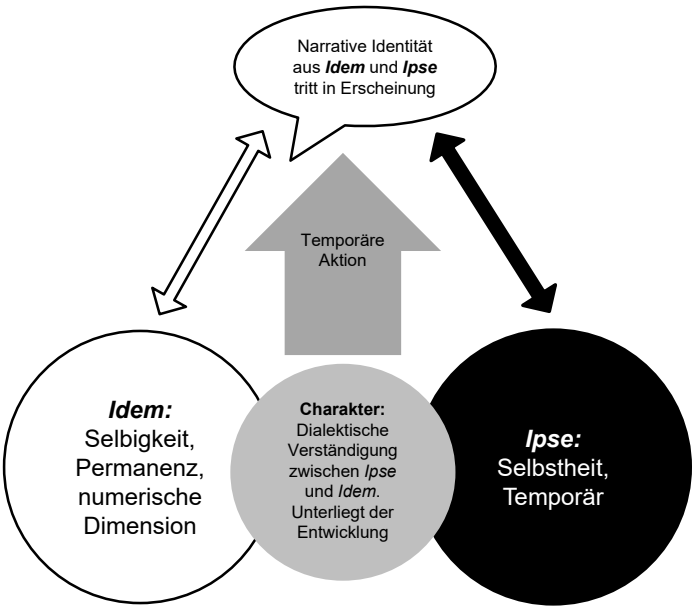

Abbildung 1: Modell zu Ricœur, „Oneself as another"[44]

III. Begründung einer regulierten mediativen Identitätsverwaltung

Die Identitätsverwaltung in IKT-Systemen könnte nach den vorgenommenen Darstellungen aus einer mediativen Identitätsverwaltung auf der Mikro- und Makroebene als ein Konzept des Selbstdatenschutzes bestehen, welches die Konzepte der *Idem*- und *Ipse*-Anteile implementiert. Mit der Prämisse eines kontextbezogenen Schutzes der personalen Identität geht es um ein ausgleichendes Schutzregime gegenüber bestehenden Informationsasymmetrien zwischen dem Verantwortlichen und Betroffenen auf der Mikro- und Makroebene.

Diese ausgleichenden Regelungsmöglichkeiten könnten auf der Mikroebene dynamisch in technischer Hinsicht ausgestaltet werden und als eine Erweiterung der bekannten informationstechnischen Berechtigungsverwaltung dienen. Die rechtlichen Anforderungen einer kontextangemessenen Identitätsverwaltung verlangen die Einbeziehung der Rechte aus dem

44 Modell orientiert an *ders.*, Oneself as another, 1994.

IKT-Recht, wozu die interoperable Ausgestaltung gehört, um die kontextübergreifende Kontrolle personaler Identitäten und die Entwicklungsbedingungen hinsichtlich des *Ipse*-Anteils zu ermöglichen. Dazu gehört ein Mechanismus, mit dem gegen diskriminierend wirkende Algorithmen auf personale Identitäten vorgegangen werden kann, was auf der rechtlichen und der technischen Ebene mit einem *„mechanism by design"* erfolgen könnte. Die Immunisierung der personalen Identität im online-Kontext würde auf der Mikroebene mit einem technischen Mediator als Vermittler erfolgen, der spieltheoretisch herzuleiten ist. Dieser würde in einem dialogischen Verfahren die Verhandlung der personalen Identitäten ermöglichen und den Schutz der *kontextuellen Integrität* gewährleisten.

Auf der Makroebene würde diese Identitätsverwaltung eine strukturelle Gewährleistung des dezentralen Identitätszugangs erfordern, mit dem die *personalen Identitäten kontrollierbar* wären. Dafür wird der Bedarf an einer erweiterten Transparenz als möglicher Lösungsmechanismus dargestellt, um strukturell einen Schutzmechanismus gegen die Intermediäre mit marktbeherrschender Stellung zu schaffen. Weiter kommt auf der Makroebene eine Plattform zur Identitätsverwaltung in Betracht, die als ein geschlossenes System zur kontextangemessenen Verwaltung personaler Identitäten fungiert. Somit ermöglicht eine mediative Identitätsverwaltung die Hinwendung zu einem differenzierten Ausgestaltungssystem für die private Datenverarbeitung als Erweiterung zur grundsätzlich bestehenden datenschutzrechtlichen Abwehrdimension. Darin lässt sich ein aktiver Gestaltungsmechanismus ausdrücken, in dem sich die Risiken der Datenverarbeitung im privaten Kontext abbilden lassen.

Mit der Förderung der Datenökonomie im europäischen Binnenmarkt bietet die europäische Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS-VO)[45] die Grundlage für ein europäisiertes interoperables Identitätsverwaltungsmodell. Darin kommt die Verwaltung der personalen Identitäten in Gestalt der *Idem*-Anteile zum Ausdruck, da die grenzüberschreitende Identifizierung für den elektronischen Rechtsverkehr geregelt wird. Dieses Konzept soll mit den datenschutzrechtlichen Maßgaben erweitert werden und Anhaltspunkte für eine mediative Identitätsverwaltung bieten. Damit wird ein Paradigmenwechsel in der Identitätsverwaltung nachgewiesen, der in einer Weiterentwicklung zu einer dynamischen Identitätsverwaltung über

45 Verordnung Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

die *Ipse*-Anteile der personalen Identität im online-Kontext liegt. Schließlich würde darin ein konkretes Modell zur Realisierung des Selbstdatenschutzes zum Ausdruck kommen.

D. Gang der Untersuchung

Der Untersuchungsgegenstand zielt insofern auf die Modellbildung für eine soziotechnische Identitätsverwaltung ab, die als ein Konzept im Selbstdatenschutz fungiert und dem dialogisch geprägten Identitätsbegriff in seinen *Idem*- und *Ipse*-Anteilen Rechnung trägt. Für die Modellbildung bedarf es zunächst der Bestimmung grundrechtlicher Anforderungen an den Schutz der Identität als Fundament für die Ausgestaltung der Identitätsverwaltung und zur Stärkung des Selbsdatenschutzes. Die Realweltphänomene der personalen Identität sind dabei in ihren einfachrechtlichen Schutzbedarfen im offline- und online-Kontext gleichermaßen abzubilden.

Demnach werden die *Grundlagen der Identitätsverwaltung* für die Modellbildung im 2. Teil der Untersuchung aus den Grundrechten abgeleitet, die mit der Einordnung des Schutzes der personalen Identität in der europäischen Grundrechtecharta aus Art. 7, 8 GRC beginnt und bereits ein Modell für die Identitätsverwaltung aufweisen könnte. Danach wird die personale Identität in ihrer inneren Dimension mit dem Recht auf Achtung des Privatlebens etwa durch Kenntnis der Abstammung geschützt und in der äußeren Dimension wird der persönliche Reputationsschutz als Kontrollmöglichkeit über die Selbstdarstellung gemäß Art. 7, 8 GRC nachvollzogen. Daneben werden die Dimensionen zum Schutz der personalen Identität von den Grundrechten des allgemeinen Persönlichkeitsrechts und der allgemeinen Handlungsfreiheit flankiert. Damit soll die grundrechtliche Gewährleistung der Persönlichkeitsentwicklung für den online-Kontext aufgezeigt werden, was die Differenzierung der *Idem*- und *Ipse*-Anteile einer personalen Identität in dem Modell nach *Ricœur* einbezieht.

Ergänzend wird das liberal geprägte Privatheitskonzept des angloamerikanischen Rechtsraumes einbezogen, da die wellenförmige Beeinflussung

der Rechtskulturen[46] der Erweiterung des Betrachtungsspektrums dient[47] und Anhaltspunkte für ein ausgleichendes Schutzregime für die personale Identität gewonnen werden können. Gleichzeitig wird eine fachübergreifende Perspektive zur personalen Identität einbezogen, da der Identitätsbegriff in seinem konkreten Bedeutungsgehalt erheblich von der Betrachtungsperspektive abhängt. Zudem sollen in Anbetracht der Rechtswissenschaft als disziplinäres Cluster[48] die informationstechnische, die psychologische und die kommunikationspsychologische Perspektive in die Untersuchung einbezogen werden. Damit werden die Ergebnisse aus der grundrechtlichen Betrachtung um weitere Fundierungen ergänzt, um die Voraussetzungen für die Modellbildung konkretisieren zu können. Maßgeblich ist dabei der Nachweis, dass die *Instruktion* innerhalb eines Kommunikationsprozesses auf der Metaebene als Schutzmechanismus in das Modell der Identitätsverwaltung einzubeziehen ist.

Mit diesen grundlegenden Feststellungen sollen im 3. Teil der Untersuchung die Anforderungen an das Modell der Identitätsverwaltung in einfachrechtlichen Typologien aus der Realwelt konkretisiert und die Anknüpfung an den Namen für die Zuordnung der Identität in ihrem *Idem*-Anteil zum Individuum vorgenommen werden. Der Name als Identifizierungsgrundlage im elektronischen Rechtsverkehr wird dabei einbezogen und gemäß Art. 8 Abs. 2 eIDAS-VO[49] das *dreistufige Vertrauens- und Sicherheitsniveau* für eine kontextangemessene Identifizierung vorgestellt, welches als Grundlage für die Beschreibung der Modellanforderungen an eine interoperable und kontextangemessene Identitätsverwaltung dient. Neben der Identifizierung mit dem *Idem*-Anteil einer personalen Indentität wird aufgezeigt, dass im elektronischen Rechtsverkehr die vertrauliche sichere Kommunikation nach dem De-Mail-G ebenfalls geschützt ist.

Mit dieser dynamischen Dimension der Kommunikation kommt der Datenzyklus über eine personale Identität zum Ausdruck. Dieser soll eben-

---

46 *Whitman*, Yale L. J. 2004, 1151 (1158 f., 1203), der die wechselseitigen Beeinflussungen der Rechtskulturen am Schutz der Privatheit beschreibt. Weiter wird auf die Wahrnehmungen und Perspektiven aus den Rechtskulturen abgestellt, wonach etwa aus der angloamerikanischen Perspektive das deutsche Meldewesen als hochgradig freiheits- und privatheitsbeschränkend wirken kann.

47 *Kischel*, Rechtsvergleichung, 2015, § 1 Rn. 16.

48 *Jestaedt*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, S. 110.

49 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.

falls als Kontrollgegenstand eingeordnet werden und führt zu der Darstellung des Erkenntnismodells über Daten, Informationen und Wissen. Anschließend wird die Differenzierung zwischen der relativen Kontrolle von Erkenntnissen aus der Kommunikation und der absoluten Kontrolle als Zugangsrecht zur personalen Identität vorgenommen. Weiter ist die Handlungsträgerschaft über die Bilder personaler Identitäten als Grundlage für die Modellbildung heranzuziehen. Sie wird in einer Prinzipal-Agenten-Beziehung dargestellt, in der die Agenten als Handlungsträger über die personale Identität fungieren.

Im 4. Teil wird das Identitätsverwaltungsmodell auf der Grundlage des IKT-Rechts begründet und die DSGVO einer chronologischen Betrachtung des Datenzyklus *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung unterzogen. Dafür wird das begründete stipulative Identitätsverwaltungsmodell mit den *Idem*- und *Ipse*-Anteilen der Identität herangezogen, um dieses dem Regelungsregime des IKT-Rechts gegenüberzustellen und das bestehende IKT-rechtliche Identitätsverwaltungsmodell herauszuarbeiten. Dabei wird nachgewiesen, dass die erste Kontrollmöglichkeit über die Informationspflichten gemäß Art. 12, 13 DSGVO besteht und auf dieser Grundlage eine risikobewußte Entscheidung von dem Betroffenen möglich wird, was die Frage nach der Risikobewertungsmethode aufwirft.

Weiter gilt die Einwilligung gemäß Art. 6 Abs. 1 a) DSGVO als maßgebliche Kontrollmöglichkeit des Betroffenen, so dass diese einer näheren Betrachtung unterzogen und die rechtswissenschaftliche Subdisziplin der Verhaltensökonomik[50] einbezogen wird. Damit soll eine mögliche „Kluft zwischen Sein und Sollen“[51] identifiziert werden und in einen effektiven Schutzmechanismus bei der Modellbildung überführt werden. Daneben werden die bereichsspezifischen Datenschutzregeln im TMG und TKG in die Modellbildung einbezogen, solange sich die EPrivacy-VO[52] noch im Entwurfsstadium befindet. Nach den Analysen des IKT-Rechts wird ein *iteratives Verhandlungssystem* zwischen Verantwortlichem und Betroffenen be-

50 *Van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (189).

51 *Grimm*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 21 (24).

52 Vorschlag für eine Verordnung des europäischen Parlamentes und Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM/2017/010 final, 2017/03.

gründet, welches dem statischen *Idem*-Anteil und dynamischen *Ipse*-Anteil einer personalen Identität Rechnung trägt und übergeordnete *Instruktionen* über die personalen Identitäten ermöglicht. Dieses Verfahren lässt sich über ein technisches *Dashboard-System* abbilden, das über den gesamten Datenzyklus hinweg die IKT-rechtlichen Schutzmechnismen und einen Zugang zu den personalen Identitäten gewährleisten könnte. Die Identitätsverwaltung über ein *Dashboard-System* wird somit als ein *Metaverfahren* mit einer interoperablen Struktur über die kontextspezifischen personalen Identitäten hergeleitet.

Mit der *spieltheoretischen Perspektive* im 5. Teil soll die Identitätsverwaltung als Metaverfahren konkretisiert werden, indem die IKT-rechtlich fingierten Handlungen spieltheoretisch modelliert und die strukturellen Wirkmechanismen im IKT-Recht aufgezeigt werden. Sobald die Anreizmechanismen für die ökonomisch motivierten Entscheidungen im IKT-Recht bestimmt werden, lässt sich daraus ein Lösungsmechanismus zum Schutz der personalen Identität ableiten, was mit dem spieltheoretisch begründeten Konzept der mediativen Identitätsverwaltung vorgesehen ist. Dafür wird die Bestimmung des öffentlichen Gutes der persönlichen Informationen als Verhandlungsgegenstand zwischen Betroffenen und Verantwortlichem vorgenommen, da die personale Identität sich aus persönlichen Informationen zusammensetzt. Weiter wird die Strategiewahl, basierend auf dem IKT-Recht, in eine defektive und kooperative Handlungsmöglichkeit unterteilt, damit die Untersuchung der Handlungsauswirkungen auf das öffentliche Gut der persönlichen Informationen folgen kann. Daraus wird ein datenschutzrechtlicher „*Market for Lemons*" nachvollzogen, der in einer gesteigerten Marktpräsenz von Diensten mit einem niedrigen Datenschutzniveau besteht und sich nachteilig auf das öffentliche Gut der persönlichen Informationen auswirkt. Folglich wird die für das öffentliche Gut schonende „*TIT for TAT*"-Strategie aufgezeigt, die der Begründung eines technischen Mediationsagenten dient. Damit wird ein „*mechanism by design*" hergeleitet, der im Datenzyklus dem Schutz der persönlichen Informationen dient und eine risikomindernde Wirkung entfaltet. Ein Gesamtkonzept der mediativen Identitätsverwaltung könnte die *iterative Verhandlung* der personalen Identitäten ermöglichen und als datenschutzrechtliche Technikanforderung gemäß Art. 25 DSGVO umgesetzt werden.

Daraus wird in dem 6. Teil ein Modell der Identitätsverwaltung gebildet, welches die Vielfältigkeit der personalen Identität in den online-Kontext von IKT-Systemen überträgt und die *Idem*- und *Ipse*-Anteile der personalen Identität zu einem Kontrollgegenstand werden lässt. Demnach wird aus den beschriebenen Realphänomenen und dem IKT-Recht ein Paradigmen-

wechsel von der Berechtigungsverwaltung zur Kontrolle über den Identitätszugang aufgezeigt, der eine Abkehr von einem statischen Identitätsbegriff bedeutet und die *iterative Verhandlungsmöglichkeit* von personalen Identitäten im online-Kontext einräumt. Weiter wird nachgewiesen, dass die Voraussetzungen für ein Identitätsverwaltungsmodell kontextspezifisch, dezentral und mit einer dialogischen Verhandlungsmöglichkeit abzubilden sind, wofür ein *Dashboard-System* als geeignet erscheint. Dieses soll in seiner Funktionalität den Zugang zu den personalen Identitäten und den Zugang zu einem *iterativen Verhandlungsverfahren* über die personalen Identitäten ermöglichen. Weiter wird die Plattform für die Identitätsverwaltung dargestellt, die als ein geschlossenes System zur Verwaltung der *Idem-* und *Ipse-*Anteile einer personalen Identität im online-Kontext funktionieren würde.

Inwieweit die Modellvoraussetzungen einen eigenständigen soziotechnischen Regelungsbedarf auslösen, wird im 7. Teil vorgestellt und ist Gegenstand der abschließenden Analysen. Diese führen zu der einfachrechtlichen Anforderung, dass die *„privacy by design"*-Regelung gemäß Art. 25 DSGVO mit einer ausdrücklichen *„identity management by design"*-Anforderung erweitert werden sollte. Ferner könnte sich eine einfachrechtliche Regelung an den Hersteller richten und das Produkthaftungsrecht um den Schutz der informationellen Selbstbestimmung erweitert werden. Schließlich wird ein prinzipienbasierter Ansatz zur Implementierung eines Schutzkonzeptes der verhandlungsfähigen Identität im online-Kontext begründet, der als konsequentes Schutzregime für die personale Identität aus den Grundrechten fungiert.

2.Teil: Grundlagen der Identitätsverwaltung

Die Grundlagen für ein Identitätsverwaltungsmodell setzen die rechtliche Bestimmung des zentralen Begriffs der personalen Identität für die Modellbildung voraus. Dafür bedarf es der grundrechtlichen Einordnung des Schutzgegenstandes der personalen Identität und der Ableitung der Identitätsverwaltung aus den Grundrechten. Demnach werden diese Begriffe in der europäischen Grundrechtecharta und in den Grundrechten nachvollzogen, was als Grundlage für die Modellbildung dient (A.). Weiter werden diese Grundrechtsregime für die *Modellbildung der Identitätsverwaltung* entscheidend sein und sollen mit einer fachübergreifenden Perspektive ergänzt werden. Damit soll der Identitätsbegriff eine weitere Differenzierung erfahren und es sollen konkrete Anhaltspunkte für ein wirksames Schutzregime zur Identitätsverwaltung aufgezeigt werden (B.). Denn mit der fachübergreifenden Gesamtbetrachtung lassen sich Lösungsmechanismen herleiten, die sich in ein Modell der Identitätsverwaltung mit einem effektiven Schutz für die personale Identität überführen lassen. Abschließend wird der Identitätsbegriff in seiner statischen und dynamischen Dimension mit den Grundrechten in Verbindung gebracht, so dass die *Idem*- und *Ipse*-Anteile der personalen Identität vom grundrechtlichen Schutz erfasst werden (C.).

A. Personale Identität in den Grundrechten

Der Begriff der personalen Identität als zentrales Element der Identitätsverwaltung bedarf der grundrechtlichen Bestimmung in seinem Umfang und in seinen Funktionalitäten, um die Grundlagen für ein Identitätsverwaltungsmodell im IKT-Recht abbilden zu können und Maßstäbe für die einfachrechtliche Auslegung zu gewinnen. Dafür ist neben den europäischen Grundrechten das Grundgesetz für die Begriffsbestimmung maßgeblich und soll mit einem Einblick in die angloamerikanische Verfassungsgebung ergänzt werden.

Auch wenn sich die Auslegung der DSGVO an der europäischen Grundrechtecharta zu orientieren hat, soll im Gang dieser Arbeit die nationale grundrechtliche Betrachtung ebenfalls einbezogen werden. Dies dient der historischen Entwicklung eines grundrechtlich geprägten Begriffs der per-

sonalen Identität und als weitere Interpretation eines möglicherweise noch im Entstehen befindlichen europäischen Schutzes der informationellen Selbstbestimmung.

Weiter fallen nationale datenschutzrechtliche Sachverhalte nach der DSGVO gemäß Art. 52 GRC in den Anwendungsbereich des Gemeinschaftsrechts und damit unter die europäische Grundrechtecharta. Gleichwohl können die nationalen Grundrechte bei einem niedrigeren Schutzniveau der europäischen Grundrechecharta direkten Schutz für das Individuum entfalten.[53] Dies könne bereits deshalb angenommen werden, weil die europäische Grundrechtecharta keine Verfassungsbeschwerde vorsieht und der Einzelne aufgrund einer fehlenden individuellen Beschwerdemöglichkeit vor dem europäischen Gerichtshof (EuGH) einem geringeren Schutzniveau unterliege.[54] Auch wird von *Britz* betont, dass der EuGH bislang den nationalen Gerichten in den Mitgliedstaaten die datenschutzrechtlichen Entscheidungen zur Konfliktlösung im Wesentlichen überlassen habe.[55] Entsprechend wurde nunmehr vom Bundesverfassungsgericht in den Entscheidungen „Recht auf Vergessen I & II" das Verhältnis der europäischen Grundrechtecharta zum Grundgesetz dahingehend klargestellt, dass die Auslegung der Grundrechte im Licht der Grundrechtecharta zu erfolgen habe und damit die Einhaltung des unionsrechtlichen Schutzniveaus ermöglicht werde.[56] Gleichzeitig wird durch das Unionsrecht der Rahmen für die nationale Grundrechtsauslegung gelegt, der im Einzelnen weiterhin Gestaltungsspielräume für die Mitgliedstaaten vorsieht, damit die mitgliedstaatlichen Gerichte auf die Integration des Unionsrechts in den nationalen Grundrechtsauslegungen hinwirken können.[57]

Demnach soll die Bestimmung des grundrechtlichen Schutzregimes der personalen Identität zunächst auf der Ebene der europäischen Grundrechtecharta (I.) erfolgen und mit den nationalen Grundrechten (II.) fortgesetzt werden. Schließlich wird der amerikanische Verfassungsansatz für die Modellbildung (IV.) herangezogen, damit weitere Anhaltspunkte für ein Identitätsverwaltungsmodell herausgearbeitet werden können.

53 BVerfGE 73, 339 – Solange II.
54 *Grimm*, JZ 2013, 585 (592).
55 *Britz*, EuGRZ 2009, 1 (11).
56 BVerfG, Urt. v. 09.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 60, 67.
57 BVerfG, Urt. v. 09.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 50–53; BVerfG, Urt. v. 09.11.2019, 1 BvR 276/17, Recht auf Vergessen II, Rn. 63.

I. Personale Identität in der Europäischen Grundrechtecharta

1. Schutz personenbezogener Daten, Art. 8 GRC

a) Personale Identität in der Schutzfunktion des Art. 8 Abs. 1 GRC

Dem Wortlaut des Art. 8 Abs. 1 GRC nach hat die Person ein Recht auf den Schutz der sie betreffenden personenbezogenen Daten. Weiter geht aus ihm hervor, dass es sich um ein „Recht" über den Schutz der personenbezogenen Daten einer betroffenen Person handelt. Dies kann dahingehend gelesen werden, dass diese personenbezogenen Daten im Zusammenhang mit der „Identität" stehen und eine Einflussmöglichkeit auf den Schutz der Identität bestehen soll, was sich aus dem Begriff „Recht auf Schutz" ableiten lässt. Diese Bewertung ist gestützt auf die historische Diskussion, nach der ein Datenschutz gewährleistet werden solle, bei dem es um die „Selbstbestimmung des Einzelnen über seine Daten" gehe.[58] Weiter lässt sich dies mit dem im Konvent diskutierten Formulierungsvorschlag, „Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu *bestimmen* und Auskunft über die Verwendung zu erlangen, soweit nicht Rechte Dritter entgegenstehen", bestätigen.[59] Mit dem Wortlaut der „Bestimmung" über die „eigenen" Daten ließe sich ein Konzept ableiten, welches dem Individuum eine Einflussmöglichkeit über „seine" personenbezogenen Daten einräumt. Der Ursprung dessen liegt in der „Autonomie und Menschenwürde als gemeinsame(r) Fluchtpunkt".[60] Denn von dem Schutzbereich des Art. 8 Abs. 1 GRC sind personenbezogene Daten im öffentlich-rechtlichen und im privatrechtlichen Kontext gleichermaßen erfasst. Zudem wurde im Konvent der Aspekt der (informationellen) Selbstbestimmung als Schutzgegenstand des Art. 8 GRC anerkannt.[61]

Der Schutzbereich des Art. 8 Abs. 1 GRC richtet sich auf personenbezogene Daten, die sich aus dem sekundären Gemeinschaftsrecht der Richtlinie 95/46/EG ableiten lassen,[62] so dass der Schutzbereich eröffnet ist, wenn

---

58 *Bernsdorff/Borowsky*, Die Charta der Grundrechte der Europäischen Union, 2002, S. 195.
59 *Dies.*, Die Charta der Grundrechte der Europäischen Union, 2002, S. 196.
60 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 93.
61 *Bernsdorff*, in: Meyer/Bernsdorff (Hrsg.), Charta der Grundrechte der Europäischen Union, 42014, Art. 8 GRC Rn. 6 f.
62 *Ders.*, in: Meyer/Bernsdorff (Hrsg.), Charta der Grundrechte der Europäischen Union, 42014, Art. 8 GRC Rn. 20.

Informationen über eine bestimmte oder bestimmbare natürliche Person betroffen sind, mit denen die Person direkt oder indirekt identifiziert werden kann. Dazu werden etwa der Personalausweis, ein Konto, eine Telefonnummer oder Elemente, die *Ausdruck* der physischen, kulturellen oder sonstigen Identität sind, genannt.[63] Aus dieser Einbeziehung des sekundärrechtlichen Wortlautes aus Art. 2 a) Richtlinie 95/46/EG und Art. 4 Nr. 1 DSGVO in die Bestimmung des grundrechtlichen Schutzbereichs geht hervor, dass in dem Schutz der personenbezogenen Daten zugleich der Schutz der physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität liegt. Weiter wird von *Marsch* hervorgehoben, dass es sich bei der Begrifflichkeit der personenbezogenen Daten um eine handelt, die „schutzmaximierend" auf der Ebene des Art. 8 GRC ausgelegt werden könne und eine Konkretisierung des Begriffsumfangs der Gegenstand sekundärrechtlicher Rechtsauslegung sei.[64] Damit kommt dem Meinungsstreit, unter welchen Kriterien eine Identitifizierbarkeit der natürlichen Person vorliegt, eine schutzbereichsbegründende Bedeutung zu. Ebenso enthält die Begrifflichkeit der personenbezogenen Daten eine kommunikative Dimension. Diese lässt sich aus dem Wortlaut der Verfassungen neuer Mitgliedstaaten[65] entnehmen, bei denen sich das Schutzgefüge über das Privatleben hinaus auf die Kommunikation erstreckt und ein eigenständiges Datenschutzgrundrecht begründet wurde.

Weiter ist im Schutzumfang ausdrücklich die Einbeziehung neuer technischer Entwicklungen vorgesehen, denn Art. 8 GRC sei als „innovatives Grundrecht" ausgestaltet, das künftige technologische Entwicklungen einbeziehe.[66] Daher erstreckt sich der Schutz personenbezogener Daten auf ihren kommunikativen Zusammenhang gerade beim Einsatz neuer Technologien. Insoweit ist der Schutzbedarf über personenbezogene Daten als „Ausdruck einer Identität" gemäß Art. 4 Nr. 1 DSGVO ohne einen technischen Kommunikationsvorgang kaum denkbar. Folglich sind personenbezogene Daten als Ausdruck einer Identität in verschiedenen technischen

63 *Jarass*, Kommentar, Charta der Grundrechte der EU, 2016, Art. 8 GRC Rn. 5.

64 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 146.

65 *Bernsdorff*, in: Meyer/Bernsdorff (Hrsg.), Charta der Grundrechte der Europäischen Union, 2014, Art. 8 GRC Rn. 3 mit Verweis auf die Verfassungen in Polen, Kroation, Slowakei, Slowenien und Ungarn, die ein eigenständiges Datenschutzgrundrecht vorsehen.

66 *Ders.*, in: Meyer/Bernsdorff (Hrsg.), Charta der Grundrechte der Europäischen Union, 2014, Art. 8 GRC Rn. 12; *Knecht*, in: Schwarze/Becker/Hatje u.a. (Hrsg.), EU-Kommentar, 2019, Art. 8 GRC Rn. 1; *González Fuster*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, S. 264.

Ausprägungen und kommunikativen Anwendungsfeldern von dem Schutzbereich des Art. 8 GRC erfasst.

Die Schutzfunktion aus Art. 8 Abs. 1 bezieht sich demnach auf die einfachrechtlich zu bestimmenden personenbezogenen Daten und die damit verbundenen Ausdrucksformen der personalen Identitäten, wie sie sich aus Art. 4 Nr. 1 DSGVO ergeben. Dabei wird in der Literatur der technische Kommunikationsvorgang als Schutzgegenstand einbezogen, wozu gerade neue Technologieentwicklungen gehören.

b) Personale Identität in der Ausgestaltungsdimension des Art. 8 Abs. 2 GRC

Der Schutz personenbezogener Daten erfährt über Art. 8 Abs. 2 S. 1 GRC Konkretisierungen unter denen Daten verarbeitet werden dürfen. Über Art. 8 Abs. 2 S. 2 GRC wird das Recht auf Erwirkung der Auskunft und der Berichtigung eingeräumt. Der Wortlaut des Art. 8 Abs. 2 GRC legt eine bindende Ausgestaltungspflicht über das „Recht auf Schutz" zu Grunde, die über das Sekundärrecht eine Konkretisierung und Eingrenzung im Rahmen des gesetzgeberischen Einschätzungsspielraums erfährt.[67] Dazu gehört, dass gemäß Art. 8 Abs. 2 S. 1 GRC die Zweckfestlegung nach Treu und Glauben primärrechtlich geregelt wird, wodurch dieser Schutzmechanismus eine gesteigerte Bedeutung erlangt. Von dem Grundsatz der Zweckfestlegung nach Treu und Glauben ist umfasst, dass der Zweck legitim sein muss und auch als *Schutz gegen Diskriminierungen* dient.[68] Weiter gehört zu der primärrechtlichen Zweckfestlegung und dem Grundsatz Treu und Glauben die Kompatibilität des ursprünglichen Zwecks mit einem im Datenzyklus geänderten Zweck, Art. 6 Abs. 4 DSGVO, EWG 50. Denn ein im Rahmen des Datenzyklus geänderter Zweck unterliegt der ursprünglich vorgenommenen Rechtfertigung, die bei einer Vereinbarkeit mit dem ursprünglichen Zweck kontinuierlich fortwirkt.

Erst mit der Zweckfestlegung nach Treu und Glauben ist die Bewertung der Rechtmäßigkeit möglich, da sich die Einwilligung, die Erforderlichkeit und das berechtigte Interesse nach dem Zweck der Verarbeitung richten. Dem übergeordneten Grundsatz von Treu und Glauben kommt dabei ein prozeduraler Charakter zu, mit dem die Transparenz über die Datenverarbeitung und das Vertrauen in eine erwartbare Weiterverarbeitung gewähr-

67 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 130 f.
68 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 156.

leistet werden sollen.[69] Darin sind die Rahmenbedingungen für die Verarbeitung von personenbezogenen Daten einer personalen Identität geregelt, indem über den Grundsatz Treu und Glauben die prozedurale Aufrechterhaltung des Schutzes der personalen Identität gesichert werden kann.

Eine weitere Stärkung erfährt die Ausgestaltung der Verarbeitung personenbezogener Daten durch die Auskunfts- und Erwirkungsrechte nach Art. 8 Abs. 2 S. 2 GRC, die als grundrechtsunmittelbare Rechte wichtige Instrumente der Kontrolle über die personenbezogenen Daten[70] und damit der personalen Identitäten sind. Diese Rechte fungieren als grundrechtsunmittelbare Leistungsrechte, die dem Betroffenen ein Auskunftsrecht als Transparenzoption über die Datenverarbeitung und ein Berichtigungsrecht einräumen.[71] Dabei gilt das Berichtigungsrecht gemäß Art. 8 Abs. 2 S. 2 GRC als exemplarischer Sammelbegriff für das Recht auf Sperrung und Löschung der Daten.[72] Aus diesen primärrechtlich verankerten Leistungsrechten geht die Wertung hervor, dass dem Betroffenen über den Datenzyklus hinweg eine Kontrollmöglichkeit eingeräumt werden muss und es ihm ermöglicht wird, korrigierend in unerwünschte Ausprägungen personaler Identitäten einzugreifen. Darin kommt ein maßgebliches Schutzregime für die Identitätsverwaltung zum Ausdruck, welches über die rechtfertigende Einwilligung hinaus zu einem späteren Zeitpunkt im Datenzyklus die Betroffenenrechte einräumt. Dem Betroffenen wird somit die Ausgestaltung seines dynamischen *Ipse*-Anteils ermöglicht, der im Laufe des Datenzyklus unterschiedlichen Risiken unterliegt und eine angepasste Kontrollmöglichkeit verlangt. Diese lässt sich im Rahmen des Selbstdatenschutzes mit der Ausübung der Betroffenenrechte und insbesondere mit der Transparenz über die vollzogene Datenverarbeitung realisieren.

Mit der primärrechtlichen Verankerung der Betroffenenrechte wird ein ausgeprägtes Schutzniveau geschaffen, welches eine restriktive Auslegung etwa des Auskunftsrechts auf der sekundärrechtlichen Anwendung verbiete.[73] Zudem verlangt der gemeinschaftsrechtliche Grundsatz des *effet utile* diejenige Auslegung, die dem Gemeinschaftsrecht zu einer effektiven Anwendung verhilft. Ebenso stellt das Recht auf Überwachung durch eine unabhängige Stelle nach Art. 8 Abs. 3 GRC sicher, dass die primär- und se-

69 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 174 f.
70 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 278.
71 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 230.
72 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 231.
73 *Reinhardt*, AöR 142 (2017), 528 (543).

kundärrechtlichen Vorgaben umgesetzt und angewendet werden. Damit ist ein weiterer Schutzmechanismus zur Wahrung der Effektivität der Rechtsvorgaben vorgesehen, so dass etwa beim Ausbleiben der aufsichtsrechtlichen Prüfung einer Beschwerde ein Verstoß gegen Art. 8 Abs. 3 GRC vorliegen kann.[74] Dieser grundrechtliche Schutzmechanismus gewährleistet eine ausdifferenzierte Sicherstellung über den Bestand der personalen Identität im Datenzyklus und ermöglicht einen wirksamen Selbstdatenschutz.

2. Kombinationsgrundrecht aus Art. 7, 8 GRC

Bei der Bestimmung des Begriffs der personalen Identität sind zugleich die Schutzbereiche über die Achtung des Privatlebens und den Schutz personenbezogener Daten betroffen, Art. 7, 8 GRC. Daraus ergibt sich der Bedarf, das Kombinationsgrundrecht als Grundlage eines Identitätsverwaltungsmodells einer genaueren Analyse zu unterziehen. In systematischer Hinsicht wird Art. 8 GRC als *lex specialis* gegenüber Art. 7 GRC gesehen.[75] Da aber gleichzeitig beide Rechte fundamentalen Charakter haben und miteinander in komplexer Beziehung stehen,[76] kann ein eigenständiger Schutzgehalt aus den Grundrechten gemeinsam abgeleitet werden. Dabei ist für den Schutz gemäß Art. 8 GRC nicht zwingend der Bezug zum Privatleben erforderlich, da etwa eine rechtswidrige Datenverarbeitung noch keinen Verstoß gegen das Privatleben darstellen muss und daher Art. 8 GRC einen zusätzlichen Schutz gegenüber dem Schutzumfang von Art. 7 GRC entfaltet.[77]

Das Kombinationsgrundrecht legt einen Vergleich mit dem Recht auf informationelle Selbstbestimmung nahe, welches von *Marsch* aber wegen der Gefahr einer pfadabhängigen Orientierung an dem Recht auf informationelle Selbstbestimmung infrage gestellt wird.[78] Zwar werde in der

74 *Jarass*, Kommentar, Charta der Grundrechte der EU, 2016, Art. 8 GRC Rn. 18.
75 *Knecht*, in: Schwarze/Becker/Hatje u.a. (Hrsg.), EU-Kommentar, 2019, Art. 7 GRC Rn. 7; *Bernsdorff*, in: Meyer/Bernsdorff (Hrsg.), Charta der Grundrechte der Europäischen Union, 2014, Art. 8 GRC Rn. 13.
76 *González Fuster*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, 2014, S. 256, 266–271. In der konstatierten Überschneidung zwischen dem Schutz des Privatlebens und dem Schutz personenbezogener Daten wird eher eine Illusion als ein Faktum gesehen.
77 *Britz*, EuGRZ 2009, 1 (8); *Kokott/Sobotta*, IDPL 2013, 222 (223).
78 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 82.

Rechtsprechung des EuGH ein umfassender Schutz personenbezogener Daten aus Art. 8 GRC abgeleitet, aber daraus könne kein Recht, über die Preisgabe und Verwendung personenbezogener Daten selbst zu entscheiden, abgeleitet werden.[79] Folglich kann die hohe Differenziertheit des Rechts auf informationelle Selbstbestimmung und der Schutz bereits bei einer *abstrakten Gefährdungslage* nicht auf das Kombinationsgrundrecht übertragen werden. Vielmehr ergibt sich aus Art. 7, 8 GRC das Erfordernis eines *qualifizierten Gefährdungspotentials*. Daneben werden sekundärrechtliche Ausgestaltungsspielräume eingeräumt. Demnach sind Datenverarbeitungen mit einem geringen Gefährdungspotential nicht vom Schutzbereich des Art. 7, 8 GRC erfasst, sondern unterliegen dem sekundärrechtlichen Schutz, womit eine Innovationsoffenheit gewährleistet werde.[80]

Bei der Bildung des Identitätsverwaltungsmodells wirkt sich dieses weniger differenzierte Schutzniveau aus Art. 7, 8 GRC im Vergleich zum Recht auf informationelle Selbstbestimmung jedoch nicht aus, da die personenbezogenen Informationen über die personalen Identitäten als Schutzgegenstand und als Anknüpfungspunkt für die Modellbildung gelten. Insoweit wird der jeweilige Schutz bei einer abtrakten und einer *qualifizierten Gefährdungslage* zwar anerkannt, dieser würde sich jedoch auf der Ebene der Risikobewertung einer Datenverarbeitung auswirken. Somit soll im Folgenden zur Beschreibung des grundrechtlichen Schutzes der personalen Identitäten aus dem Kombinationsgrundrecht gemäß Art. 7, 8 GRC die Begrifflichkeit der informationellen Selbstbestimmung verwendet werden.

Mit der Annahme eines engen Schutzbereiches aus Art. 7, 8 GRC und einem ausdifferenzierten Schutzregime auf der sekundärrechtlichen Ebene lässt sich für die *Modellbildung der Identitätsverwaltung* ableiten, dass den sekundärrechtlichen Maßgaben ein hohes Gewicht beizumessen ist. Weiter sind aus dem Schutz des Privatlebens ebenso Anforderungen für die Modellbildung abzuleiten (a) und im Rahmen der abwehrrechtlichen Schutzdimension aus Art. 7, 8 GRC (b) zu konkretisieren.

79 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 209 f.
80 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 211 f.

a) Personale Identität als Schutzgegenstand des Privatlebens, Art. 7 GRC

Aus den vier[81] geregelten Schutzbereichen in Art. 7 GRC sollen vorliegend die Achtung des Privatlebens und der Kommunikation für die Bestimmung der personalen Identität maßgeblich sein. Das Privatleben nach Art. 7 GRC umfasse im Gegensatz zu Art. 8 GRC den Schutz von Informationen zum Privatleben und weniger die Daten mit dem Prozess der Selbstbestimmung, wie er aus dem deutschen Recht auf informationelle Selbstbestimmung bekannt ist.[82] Das Recht auf Achtung des Privatlebens soll folgend in seinen Funktionen und Ausprägungen dargestellt werden.

Die Achtung des Privatlebens steht in Abgrenzung zum öffentlichen Leben und soll dabei den privaten Bereich vor Einblicken und Einwirkungen von außen schützen, was den Schutz der Selbstbestimmung und der Handlungen im Privatleben umfasst.[83] Die innere Dimension des Privatlebens betrifft den Schutz privater Entscheidungen und die äußere Dimension betrifft das dazugehörige erkennbare Verhalten, wie es etwa bei der sexuellen Selbstbestimmung und der damit verbundenen äußerlich erkennbaren Partnerwahl der Fall ist.[84] Dabei ist das Verhalten des Grundrechtsträgers in seiner Privatheit auch an die Kontrolle über die Örtlichkeit gebunden, so dass die konkrete Bestimmung der Grenzen von Privatheit und Öffentlichkeit kontext- und ortsabhängig ist. Im Kern des Begriffs „Privatleben" würde damit die innere Dimension stehen, die eigene Identität selbst zu bestimmen und zu konstituieren, so dass es um den Schutz der Identitätsbildung ginge.[85] Somit wird aus dem Begriff der Privatheit ein Konzept der Kontrolle über die Sammlung und Offenlegung von Informationen angenommen, wohingegen der Begriff der Identität auf die Anerkennung der „Gleichheit" von Name und Individuum und der Einmaligkeit des Individuums abstellt. Dies geht auch aus dem im Konvent beratenen Wortlaut, „Jeder hat das Recht auf [...] individuelle Einmaligkeit", hervor.[86] Darin ist die Intention erkennbar, dass der Individualität in ihren *Ipse*-Anteilen einer personalen Identität und der Einmaligkeit einer Person in ihrem

81 *Knecht*, in: Schwarze/Becker/Hatje u.a. (Hrsg.), EU-Kommentar, 2019, Art. 7 GRC Rn. 7.
82 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 77 f.
83 *Jarass*, Kommentar, Charta der Grundrechte der EU, 2016, Art. 7 GRC Rn. 13 f.
84 *Ders.*, Kommentar, Charta der Grundrechte der EU, 2016, Art. 7 GRC Rn. 15.
85 *Weber*, in: Stern/Sachs (Hrsg.), Europäische Grundrechte-Charta, 2016, Art. 7 GRC Rn. 1 f., 9.
86 *Bernsdorff/Borowsky*, Die Charta der Grundrechte der Europäischen Union, 2002, S. 154 f.

Idem-Anteil der personalen Identität Rechnung getragen werden soll. Demgegenüber wurde der Vorschlag diskutiert, den Begriff der „Identität" in den Wortlaut aufzunehmen, da mit diesem der Schutz „individueller Einmaligkeit" und die mögliche Ausprägung der „kulturellen Identität" umfasst sei.[87] Insbesondere aus der angelsächsischen Perspektive wurde der Vorschlag als abwegig bewertet mit dem Argument, dass ein Recht auf Achtung der Identität als ein neues Grundrecht anzusehen wäre, welches in der Form im Recht der Mitgliedstaaten bislang fehle.[88]

Es lässt sich nach diesen historischen Betrachtungen festhalten, dass auch ohne den Begriff der Identität im Wortlaut der Art. 7, 8 GRC oder dem zugrundeliegenden Art. 8 EMRK, die Identität der Person von dem Schutzbereich des Art. 7 GRC umfasst ist. Denn der eigene Name, das Bild der Person oder die Kenntnis von der Abstammung sind von der inneren Dimension des Privatlebens in Gestalt der Selbstbestimmung geschützt[89] und sind zugleich konstitutive Elemente der Identität. Somit wird grundrechtlich anerkannt, dass die Identität auf die verschiedenen Ausprägungen der Individualität zurückgeführt werden kann und Gegenstand der individuellen und privaten Entscheidung über die nach außen erkennbaren Informationen ist.

Die Achtung des Privatlebens und der Schutz des Individuums soll mit Blick auf die Interaktionen im gesellschaftlichen Gefüge erweitert werden. Demnach wird der Schutz der Ehre von dem Begriff des Privatlebens erfasst und schützt die persönliche Reputation auch im online-Kontext.[90] Der Begriff des Privatlebens wurde dem als antiquiert geltenden Begriff der Ehre in den Konventsverhandlungen vorgezogen,[91] beschreibt aber zugleich den Schutz des guten Rufes und des eigenen Bildes als Bestandteil des Privatlebens.[92] Entscheidend ist dabei, dass die Schutzdimension des Privatlebens in der Kommunikation mit anderen Grundrechtsträgern einzubeziehen ist. Denn das Recht auf Achtung des Privatlebens stellt kein ab-

87 *Dies.*, Die Charta der Grundrechte der Europäischen Union, 2002, S. 155.
88 *Dies.*, Die Charta der Grundrechte der Europäischen Union, 2002, S. 155.
89 *Jarass*, Kommentar, Charta der Grundrechte der EU, 2016 Art. 7 GRC Rn. 3, 14; *Weber*, in: Stern/Sachs (Hrsg.), Europäische Grundrechte-Charta, 2016, Art. 7 GRC Rn. 16–18.
90 *Bernsdorff/Borowsky*, Die Charta der Grundrechte der Europäischen Union, 2002, S. 182, 186
91 *Bernsdorff*, in: Meyer/Bernsdorff (Hrsg.), Charta der Grundrechte der Europäischen Union, 2014, Art. 7 GRC Rn. 8.
92 *Weber*, in: Stern/Sachs (Hrsg.), Europäische Grundrechte-Charta, 2016, Art. 7 GRC Rn. 14.

solutes Recht dar, sondern schützt ebenso die privaten Beziehungen zu anderen und die Entscheidung des Einzelnen, sich mit privaten Informationen an die Außenwelt zu richten.[93] Folglich lässt sich der Terminus der Kommunikation als Gelenk zwischen dem Recht auf Achtung des Privatlebens und dem Schutz personenbezogener Daten im Zusammenhang mit einem Schutzverständnis der personalen Identität einordnen.

Der Schutz des Privatlebens und der personenbezogenen Daten in Verbindung mit dem Schutz der Kommunikation führt zu einer Anerkennung der personalen Identität dahingehend, dass innerhalb der Kommunikation bei den Kommunikationspartnern Bilder über eine personale Identität entstehen. Denn mit dem Bild einer personalen Identität erlangt das Individuum eine bestimmte Reputation, die zum Bestandteil der Kommunikation wird und sich wiederum im kommunikativen Wechselspiel auf den Schutzbedarf der personalen Identität auswirkt. Damit wird die enge Beziehung zwischen Privatleben, Kommunikation und dem Schutz der personenbezogenen Daten deutlich.

Indem mit der Verarbeitung personenbezogener Daten über eine personale Identität Reputationen entstehen können, die sich auf das Privatleben auswirken, besteht der Bedarf nach dem Schutzmechanismus aus Art. 7 GRC. Durch den ausdrücklichen Schutz der Kommunikation in Art. 7 GRC, welcher sich über den Schutz der Kommunikation unter Anwesenden hinaus auf den Schutz der Kommunikation im online-Kontext erstreckt, kann daraus der Schutz über die personale Identität bildende Kommunikation abgeleitet werden. Dazu gehört die Einflussnahmemöglichkeit des Individuums auf die Kommunikation und die Gestaltung der Bilder personaler Identitäten, welche über das Konzept der Kontrolle von personalen Identitäten erfolgen kann. Dabei lässt sich die Kontrolle der Grundrechtsträger über den Zugang zu Informationen an Dritte aus dem Verständnis der Privatheit nach Art. 8 EMRK ableiten.[94]

Insgesamt umfasst die Achtung des Privatlebens gemäß Art. 7 GRC den Schutz personaler Identitäten in ihrem kommunikativen Wechselspiel. Für die Modellbildung der Identitätsverwaltung ist somit die personale Identität in ihren *Idem*- und *Ipse*-Anteilen einzubeziehen und in einen kommunikativen Zusammenhang zu bringen. Dabei geht es um den

93 *Bernsdorff/Borowsky*, Die Charta der Grundrechte der Europäischen Union, 2002, S. 183; *Jarass*, Kommentar, Charta der Grundrechte der EU, 2016 Art. 7 GRC Rn. 13.

94 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 115.

Schutz der Bilder personaler Identitäten in Gestalt von Reputationen, die der Kontrolle unterliegen. Diese grundrechtlichen Schutzgegenstände sind in dem Identitätsverwaltungsmodell abzubilden, so dass für den Schutz der personalen Identität die Kommunikation und die Kontrolle über die Bilder personaler Identitäten einzubeziehen sind.

b) Personale Identität in der Abwehrfunktion

Nach der Darstellung des Schutzgegenstandes des Privatlebens sollen die grundrechtlichen Abwehrfunktionen aus Art. 7 GRC zur Gewährleistung der personalen Identität analysiert werden. Dafür soll die von *De Hert/Gutwirth* begründete Einteilung in „*opacity tool*" und „*transparency tool*" aufgenommen werden: Danach werden zum Schutz des Privatlebens „*opacity tools*" als Mechanismen beschrieben, die den Grundrechtsträger etwa durch Limitierung staatlicher Macht schützen und die „*transparency tools*" zeigen dem Grundrechtsträger die Datenverarbeitungen und geschäftlichen Praktiken auf.[95] Aus dem Betrachtungswinkel der Grundrechtsfunktionen sollen die Grundlagen für ein Identitätsverwaltungsmodell im Folgenden anhand der „*opacity*" und „*transparency tools*" herausgearbeitet werden.[96]

Primär ist die abwehrrechtliche Dimension zum Schutz vor staatlicher Datenverarbeitung, der ein *qualifiziertes Gefährdungspotential* innewohnt, zu nennen. Daraus ergibt sich im Vergleich zum grundrechtlichen Recht auf informationelle Selbstbestimmung ein undifferenzierteres Schutzregime gegenüber den Rechten der betroffenen Person. Es liege eine Engführung des Grundrechtsschutzes in dem Kombinationsgrundrecht aus Art. 7, 8 GRC vor,[97] welches zugleich Ausgestaltungsspielräume für den Gesetzgeber lässt. In diesen Ausgestaltungsspielräumen sind die Anforderungen der Zweckbestimmung und Rechtfertigung der Datenverarbeitungen, die als „*transparency tools*" eingeordnet werden können, maßgeblich. Mit diesen „*transparency tools*" werden dem Betroffenen auf grundrechtlicher Ebene Kontrollmöglichkeiten gegenüber staatlichen Datenverarbeitungen eingeräumt. Daraus lässt sich wiederum die enge Verbindung zwischen der Abwehrdimension, dem daraus ableitbaren sekundärrechtlichen Ausgestal-

95 *DeHert/Gutwirth*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 61 (62, 95).
96 Angelehnt an *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 97 f.
97 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 213 f.

tungsbedarf und dem darin zum Ausdruck kommenden *Vorfeldschutz* ableiten.[98] Dennoch stellt sich bei der Datenverarbeitung durch öffentliche und private Stellen die Frage nach der konkreten Bestimmung des Gefährdungspotentials und deren *Quantifizierbarkeit*, um den Grad an Abwehrbedarf zum Schutz des Privatlebens und der personenbezogenen Daten gemäß Art. 7, 8 GRC im Vorfeld bestimmen zu können. In der Literatur fehlt es bislang an einer entsprechenden Festlegung über den Rang oder das Gewicht der Gefährdungslagen gegen den Betroffenen und ihren potentiellen Auswirkungen.[99] Weiter stellt *Marsch* fest, dass es sich bei der Bewertung der Gefährdungslagen um spekulative Einschätzungen mit „typisierenden Vermutungen" über die drohenden Nachteile bei der Entfaltungsfreiheit nach Art. 7, 8 GRC handelt.[100] Diese Feststellung legt die Anforderung an die Modellbildung für die Identitätsverwaltung nahe, dass die Risiken der Datenverarbeitung einbezogen und transparent gemacht werden, damit eine subjektive Risikobewertung für die Entscheidungsfindung des Betroffenen über die personalen Identitäten ermöglicht wird. Gleichzeitig könnte eine konkrete Bestimmung des Risikos, in Gestalt von *Quantifizierungen der Gefährdungslagen*, langfristig die Identifizierung der geeigneten Schutzmaßnahmen des Verantwortlichen und des Betroffenen im Rahmen des Selbstdatenschutzes erleichtern. Das Erfordernis einer transparenten Risikobewertung lässt sich auch aus dem Vorfeldschutz ableiten, wonach die Risiken einer Verletzung der Grundrechte im Vorfeld bekannt sein sollten, weil sich danach die Schutzbedarfe und Schutzmechanismen richten.[101] Demnach ist die Bewertung des Risikos und dessen hypothetische Quantifizierbarkeit primär als *„opacity tool"* einzuordnen, wonach die Schutzmaßnahmen bestimmt werden können. Als *„transparency tools"* würden die konkretisierte Mitteilung über die Umstände der Datenverarbeitung und die Risiken der Datenverarbeitung dienen. Damit könnte ein Ausgleich bei möglichen Informationsasymmetrien und Machtungleichgewichten zwischen Verantwortlichen und Betroffenen er-

98 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 205 f.

99 Eine Kategorisierung von Datenverarbeitungsrisiken in ihren individuellen und gesamtgesellschaftlichen Auswirkungen nimmt *Drackert* vor, vgl. *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014.

100 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 223–225.

101 *Ders.*, Das europäische Datenschutzgrundrecht, 2018, S. 88. Ebenso wird als Anforderung an die Zulässigkeit der Datenverarbeitung die Erkennbarkeit der Vorteile und Gefahren der Datenverarbeitung verlangt, damit die Tragweite der Datenverarbeitung abschätzbar wird, *Johlen*, in: Stern/Sachs (Hrsg.), Europäische Grundrechte-Charta, 2016, Art. 8 GRC Rn. 52.

folgen. Gleichwohl ist die grundrechtliche Abwehrdimension zunächst auf die Gefährdungslagen im Verhältnis zwischen dem Staat und dem Bürger ausgerichtet,[102] so dass sich die Schutzmechanismen auf die Datenverarbeitungen in diesem Kontext richten, sofern die Drittwirkung der Grundrechte nicht eine Ausweitung der Schutzmechanismen auf Datenverarbeitungen zwischen Privaten vorsieht.

Ebenfalls kommen Schutzmechanismen als „*opacity tools*" in der Leistungsdimension der Grundrechte in Betracht, mit denen der Schutz des Privatlebens bei eingeschränkten Möglichkeiten des Selbstschutzes gewährleistet wird, wie es etwa bei Kindern der Fall ist. Aufgrund der geringen Ausprägung eines wissensbasierten Selbstschutzes bei Kindern gegenüber den Gefährdungslagen bei Datenverarbeitungen, ist ein einfachrechtlicher Schutzmechanismus gemäß Art. 12 Abs. 1 S. 1 DSGVO, EWG 38 vorgesehen. Es stellt sich entsprechend die Frage nach einem zusätzlichen einfachrechtlichen Schutzmechanismus für solche Konstellationen, in denen der Selbstschutz des Individuums nur eingeschränkt möglich ist. In diesen Konstellationen ließe sich an den Einsatz von „*opacity tools*" in einer erweiterten Form als *Konzept des Selbstdatenschutzes* denken. Damit könnte die Abwehrdimension zum Schutz der personalen Identität mit Transparenzanforderungen erweitert werden, die dem Betroffenen eine weitere Option der Kontrolle zur Abwehr von Grundrechtseingriffen einräumen. Eine solche Option sollte in dem Modell der Identitätsverwaltung einbezogen werden.

3. Drittwirkung aus Art. 7, 8 GRC

Die Bestimmung des kontextspezifischen Schutzumfanges personaler Identitäten richtet sich danach, ob die Wirkung der Grundrechte ausschließlich im Verhältnis zwischen Staat und Privaten erfolgt. Grundsätzlich ist die europäische Grundrechtecharta dahingehend auszulegen, dass die Schutz-, Ausgestaltungs- und Abwehrfunktionen durch den Staat auszuüben sind und die Mitgliedstaaten an eine grundrechtskonforme Auslegung des Sekundärrechts gebunden sind. Dem liegt das Freiheitskonzept der Privatau-

102 Gleichzeitig stellt sich der Schutzbedarf gegenüber staatlichen Überwachungsmaßnahmen nicht allein auf nationaler oder europäischer Ebene, sondern ebenfalls im internationalen Datenverarbeitungsprozess, wie *Di Fabio* im Zusammenhang mit der Snowden-Affäre betont, vgl. *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 23.

tonomie zu Grunde, dass sich private Akteure grundsätzlich im Rechtsverkehr ohne staatliche Freiheitsbeschränkung bewegen können, es sei denn, es liegt ein gerechtfertigter Eingriff in diese Freiheit vor.

Dieser Grundsatz gilt zunächst auch für die informationelle Selbstbestimmung aus dem Kombinationsgrundrecht nach Art. 7, 8 GRC. Gleichwohl können die Gefährdungslagen in den Rechtsbeziehungen zwischen Privaten derart ausgestaltet sein, dass informatorische Machtasymmetrien zu den gleichen Risiken für den Grundrechtsschutz führen, wie sie bei den Datenverarbeitungen durch den Staat angenommen werden. Demnach lässt sich in der unmittelbaren Geltung des Verbotsprinzips nach Art. 8 Abs. 1 GRC ebenso im Sekundärrecht, eine faktische unmittelbare Drittwirkung für öffentliche oder private Stellen annehmen. Ebenso wurde in der Rechtsprechung des EuGHs mehrfach eine unmittelbare Wirkung der Grundrechte angenommen, so dass die nationale Rechtsdogmatik zur mittelbaren Drittwirkung deutlich restriktiver erscheint und nicht übertragbar ist, obwohl vereinzelt auch die mittelbare Grundrechtswirkung angenommen wird.[103]

In der Erstreckung des Verbotsprinzips auf Datenverarbeitungen von Privaten wird von *Marsch* ein überschießender Grundrechtsschutz gesehen, denn nicht jede Datenverarbeitung führe zu einer Gefährdung der Interessen des Betroffenen.[104] Demnach bestünde aufgrund der Informationsasymmetrie gegenüber privaten Intermediären der Bedarf eines effektiven Datenschutzes, der mit einer unmittelbaren Grundrechtsbindung erreicht werden könne.[105] Dem ließe sich entgegenhalten, dass die unmittelbare Geltung des Verbotsprinzips keine Gewähr für ein höheres Schutzniveau bedeutet, da die Einwilligung kein Garant für einen umfassenden Schutz über den Datenzyklus hinweg darstellt.

Zum Verständnis des Begriffs der personalen Identität lässt sich daraus ableiten, dass die begründeten Abwehr- und Leistungsfunktionen mittelbar und unmittelbar auf der Grundrechtecharta basieren und sich daher die rechtliche Modellgrundlage aus dem Primärrecht und Sekundärrecht begründen lässt. Folglich wirken sich die Schutzdimensionen für die personalen Identitäten aus dem Kombinationsgrundrecht gemäß Art. 7, 8 GRC unmittelbar auf die Modellierung der Identitätsverwaltung aus und können mit dem Sekundärrecht konkretisiert werden.

---

103 EuGH, Urt. v. 13.05.2014 – C-131/12, Google Spain, Rn. 69, 99; EuGH, Urt. v. 06.11.2003 – C-101/01, Linquist, Rn. 35, 86; *Britz*, EuGRZ 2009, 1 (8).

104 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 258.

105 *Reinhardt*, AöR 142 (2017), 528 (551 f.).

4. Zusammenfassung

Der Schutzbedarf der personalen Identität für ein Identitätsverwaltungsmodell lässt sich aus Art. 7, 8 GRC ableiten. Demnach gehört zum Schutz der personalen Identität gemäß Art. 7 GRC die innere Dimension etwa durch Kenntnis der Abstammung und die äußere Dimension des erkennbaren Verhaltens. Weiter werden mit dem Schutz der personenbezogenen Daten die primärrechtlichen Kontrollmöglichkeiten im Datenzyklus durch die Einwilligung und das Auskunfts- und Berichtigungsrecht gewährleistet, Art. 8 Abs. 2 GRC. Somit ist von dem grundrechtlichen Schutzregime das Verständnis der personalen Identität erfasst, welches die *Idem*- und *Ipse*-Anteile, das Bild der personalen Identität und die Reputationen umfasst. Damit werden die Kontrolle über die Bilder personaler Identitäten und der Zugang zu personalen Identitäten grundrechtlich geschützt.

Daraus geht die Kommunikation als Voraussetzung für die personale Identität und die Identitätsverwaltung hervor, die dem Schutzbereich gemäß Art. 7 GRC unterliegt. Die personale Identität ist folglich als Bestandteil eines kommunikativen Systems einzuordnen, in dem die Bilder personaler Identitäten und Reputationen zum Gegenstand der Kommunikation werden. Entsprechend lässt sich aus dem Kombinationsgrundrecht gemäß Art. 7, 8 GRC ein Schutzregime für die personale Identität ableiten, welches gegen ein gesteigertes Gefährdungspotential schützt und damit ein undifferenzierteres Schutzregime als das des Rechts auf informationelle Selbstbestimmung schafft. Gleichwohl ermöglicht die grundrechtliche Ausgestaltungsdimension mit den primärrechtlichen Vorgaben für die Datenverarbeitung ein sich auf der sekundärrechtlichen Ebene realisierendes Schutzregime. Diese sekundärrechtlichen Vorgaben erscheinen als prozedurale Maßgaben, die als Grundlage für die Begründung des Identitätsverwaltungsmodells dienen.

Im Einklang mit der Schutzfunktion der informationellen Selbstbestimmung bedarf es eines effektiven Vorfeldschutzes zur Identifizierung und Begegnung der grundrechtsspezifischen Gefährdungslagen, was mit einer *quantifizierbaren Risikobewertung* erfolgen könnte. Diese könnte in Gestalt der Transparenz über das Risiko der Datenverarbeitung in die Modellbildung der Identitätsverwaltung einbezogen werden, damit die Risikobewertung in der Entscheidungsfindung des Betroffenen berücksichtigt wird. Demnach sind die spezifischen Gefährdungslagen im Kontext der öffentlichen und privaten Datenverarbeitung in das Identitätsverwaltungsmodell einzubeziehen und können als „*transparency tool*“ fungieren.

II. Personale Identität im Grundgesetz

Für die Bestimmung des Begriffs der personalen Identität nach dem Grundgesetz, sollen folgend das allgemeine Persönlichkeitsrecht (1.), die allgemeine Handlungsfreiheit (2.) und die mittelbare Drittwirkung (3.) der Grundrechte dargestellt und abschließend bewertet (4.) werden.

1. Personale Identität im allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 GG

Mit dem allgemeinen Persönlichkeitsrecht verbunden ist der Schutz der Privatheit. Der Begriff der Privatheit enthalte einerseits eine von vorrechtlichen und historischen Maßstäben geprägte „schillernde Ambivalenz" und andererseits eine vom Staat aufgegebene Kategorie, an der sich die Rechtsprechung zu orientieren habe.[106] Augenscheinlich kommt dies in der Caroline von Monaco-Rechtsprechung zum Ausdruck, wonach ein Recht auf Achtung der privaten Lebensgestaltung solche Angelegenheiten betrifft, die „typischerweise als Privat" zu bewerten sind und daher dem rechtlichen Schutz unterliegen.[107] Aus dieser begrifflichen Offenheit des typischerweise Privaten lässt sich der vom Bundesverfassungsgericht betonte Bedarf ableiten, dass das allgemeine Persönlichkeitsrecht keiner abschließenden Definition unterzogen werden soll und gegenüber modernen Enwicklungen offen zu verstehen ist.[108] Gleichzeitig verlangt die Bestimmung des Begriffs der personalen Identität und der Identitätsverwaltung eine Herleitung aus dem allgemeinen Persönlichkeitsrecht, die zugleich den Schutzbereich nach der europäischen Grundrechtecharta ergänzen soll. Demnach wird das allgemeine Persönlichkeitsrecht in seinen Ausprägungen, die zugleich als Chronologie der Identitätsgenese fungieren können, dargestellt. Dazu gehören das Recht auf Selbstbestimmung (a), das Recht auf Selbstbewahrung (b) und das Recht auf Selbstdarstellung (c).

---

106 *Nettesheim*, in: Diggelmann/Lege/Nettesheim (Hrsg.), Der Schutzauftrag des Rechts, 2011, 8 (45).

107 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 71; BVerfGE 101, 361 (382) – Caroline von Monaco.

108 BVerfGE 54, 148 (153); BVerfGE 72, 155 (170); BVerfGE 79, 256 (268).

a) Recht auf Selbstbestimmung

Das Recht auf Selbstbestimmung erlaubt dem Individuum, seine Identität selbst zu bestimmen.[109] Dies setzt einen Rahmen voraus, in dem eine unbeeinträchtigte Ausbildung der Identität möglich ist und die Freiheit gewährleistet wird, seine Identität vor äußeren Beschränkungen zu schützen und sich der gefundenen Identität zu vergewissern.[110]

Da die Selbstbestimmung der personalen Identität in ihrer inneren Dimension aus dem inneren und äußeren Dialog besteht, geht es um den Schutz und die Sicherung des eigenen Anteils in diesem dialogischen Prozess. Damit wird die Autonomie zur Selbstbestimmung in innerer und äußerer Hinsicht gewährt. Dass dieses ermöglicht wird, ist Bestandteil des Gewährleistungsgehaltes des allgemeinen Persönlichkeitsrechts und wird durch das Erfordernis des „Raums" für die Selbstwahl, die Selbstdistanzierung, Selbstvergewisserung und erneute Selbstannahme beschrieben.[111]

Zur inneren Dimension des Schutzes kann die Kenntnis der eigenen Abstammung[112] gehören und der Schutz gegen Vorenthaltung erlangbarer Informationen über die Abstammung, um das Selbstverständnis der eigenen Identität zu ermöglichen.[113]Aus den Gewährleistungsbestandteilen ergibt sich, dass die personale Identität in ihrer inneren Dimension als Schablone für das identitätsvermittelte Verhalten dient.[114] Die innere Identitätswahl fungiert somit als Grundlage für die Handlung und unterliegt damit wiederum der relativen und graduellen Autonomie in Gestalt der persönlichen Entfaltung, Art. 2 Abs. 1 GG. Nach *Britz* geht aus dem Wortlaut „freie Entfaltung seiner Persönlichkeit" gemäß Art. 2 Abs. 1 GG hervor, dass bei der Persönlichkeit etwas *eingefaltet* sei und durch das Verhalten

109 *Kingreen/Poscher*, Grundrechte: Staatsrecht II, 2019, Rn. 442.
110 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 74 f.
111 *Dies.*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 28 f.
112 Das Recht auf Kenntnis der Abstammung findet seine einfachrechtliche Realisierung in § 1598a Abs. 1 BGB, wonach ein Anspruch auf Einwilligung in eine genetische Untersuchung zur Klärung der leiblichen Abstammung bestehen kann. Darin kommt zum Ausdruck, dass die Kenntnis der Abstammung einen dauerhaften Beitrag zur eigenen Identitätsfindung darstellt. Jedoch ist das Recht auf Kenntnis der Abstammung nicht grenzenlos realisierbar, sondern kann aufgrund des Kindeswohls begrenzt werden, § 1598a Abs. 3 BGB. Konsequent wird aus sozialpsychologischer Perspektive der Begriff des „Identitätserbes" verwendet, *Keupp*, Identitätskonstruktionen, 1999, S. 100.
113 BVerfG, NJW 1989, 891; BVerfG, NJW 1994, 2475 (2476).
114 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 14.

entfaltet werden könne.[115] Die konkrete Entfaltung und das Entfaltungsmaß der Persönlichkeit erfolgen demnach kontextspezifisch, so dass die damit verbundene und im dialogischen Prozess erkennbare Identität variiert. Dies entspricht dem *Ipse*-Anteil der personalen Identität.

Dem Grunde nach handelt es sich bei der Selbstbestimmung um einen sich auf die Lebenszeit erstreckenden schutzbedürftigen Prozess der Persönlichkeitsentwicklung. Folglich kann etwa in einem späteren Lebensabschnitt die innere Entscheidung über das sexuelle Selbstverständnis und die subjektiv empfundene Identitätszugehörigkeit die Grundlage für ein neues äußerlich erkennbares Erscheinungsbild werden, was auch die Anerkennung im Namensrecht verlangt, §§ 1–8 TSG. Dies wurde im Rahmen der verfassungskonformen Auslegung des § 47 PStG durch Zulassung einer Randbemerkung im Geburtenregister über das Vorliegen einer Intersexualität vorgenommen.[116] Ferner wurde die Erweiterung der binären Geschlechtszugehörigkeit[117] mit der Eintragungsmöglichkeit der Geschlechtsangabe „inter/divers" in das Geburtenregister entschieden. In der Urteilsbegründung wurde festgestellt, dass die geschlechtliche Identität als konstitutiver Bestandteil der Persönlichkeit fungieren könne und eine identitätsbildende Funktion habe, so dass es der einfachrechtlichen Anerkennung eines dritten Geschlechts bedürfe.[118]

Ebenso kommt dem Namen als Vorname, Geburtsname oder Familienname eine identitätsbegründende Funktion zu, was dem *Idem*-Anteil der personalen Identität entspricht. Dabei entschied das Bundesverfassungsgericht über den Ehenamen, dass dieser Anknüpfungspunkt für die Identitätsentwicklung und Identitätsdarstellung sei und damit auch bei einer neuen Eheschließung verwendet werden dürfe, § 1355 Abs. 2 BGB.[119] Folglich verlangt die Identitätswahlfreiheit als innere Dimension der Selbstbestimmung im Zusammenhang mit der Namens- und Geschlechtsänderung den staatlichen Schutz und die Gewährleistung, um das dafür erforderliche äußere Verhalten realisieren zu können.

Für den Schutz der inneren Selbstbestimmung konnte ein einfachrechtlicher Gewährleistungsauftrag im Personenstandswesen nachgewiesen werden. Ebenso besteht ein staatlicher Gewährleistungsauftrag im Rahmen des staatlichen Erziehungsauftrags im Schulwesen neben dem Erziehungs-

115 *Dies.*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 19–22.
116 BVerfG, NJW 1979, 595 (596).
117 *Gössl*, ZRP 2018, 174.
118 BVerfG, NJW 2017, 3643 (3645) Rn. 40–47.
119 BVerfG, NJW 2004, 1155 (1156).

auftrag der Eltern. Denn neben der Bildung der eigenen Persönlichkeit des Kindes besteht ein Schutzauftrag zur Gewährleistung dieser Persönlichkeitsentwicklung, die sich aus der „Gesamterziehung zwischen Staat und Eltern“[120] etwa hinsichtlich der Bildung der „sexuellen Identität“[121] ergibt. Daraus lässt sich ableiten, dass die Identitätsbildung und ihre Einflussfaktoren in der frühen Lebensphase nach der grundrechtlichen Wertung gemäß Art. 6, 7 GG nicht ausschließlich eine private Angelegenheit der Eltern sind, sondern auch ein staatliches Interesse an den Rahmenbedingungen des staatlichen Erziehungsauftrags im Schulwesen besteht. Ein vergleichbarer Gewährleistungsauftrag könnte hinsichtlich der Selbstbestimmungsmöglichkeiten im online-Kontext erforderlich sein, wenn im Vergleich zu den grundrechtlichen Annahmen aus dem offline-Kontext eine eigenständige Gefährdungslage für die Selbstbestimmung im online-Kontext festgestellt wird. Diese könnte einen Schutzbedarf zur Gewährleistung der Selbstbestimmung in ihrer inneren und äußeren Dimension im online-Kontext auslösen.

Insgesamt lässt sich aus dem Recht auf Selbstbestimmung ein Gewährleistungsumfang für den Schutz der dynamischen inneren Dimension der Identität und ihrer äußerlichen Realisierung im Verhalten erkennen, welches dem *Ipse*-Anteil der personalen Identität zuzuordnen ist. Daher kann für die Bestimmung des Begriffs der personalen Identität der dialogische Prozess der Selbstbestimmung als eine Voraussetzung beschrieben werden. Dessen Gewährleistung im online-Kontext könnte für die personale Identität in ihrem *Ipse*-Anteil eines eigenen Schutzregimes bedürfen, was vergleichbar mit dem Gewährleistungsauftrag aus dem Schul- und Erziehungswesen nach Art. 6, 7 GG ausgestaltet sein könnte. Gleichwohl handelt es sich um einen spezifischen Kontext, so dass diese Generalisierung auf den Schutz der personalen Identität im online-Kontext sehr weitgehend wäre und der grundrechtlichen Abwehrdimension zum Schutz der Freiheit zur Selbstbestimmung widersprechen würde. Denn die personale Identität im online-Kontext muss dem gleichen freiheitlichen Schutzniveau wie im offline-Kontext unterliegen. Insgesamt lässt sich jedoch aus der Rechtsprechung über den staatlichen Schutzauftrag zu dem Begriff der

120 BVerfG, NJW 1978, 807 (809–811).

121 Die Begrifflichkeit der „sexuellen Identität“ ist dem europäischen Recht entlehnt, worin die „sexuelle Ausrichtung“ verwendet wird, Richtlinie 2000/78/EG vom 27.11.2000 zur Festlegung eines gemeinsamen Rahmens zur Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf. Darin liegt die Grundlage für den im einfachen Recht verwendeten Begriff der „sexuellen Identität“, §§ 1, 19, 20 AGG.

„sexuellen Identität" das grundrechtliche Identitätsverständnis ableiten, das von mehreren Teilen der Identität ausgeht.

b) Recht auf Selbstbewahrung

Das Recht auf Selbstbewahrung umfasst die Ausprägungen sich zurückzuziehen, abzuschirmen und für sich allein zu bleiben.[122] Maßgeblich ist dabei die vom Bundesverfassungsgericht entwickelte Sphärentheorie, die zwischen der Intims-, Privat- und Sozialsphäre differenziert.[123] Dem liegt zugrunde, dass die „freie Entfaltung der Persönlichkeit" nicht allein über die innere Dimension erfolgt, sondern in einem graduellen sich steigernden dialogischen Verhältnis zur Außenwelt steht. Dieses beginnt im Kernbereich intimer Lebensgestaltung als Ausprägung der Menschenwürde, setzt sich im privaten dialogischen Austausch fort und umfasst schließlich den sozialen Austausch als Bestandteil der Handlung in der Öffentlichkeit. Zum Schutz des Kernbereichs gehört etwa der Schutz von Informationen über den Gesundheitszustand, was die Beschlagnahme von Patientenkarteikarten erfasst.[124] Weiter macht die Entscheidung des Bundesverfassungsgerichts zu der Beschlagnahme von Tagebuchaufzeichnungen den graduellen Schutz des Kernbereichs besonders deutlich, indem zwar die Auseinandersetzung mit dem Selbst vom Kernbereich geschützt wird, dieser Schutz jedoch infolge der Verschriftlichung dieser Auseinandersetzung nachlässt, wenn es bei den Aufzeichnungen um bevorstehende Straftaten geht.[125] Somit ist von dem Recht auf Selbstbewahrung der Schutz der inneren Auseinandersetzung zur Bildung der personalen Identität erfasst und genießt absoluten Schutz, sofern das strafrechtliche Aufklärungsinteresse dem nicht entgegensteht.

Daraus lässt sich der Schutzbedarf der personalen Identität in seiner Ausprägung als Selbsterhaltung und -bewahrung folgern und verlangt von einem Identitätsverwaltungsmodell die Sicherstellung des Erhalts der personalen Identität in einem bestimmten Zustand. Dazu gehört, dass im online-Kontext die IT-sicherheitsrechtlichen Anforderungen über den Vertraulichkeits- und Integritätsschutz gewährleistet werden müssen, damit die personale Identität gewahrt bleibt. Ebenso lässt sich der Schutz gegen

122 *Kingreen/Poscher*, Grundrechte: Staatsrecht II, 2019, Rn. 444.
123 *Dies.*, Grundrechte: Staatsrecht II, 2019, Rn. 446.
124 BVerfG, NJW 1972, 1124.
125 BVerfG, NJW 1990, 563 (564).

Profile im online-Kontext, die im Widerspruch zu der personalen Identität stehen, einbeziehen.

c) Recht auf Selbstdarstellung

Das Recht auf Selbstdarstellung schützt vor herabsetzender, verfälschender, unerbetener öffentlicher Darstellung und Wahrnehmung.[126] Der Schutz stellt gerade auf die kommunikative Beziehung des Einzelnen zu anderen und der Öffentlichkeit ab. Diese Schutzausprägung des allgemeinen Persönlichkeitsrechts gewährt dem Individuum einen Schutzraum gegenüber fremden Identitätserwartungen.[127] Denn das Recht auf Selbstbestimmung und das Recht auf Selbstbewahrung setzen einen inneren Freiraum voraus, der im dialogischen Wechselspiel zwischen Selbst- und Fremdbildern stehe und gerade keinem solipsistischen Verständnis der personalen Identität unterliegen dürfe.[128] Durch den Blick des Anderen kann die Persönlichkeit bestätigt oder abgelehnt werden. Demnach steht das Selbstbild der personalen Identität in einem kommunikativen Dialog mit dem Fremdbild der personalen Identität. Sobald das Fremdbild der personalen Identität auf diskriminierend wirkenden stereotypen Denk- und Verhaltensmustern beruht, kann dies einen eigenständigen Schutzbedarf gegen Diskriminierungen auslösen.

Damit wird deutlich, dass wirkmächtige Fremdbilder die Realisierung der Selbstdarstellung einer selbstbestimmten personalen Identität erschweren und zu einer Einschränkung des subjektiven Entfaltungspotentials führen können.[129] Im online-Kontext kann hinzukommen, dass mit Profilen bereits Fremdbilder der personalen Identität bestehen. Daraus können sich Einschränkungen der Selbstdarstellung des Selbstbildes der personalen Identität im online-Kontext ergeben. Insofern könnte mit dem Selbstdatenschutz und den Diskriminierungsverboten eine Kompensation erfolgen.

Ungeachtet möglicher Beeinträchtigungen des Rechts auf Selbstdarstellung kann die kommunikative Beziehung zu anderen bestätigenden Charakter haben und die Selbstwahrnehmung stabilisieren, womit die gewähl-

126 *Kingreen/Poscher*, Grundrechte: Staatsrecht II, 2019, Rn. 447.
127 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 37 ff.
128 *Nettesheim*, in: Diggelmann/Lege/Nettesheim (Hrsg.), Der Schutzauftrag des Rechts, 2011, 8.
129 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 43.

te Identitätsvorstellung aufrechterhalten werden könne.[130] Dies lässt sich mit dem Terminus der Kontrolle umschreiben, wonach die Wahrung und Fortentwicklung der gewählten Selbstdarstellung gegenüber den Fremdbildern von der natürlichen Person kontrollierbar ist. Demnach wird die personale Identität als steuerbar begriffen und es besteht die Möglichkeit, auf die Identitätserwartungen anderer Einfluss zu nehmen. Gleichzeitig könne kein Anspruch auf Schutz gegen Fremdzuschreibung und andere Identitätserwartungen bestehen.[131]

Die private Entscheidung des Individuums über die Steuerung, was in seiner äußeren Darstellung öffentlich oder privat zugänglich sein soll, unterliege seiner Kontrolle, so dass mit dem Begriff des Privaten auch der der Kontrolle in Verbindung gebracht werden könne.[132] Zur Realisierung dieser Steuerungs- und Kontrollmöglichkeit müsse der Staat nach Wegen suchen, die Entfaltung der Persönlichkeit vor negativen Auswirkungen fremder Identitätserwartungen zu schützen und gleichzeitig die Freiheit zur Persönlichkeitsentfaltung zu gewährleisten.[133] Dies ist gerade im Hinblick auf die unterschiedlichen Eigenschaften und Gefährdungslagen der Selbstdarstellung im offline- und online-Kontext maßgeblich, so dass der sich aus dem Recht auf Selbstdarstellung ergebende Kontrollbedarf über das Private im online-Kontext höheren staatlichen Gewährleistungsanforderungen unterliegen könnte. Weiter sollen zu dem Recht auf Selbstdarstellung die dazu gehörenden Rechte[134] auf Neubeginn (aa), auf informationelle Selbstbestimmung (bb) und das Recht am eigenen Bild (cc) zur Bestimmung der personalen Identität und zu den Grundlagen der Identitätsverwaltung herangezogen werden.

aa) Recht auf Neubeginn

Das *Recht auf Neubeginn* lässt sich am strafrechtlichen Rehabilitationsverfahren und dem Schutz Minderjähriger vor finanzieller Überschuldung

130 *Dies.*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 39; *Kingreen/Poscher*, Grundrechte: Staatsrecht II, 2019, Rn. 448.
131 *Dies.*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 40–48; *Nettesheim*, in: Diggelmann/Lege/Nettesheim (Hrsg.), Der Schutzauftrag des Rechts, 2011, 8 (47).
132 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 72.
133 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 37 ff.
134 *Kingreen/Poscher*, Grundrechte: Staatsrecht II, 2019, Rn. 448–452.

nachweisen.[135] Das Rehabilitationsinteresse von strafrechtlich verurteilten Individuen zielt auf den Schutz gegen soziale Stigmatisierung ab und dient der Chance auf einen Neubeginn.[136] Diese ist in den Tilgungsfristen im Bundeszentral- und Erziehungsregister gemäß § 46 BZRG einfachrechtlich geregelt und ermöglicht nach dem Ablauf der Fristen ein straffreies Fremdbild der personalen Identität. In diesem Zusammenhang werden die langfristigen Auswirkungen von Stigmatisierungen aufgrund von Attributen etwa dem des Strafurteils sichtbar, worin ein *tabula rasa*-Recht gesehen wird.[137] Dieses wurde in der Entscheidung des Bundesverfassungsgerichts „Recht auf Vergessen I"[138] über das Auffinden von Medienberichten zu einem weit in der Vergangenheit liegenden Mordfall konkretisiert. Dabei wurde der Schutz des sich wieder in Freiheit befindenden Straftäters vor der Konfrontation mit Handlungen aus der Vergangenheit beschrieben, die bereits so weit zurücklagen, dass das Informationsinteresse der Allgemeinheit gegenüber dem Interesse an einer reellen Chance auf Neubeginn zurückträte.[139] Weiter wurde das unbegrenzte Vorhalten von Irrtümern und Fehltritten aus der Vergangenheit nicht nur als Beeinträchtigung der Entfaltungsmöglichkeiten des Individuums, sondern auch als Beeinträchtigung des Gemeinwohls angesehen.[140] Daraus lässt sich insgesamt eine Steigerung des Schutzniveaus gerade hinsichtlich der hohen Reproduzierbarkeit von Zuschreibungen im online-Kontext ableiten, in der zugleich eine Anerkennung der divergierenden Risikolagen für das allgemeine Persönlichkeitsrecht zwischen dem offline- und online-Kontext liegt.

Ein aus dem Recht auf Neubeginn ebenso ableitbarer Schutzmechanismus liegt in der Verhinderung der Überschuldung Minderjähriger gemäß § 1929a BGB, damit dem Minderjährigen die Chance eines finanziell unbelasteten Eintritts in die Volljährigkeit gewährt und ein nachteiliges Fremdbild der personalen Identität über finanzielle Dispositionen vermieden wird. In dieser einfachrechtlichen Ausprägung des Rechts auf Neubeginn werden die Bewahrung von Identitätsoptionen und das Bestehen einer tatsächlichen Wahl zwischen den Bildern personaler Identitäten ermöglicht.[141]

135 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 74.
136 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 105 f.
137 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (31).
138 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I.
139 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 148.
140 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 107 f.
141 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 74.

Diese für den offline-Kontext geltenden Wertungen sind auf den online-Kontext zu übertragen und sollen mit den Schutzmechanismen gegen Fremdbilder personaler Identitäten im online-Kontext erweitert werden. Daher sollte aufgrund des Rechts auf Neubeginn ebenso die Loslösung von algorithmusbasierten Zuschreibungen identitätsrelevanter Attribute und damit verbundener Fremdbilder personaler Identitäten ableitbar sein, um eine Rehabilitierung der personalen Identität zu ermöglichen. Dies lässt sich aus der Entscheidung des EuGHs in *Google Spain*[142], in der das Recht auf Vergessenwerden begründet wurde, folgern. Denn aus dem Recht auf Neubeginn kann für ein Identitätsverwaltungsmodell die Erforderlichkeit einer direkten Einflussnahme auf die Datensätze über identitätsrelevante Eigenschaften begründet werden, die in der Löschung und in dem Vergessen dieser Informationen liegt. Infolge der Konkretisierung durch das Bundesverfassungsgericht[143] bedarf es dabei der Einbeziehung des Zeitfaktors über den Zuschreibungsgegenstand zur personalen Identität, um sukzessive einen gesteigerten Schutz für die individuellen Entfaltungsmöglichkeiten im online-Kontext gegenüber dem Informationsinteresse und der allgemeinen Meinungsfreiheit gewährleisten zu können.

bb) Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung wurzelt in dem allgemeinen Persönlichkeitsrecht und der Menschenwürde, Art. 2 Abs. 1 i.V.m. Art. 1 GG,[144] worin die Leitlinie für die Inhaltsbestimmung dieses Grundrechts liegt.

Von dem Recht auf informationelle Selbstbestimmung wird die Befugnis des Individuums erfasst, grundsätzlich über die Offenbarung persönlicher Lebenssachverhalte selbst zu entscheiden.[145] Weiter wird geschützt, dass das erlangte Wissen der Kommunikationspartner für das Individuum abschätzbar ist.[146] Sobald dies aufgrund umfangreicher Datensammlungen in Informationssystemen erschwert wird und dazu führt, dass Persönlichkeitsbilder und Persönlichkeitsprofile entstehen können, die für den Be-

142 EuGH, Urt. v. 13.05.2014 – Rs. C – 131/12 – Google Spain.
143 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 120 ff.; BVerfG, Urt. v. 06.11.2019 – 1 BvR 276/17, Recht auf Vergessen II, Rn. 131–133.
144 BVerfGE 65, 1 (43).
145 BVerfGE 65, 1 (43).
146 BVerfGE 65, 1 (43).

troffenen unzureichend kontrollierbar sind, bedarf es eines erweiterten Schutzes nach dem Recht auf informationelle Selbstbestimmung.[147] Ebenso führt die Undurchsichtigkeit der Speicherung und Verwendung von Daten zu einem gesteigerten Schutzbedarf, der sich gegen die Risiken aus umfangreichen Datensammlungen richtet.[148] Maßgeblich ist dabei, eine Einschränkung der Selbstbestimmung durch unüberschaubare Zuschreibungen im online-Kontext zu begegnen und eine Mitentscheidungsmöglichkeit bei der Zuschreibung von Profilen einzuräumen.[149]

Daraus ergibt sich die risikobasierte Auslegung des Datenschutzrechts, bereits vor solchen Datenverarbeitungen zu schützen, die eine „Furcht vor einer unkontrollierten Persönlichkeitserfassung"[150] auslösen können. Die umfangreiche staatliche Informationssammlung über ein Individuum kann sich deshalb auf sein Verhalten auswirken, so dass mit der *abstrakten Gefährdungslage* seit dem Volkszählungsurteil bereits ein Eingriff in den Schutzbereich vorliegen kann. Das Risiko der Gefährdung potenziere sich und wirke sich gesellschaftlich aus, wenn umfangreiche Datenverarbeitungen erfolgen, so dass weitreichende Erkenntnisse über ein Individuum generiert werden können und das Konzept der „berechtigten Privatheitserwartung" kaum realisierbar sei.[151] Aus dem Blickwinkel der personalen Identität geht es bei der informationellen Selbstbestimmung um den Schutz der inneren und äußeren Kommunikationen, so dass die technisch bedingte Gefährdung einen eigenständigen Schutzbedarf auslöst.

Das Recht auf informationelle Selbstbestimmung hat im online-Kontext in dem Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, sog. „IT-Grundrecht", eine weitere Differenzierung erfahren.[152] Danach wurde der eigenständige Schutzbedarf bei der online-Durchsuchung begründet, der sich auf die Gewährleistung der Persönlichkeitsentfaltung bei der Nutzung informationstechnischer Systeme bezieht.[153] Denn mit der Nutzung informationstechnischer Systeme werden Daten aus der Privatsphäre generiert, was bei einer Infiltration des Systems zu einem umfassenden Bild über das Leben des Nutzers führen

147 BVerfGE 65, 1 (42).
148 BVerfGE 65, 1 (46).
149 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 84, 87.
150 BVerfGE 65, 1 (4).
151 *Nettesheim*, in: Diggelmann/Lege/Nettesheim (Hrsg.), Der Schutzauftrag des Rechts, 2011, 8 (31).
152 *Kingreen/Poscher*, Grundrechte: Staatsrecht II, 2019, Rn. 450.
153 BVerfGE 120, 274 (312 f.).

kann.[154] Demnach wird von dem IT-Grundrecht die vielfältige und umfangreiche Vernetzung personenbezogener Daten, die einen „Einblick in wesentliche Teile der Lebensgestaltung einer Person" und ein „aussagekräftiges Bild der Persönlichkeit" ermöglichen, geschützt.[155] Weiter erhöht die längerfristige Überwachung das Risiko von umfangreichen Verhaltens- und Kommunikationsprofilen über den Nutzer,[156] die im Rahmen der informationellen Selbstbestimmung nicht geschützt werden können. Damit werden neben der informationellen Selbstbestimmung die Vertraulichkeits- und Integritätserwartung im öffentlichen Raum des Internets geschützt,[157] die sog. „digitale Handlungsfreiheit".[158] Entsprechend unterliegen nunmehr Zugangsberechtigungen, Benutzernamen, Passwörter, Online-Bankdaten einem eigenen Schutzregime, wobei der Schutz auch bei einem mangelndem Überprüfungsmechanismus über die Identität der Nutzer besteht.[159] Daraus ableitend ist für die Bestimmung des Begriffs der personalen Identität maßgeblich, dass auch im online-Kontext die Bildung und Wahrung der personalen Identität einem eigenständigen Schutz und den Schutzanforderungen des „IT-Grundrechts" unterliegt. Denn mit dem „IT-Grundrecht" kann aufgefangen werden, dass die aus dem offline-Kontext stammende Sphärentheorie kaum auf den online-Kontext übertragen werden könne und einer Relativierung bedürfe,[160] da etwa bei der Nutzung sozialer Medien gleichermaßen die Intim-, Privat- und Sozialsphäre zusammenwirken können.

Das Recht auf informationelle Selbstbestimmung und das IT-Grundrecht richten sich auf personenbezogene Daten und verlangen gleichzeitig die Einbeziehung des Informations- und des Wissensbegriffs. Denn der wirksame Schutz schließt die Daten und die erzielbaren Erkenntnisse ein, wie es sich bereits aus der „informationellen" Selbstbestimmung ergibt. So wird etwa von *Spiecker gen. Döhmann* klargestellt, dass es beim Datenschutzrecht auf den Schutz der Informationen über einen Betroffenen und

154 BVerfGE 120, 274 (311).
155 BVerfGE 120, 274 (314).
156 BVerfGE 120, 274 (323 f.).
157 BVerfGE 120, 274 (315).
158 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 19.
159 *Böckenförde*, JZ 2008, 925 (937).
160 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 178; *Böckenförde*, JZ 2008, 925 (938); *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 41; *Albers*, Informationelle Selbstbestimmung, 2005, S. 221 f.

nicht der Daten über eine Person ankomme.[161] Daraus geht hervor, dass Erkenntnisse aus dem dialogischen Prozess ebenso von dem Schutz umfasst sind, so dass damit ein immanenter Schutz gegenüber technisch bedingten Erkenntnisprozessen einhergeht. Dazu können in dem Erkenntnisprozess indirekte Diskriminierungen einfließen, die dem einfachrechtlichen Schutz gemäß §§ 7, 1 AGG unterliegen können. Infolge dieser Erkenntnisse können kommunikative Rückkoppelungen gegenüber dem Recht auf informationelle Selbstbestimmung entstehen, die sich auf die personale Identität auswirken und zum Schutzgegenstand der informationellen Selbstbestimmung werden. Demnach besteht ein Steuerungsbedarf des Individuums nicht nur gegenüber den personenbezogenen Daten, sondern auch gegenüber dem Erkenntnisgehalt aus diesen Daten. Damit verbunden ist die Kontrolle der Informationen, die nach außen sichtbar werden und eine Ausprägung der inneren Selbstbestimmung in Gestalt einer Selbstwahl[162] sein können. Daneben gehört zu der Steuerungs- und Kontrollmöglichkeit über die personenbezogenen Daten und Erkenntnisse, dass die Risiken der Datenverarbeitungen einbezogen werden. Der vorgelagerte Schutz der informationellen Selbstbestimmung bezieht die Kontrollmöglichkeit über die zukünftigen Risiken ein, so dass der Schutz personaler Identitäten bereits mit der Kenntnis potentieller Gefährdungslagen beginnt. Damit sind bereits empfundene Gefährdungslagen, die sich in einem Gefühl des Überwachtwerdens oder durch Einschüchterungseffekte[163] äußern können, in die Modellbildung einzubeziehen.

Insgesamt verfügen das Recht auf informationelle Selbstbestimmung und das IT-Grundrecht primär über eine Abwehrdimension, dennoch lassen sich daraus eigenständige Schutzmechanismen zur Gewährleistung der Grundrechtsausübung im online-Kontext herleiten. Diese könnten in der personalen Identität und in der Identitätsverwaltung liegen, mit der dem Individuum eine Steuerungs- und Kontrollmöglichkeit zukommt. Dabei würde sich die Kontrollmöglichkeit auch auf den möglichen Erkenntnisgewinn aus Daten richten und es käme ein Konzept der „Kontrolle durch Intransparenz“[164] in Betracht, mit dem das Weglassen von Daten zu einer Steuerung der Erkenntnismöglichkeiten führt. Somit kann aus dem Recht

161 *Spiecker gen. Döhmann*, in: Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, 263 (265).
162 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 18–21.
163 *Nettesheim*, in: Diggelmann/Lege/Nettesheim (Hrsg.), Der Schutzauftrag des Rechts, 2011, 8 (46).
164 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 96.

auf informationelle Selbstbestimmung und dem IT-Grundrecht ein Schutz- und Gewährleistungskonzept hergeleitet werden, welches für den online-Kontext die Begründung eines eigenständigen Schutzmechanismus rechtfertigen kann.

cc) Recht am eigenen Bild

Das Recht am eigenen Bild stellt eine Ausprägung des Rechts auf informationelle Selbstbestimmung dar.[165] Von dem Recht ist geschützt, dass darüber befunden werden kann, welches Bild der personalen Identität in der Öffentlichkeit erscheinen soll. Dazu gehört die Möglichkeit des Individuums, das Erscheinungsbild in einem bestimmten Kontext aufzulösen, datenmäßig zu fixieren und jederzeit vor einem weiten Personenkreis zu reproduzieren.[166] Dabei geht es um den Schutz der Privatsphäre und um die Entscheidung, inwieweit die Darstellung gegenüber Dritten oder in der Öffentlichkeit mit einer Abbildung erfolgen soll.[167] Insofern bedarf jedes Abbild eines Individuums einer vorangegangenen Entscheidung über das äußerlich erkennbare Bild der personalen Identität, die etwa mit der einfachrechtlichen Einwilligung gemäß § 22 KUG erfolgt. Gleichzeitig ist das Bild einer personalen Identität das Ergebnis einer inhaltlichen Entscheidung des Individuums, die sich auf den dialogischen Prozess zwischen den *Idem*- und *Ipse*-Anteilen zurückführen lässt.

In Anbetracht der vielfältigen Selbstdarstellungsmöglichkeiten im online-Kontext mit „*Selfies*“ oder anderen Abbildungen in sozialen Medien, lässt sich ein gesteigertes Risiko zum Schutz der personalen Identität annehmen. Denn die vorübergehende Darstellung eines *Ipse*-Anteils einer personalen Identität in einem Bild erlangt an Permanenz, obwohl es sich um eine Momentaufnahme handelt. Zudem können die Bilder personaler Identitäten im online-Kontext in Gestalt von Profilen aus Informationen bestehen, die sich diskriminierend auswirken, wenn das Profil aufgrund des Geschlechts, der Abstammung oder der politischen Anschauung eine bestimmte Bewertung enthält.[168] Daraus könnte sich das Erfordernis eines

---

165 *Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 71; *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 41 f.

166 BVerfGE 101, 361 (381) – Caroline von Monaco.

167 BVerfGE 101, 361 (373, 382) – Caroline von Monaco.

168 *Kieck* erkennt in den aus Art. 3 GG vermittelten Gleichheitsrechten ebenfalls einen grundgesetzlichen Identitätsschutz aufgrund des Verbotes von Ungleich-

graduellen Schutzmaßes über die erstellten Bilder als Gegenbilder ergeben. Dieser Schutzbedarf wird von *Nettesheim* mit dem Neuansatz des Schutzes vor freiheitsbeeinträchtigender Vergegenbildlichung[169] beschrieben.

Im Einzelnen geht der Bedarf nach einem erweiterten Schutzkonzept im online-Kontext etwa aus der Rechtsprechung über die Bewertungsportale hervor. Denn in diesen wird gegen das im online-Kontext geschaffene Gegenbild oder Profil vorgegangen, welches in seinem Schutzbedarf zwischen dem Recht auf informationelle Selbstbestimmung und der Meinungsfreiheit einzuordnen ist. Dabei tritt das entstandene Bild der personalen Identität in ihrem *Ipse*-Anteil als Ergebnis zwischen Selbstbestimmung und Meinungsfreiheit in Erscheinung. Folglich wurde vom BGH entschieden, dass Ärzte-Bewertungsportale zwischen zahlenden und nicht zahlenden Kunden unterscheiden und damit nicht „neutral" seien, was zu einem gesteigerten Schutz der nicht zahlenden Ärzte, die von Bewertungen betroffen sind, führe und einen Löschungsanspruch auslösen könne.[170] Weiter wurde dem Betreiber des Ärzte-Bewertungsportals bei einer nicht ausschließbaren falschen Bewertung, die sich „abträglich auf das Bild (...) in der Öffentlichkeit"[171] auswirke, eine umfassende Prüfungspflicht auferlegt. Diese solle die Feststellung der Tatsachengrundlage und Richtigkeit einer Meinungsäußerung in Anbetracht der beeinträchtigenden Wirkungen auf die Wettbewerbsfähigkeit zu anderen Ärzten ermöglichen.[172] Grundsätzlich aber wurde entschieden, dass die Aufnahme der Ärzte in Bewertungsportale dem Interesse der Öffentlichkeit an Informationen über ärztliche Dienstleistungen diene und die Bewertungen als Abwägungsgegenstand zwischen dem Schutz der informationellen Selbstbestimmung des Arztes und dem allgemeinen Informationsinteresse stehen.[173] Schließlich wurde die vorgenommene Verlinkung und Darstellung eines Suchergebnisses durch den Algorithmus der Suchmaschine nicht als Verletzung des allgemeinen Persönlichkeitsrechts eingeordnet, da die Prüfpflicht des Suchmaschinenbetreibers sich nicht auf die Inhalte erstrecken könne.[174]

---

behandlungen wegen persönlicher Merkmale an, *Kieck*, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe, 2019, S. 169.

169 *Nettesheim*, in: Diggelmann/Lege/Nettesheim (Hrsg.), Der Schutzauftrag des Rechts, 2011, 8 (33 f.).

170 BGHZ 217, 340 (348) – Ärztebewertungsportal III.

171 BGHZ 209, 139 (149) – Ärztebewertungsportal III.

172 BGHZ 209, 139 (150–155) – Ärztebewertungsportal III.

173 BGHZ 202, 242 (255 f.) – Ärztebewertungsportal II.

174 BGHZ 217, 350 (361).

Bei diesen Fallkonstellationen geht es regelmäßig darum, dass sich die Kläger gegen ein erzeugtes Gegenbild in Gestalt von Bewertungen auf einem Internetportal zur Wehr gesetzt haben, um die Kontrolle des Bildes[175] über die Selbstdarstellung wiederzuerlangen. Gleichzeitig wird der Rechtsprechung zu den Bewertungsportalen vorgeworfen, dass die Begründungen weiterhin von der Phänomenologie im offline-Kontext geprägt seien, wodurch ein Anpassungsbedarf an die Spezifika im online-Kontext bestünde.[176] Denn im online-Kontext vergesse das Internet nicht und könne die Daten, Postings als Repräsentationen der Bilder personaler Identitäten in Bewertungsportalen in hohem Maße miteinander verbinden, so dass hinsichtlich der Reichweite, im Vergleich zum offline-Kontext, ein „Elefantengedächtnis" entstünde, welches mit der klassischen Abwägung nicht ausreichend erfasst werden könne.[177] Diese *Bilder personaler Identitäten* könnten als komplexitätsreduzierendes Ergebnis des *Idem-* und *Ipse*-Dialoges der personalen Identität zum Gegenstand der Identitätsverwaltung werden.

d) Zusammenfassung

Aus dem allgemeinen Persönlichkeitsrecht lassen sich in den Ausprägungen des Rechts auf Selbstbestimmung, Selbstbewahrung und Selbstdarstellung die jeweiligen Dimensionen zur Bestimmung der personalen Identität ableiten. Dazu gehört, dass sich das Individuum im Rahmen der Selbstbestimmung in einem dialogischen Prozess den Eigenanteil an dem Bild der personalen Identität sichert und damit die innere Dimension einer dynamischen Identitätsbildung geschützt wird. Dabei konnte der staatliche Schutz etwa in dem offline-Kontext des staatlichen Erziehungsauftrages im Schulwesen aus Art. 7 GG zur Identitätsbildung oder zur Anerkennung des „dritten Geschlechts" im Personenstandsregister exemplarisch herangezogen werden. Denn in beiden Schutzmechanismen geht es darum, dass für die Freiheit zur Selbstbestimmung und Identitätsbildung der Staat den Rahmen gewährleisten soll. Daraus lassen sich Anhaltspunkte ableiten, nach denen der staatliche Schutzauftrag im offline-Kontext seine Realisie-

175 *Whitman*, Yale L. J. 2004, 1151 (1184 f.): Die Konzeption der Kontrolle über die Begründung und Entwicklung eines eigenen Bildes umfasst ebenso den Erhalt dieses begründeten Bildes.
176 *Boehme-Neßler*, K&R 2016, 637 (644).
177 *Ders.*, K&R 2016, 637 (642).

rung findet und auch auf den online-Kontext erstreckt wird. Entsprechend aufschlussreich ist das IT-Grundrecht, was vor der Infiltration des Systems schützt, aus der sich ein umfassendes Bild über das Leben des Nutzers generieren lässt. Damit wird den spezifischen Gefährdungslagen im online-Kontext Rechnung getragen, die aus dem Nutzungsverhalten ein aussagekräftiges Bild der Persönlichkeit und der Lebensführung ermöglichen. Darin kommt eine Erstreckung des Schutzes der informationellen Selbstbestimmung auf die allgemeine Handlungsfreiheit zum Ausdruck, die von *Schallbruch* als „digitale Handlungsfreiheit“[178] beschrieben wird.

Somit erfährt im online-Kontext das Recht auf Selbstdarstellung eine eigenständige Schutzausgestaltung in der kommunikativen Beziehung und der Kontrolle über das daraus entstandene Gegenbild. Weiter gehören zu dem Recht auf Selbstdarstellung das Recht auf Neubeginn, welches sich vom Rehabilitationsrecht im Strafprozessrecht ableiten lässt und den Bedarf nach einem *tabula-rasa*-Recht über die Außendarstellung der personalen Identität begründet. Diese für den offline-Kontext geltende Regelungslage könnte ebenso für online-Kontexte von Bedeutung sein, wenn es um einen „Neubeginn“ als Loslösung von algorithmusbasierten Zuschreibungen mit dem Risiko diskriminierend wirkender Profilerstellung geht. Daher ist es notwendig, dass die Daten und die Erkenntnismöglichkeiten über eine Identität dem Identitätsbegriff zugeordnet werden, wie es mit dem Recht auf informationelle Selbstbestimmung ermöglicht wird. In dem Recht auf informationelle Selbstbestimmung wird vereint, dass über die Offenbarung persönlicher Lebenssachverhalte selbst bestimmt und das erlangte Wissen der Kommunikationspartner abschätzbar wird. Folglich wird mit dem Recht auf informationelle Selbstbestimmung auch die Kontrollierbarkeit der personalen Identitäten beschrieben.

Ebenso sieht das Recht am eigenen Bild die Kontrolle über die personale Identität vor. Das Bild der personalen Identität ergeht als Ergebnis und Abbild einer vorangegangenen Entscheidung über die Außendarstellung. Weiter dient das Recht am eigenen Bild dem Schutz der Identität vor einer voyeuristischen Kultur im online-Kontext. Dabei wird vorausgesetzt, dass der Gegenstand der Kontrolle durch das Individuum das Bild der personalen Identität sei, wohingegen das im dialogischen Prozess entstehende Fremdbild unkontrollierbar bleibt. Folglich seien die Grenzen des Bildes der personalen Identität und das Gegenbild der Gegenstand privater Ver-

178 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 19.

handlung[179]. Daraus lässt sich eine wesentliche Grundlage für das Identitätsverwaltungsmodell ableiten, wonach sich die Verhandlungsdimension über die Privatheit der Bilder personaler Identitäten auf den online-Kontext erstreckt und das Verständnis einer „*verhandelbaren Identität*" ermöglicht wird.

2. Personale Identität in der allgemeinen Handlungsfreiheit, Art. 2 Abs. 1 GG

Die allgemeine Handlungsfreiheit stellt die äußere Dimension des allgemeinen Persönlichkeitsrechts dar, womit die Verhaltensebene der Identitätsrealisierung geschützt wird. Gerade die inneren Entscheidungen sind auf die Notwendigkeit einer äußeren Handlung gerichtet, worin die grundlegende Zwangslage des Menschen beschrieben wird.[180] Gleichzeitig handelt es sich bei der allgemeinen Handlungsfreiheit um ein Auffanggrundrecht, welches einen subsidiären Schutz gegenüber anderen Grundrechten entfaltet.[181] Im Hinblick auf die Bestimmung des Begriffs der personalen Identität und die Grundlagen eines Identitätsverwaltungsmodells geht es um den absolut geschützten Kernbereich privater Lebensgestaltung, dessen Schutzbereich aber gerade gegenüber neuen Gefährdungslagen im online-Kontext anzupassen ist. Dies deckt sich mit dem im Gesetzgebungsverfahren diskutierten Wortlaut, „Jeder kann tun und lassen, was er will"[182], der die äußerlich erkennbare Selbstwahl durch den autonomen Freiheitsgebrauch deutlich macht. Damit ist der Schutzbereich der allgemeinen Handlungsfreiheit nicht kontext- oder ortsgebunden und verlangt keine physische Zugangsmöglichkeit. Demnach ist vom Schutzbereich jedes Tun und Unterlassen erfasst, das sich auf die Persönlichkeits- und Identitätskonstituierung auswirken kann, auch wenn es sich um objektiv scheinbar triviale Verhaltensweisen handelt.[183] Mit der äußerlichen Realisierung des allgemeinen Persönlichkeitsrechts in einer Handlung geht die Frage nach der Zurechnung und Verantwortlichkeit dieser Handlung einher.

---

179 *Nettesheim*, in: Diggelmann/Lege/Nettesheim (Hrsg.), Der Schutzauftrag des Rechts, 2011, 8 (48); *Lanzing*, Ethics and Information Technology 2016, 9 (15).
180 *Korsgaard*, Self-Constitution, 2009, S. 1 f.
181 *Kingreen/Poscher*, Grundrechte: Staatsrecht II, 2019, Rn. 437.
182 BVerfG, NJW 1957, 297.
183 *Kieck*, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe, 2019, S. 103.

Die Bestimmung des Begriffs der personalen Identität kann, neben der inneren Dimension des allgemeinen Persönlichkeitsrechts, von der äußeren Verhaltensdimension abgeleitet werden. Danach besteht das Bild der personalen Identität aus der inneren Selbstbestimmung und der äußeren verhaltensbezogenen Realisierung. Daraus ergibt sich als Anforderung für ein Identitätsverwaltungsmodell, dass die innere und die äußere Dimension in dem Modell abgebildet werden müssen. Einerseits muss das Individuum in seinen inneren Entscheidungen über die personale Identität in ihrer graduellen dialogischen Dynamik zur Außenwelt diese Kontrolle ausüben und andererseits muss das Individuum seine äußeren Verhaltensweisen kontrollieren und sich zurechnen lassen können. Beides genießt den Schutz der allgemeinen Handlungsfreiheit in der Auffangfunktion des Art. 2 Abs. 1 GG.

3. Mittelbare Drittwirkung

Die Grundrechtswirkung entfaltet sich grundsätzlich zwischen Staat und Bürger. Der Staat darf nur aufgrund oder durch ein Gesetz in die Grundrechte des Individuums eingreifen. In datenschutzrechtlicher Hinsicht lässt sich daraus das Verbot mit Erlaubnisvorbehalt ableiten, wonach es dem Staat grundsätzlich verboten ist, eine das Recht auf informationelle Selbstbestimmung einschränkende Datenverarbeitung vorzunehmen, es sei denn, es besteht ein Rechtfertigungsgrund. Gleichzeitig wird seit dem *Lüth*-Urteil die objektive Wertordnung der Grundrechte anerkannt und auf das Verhältnis zwischen Privaten erstreckt, sog. mittelbare Drittwirkung.[184] Entsprechend lässt sich aus den Grundrechten über das Abwehrrecht hinaus eine Schutzpflicht im Verhältnis zwischen Privaten ableiten, die als zweite große Dimension der Grundrechte angesehen wird und sich im einfachen Recht abbildet.[185]

Die Ausstrahlungswirkung durch die mittelbare Drittwirkung der Grundrechte lässt sich auf das Machtgefälle zwischen Privaten, vergleichbar mit dem Machtgefälle zwischen Staat und Bürger, übertragen. Demnach wird die mittelbare Grundrechtswirkung bei staatsähnlich agierenden Privaten dahingehend angenommen, dass etwa bei der Gewährleistung der öffentlichen Kommunikation durch Private die Grundrechte als

184 BVerfGE 7, 198 (205 f.).
185 *Masing*, NJW 2012, 2305 (2306).

„Richtlinien“[186] wirken. Dies wird augenscheinlich in dem Verhältnis zwischen den datensammelnden privaten Intermediären mit marktbeherrschender Stellung und dem betroffenen Verbraucher, wenn dabei grundrechtstypische Gefährdungslagen entstehen.[187] In dieser Konstellation wird sogar eine starke Gefahr etwa durch Cybermobbing in sozialen Netzwerken und Zurschaustellung von Straftaten gesehen, auf die der Staat noch nicht ausreichend vorbereitet sei.[188] Dem kann gegenübergestellt werden, dass das Recht gerade das private Umfeld privilegiere unter der Annahme, dass gerade in sozialen Nähebeziehungen die Konflikte besonders von Emotionen geprägt sein können und dieser Bereich entsprechend auch privatrechtlich geregelt werden soll, wie es sich aus dem Schutzbereichsausschluss gemäß Art. 2 Abs. 2 c) DSGVO ergibt. Insgesamt könne der aus der mittelbaren Drittwirkung abgeleitete Schutzauftrag darin bestehen, die Voraussetzungen für eine wirksame und freiwillige Willensentscheidung zu stärken und dabei aber die Grenze zu einer paternalistischen Regelung zu wahren.[189] Entsprechend können aus der mittelbaren Drittwirkung die Grundlagen für das Identitätsverwaltungsmodell hergeleitet werden, das einen Gewährleistungsrahmen nicht nur gegenüber dem Staat, sondern auch gegenüber Privaten schafft. Dieser könnte darin bestehen, dass kontextspezifisch die graduell sich verändernden Risiken über die Datenverarbeitungen in ein Identitätsverwaltungsmodell aufgenommen werden, um dem Individuum eine tatsächliche Selbstbestimmungs- und damit Kontrollmöglichkeit über den Datenverarbeitungsvorgang einzuräumen.

4. Bewertung

Die personale Identität im Grundgesetz wird von dem Schutzbereich des allgemeinen Persönlichkeitsrechts und der allgemeinen Handlungsfreiheit erfasst und erfährt in ihren Ausprägungen im online-Kontext eine Konkretisierung über das Recht auf informationelle Selbstbestimmung und das IT-Grundrecht. Mit dem Recht auf informationelle Selbstbestimmung werden die Realisierung der personalen Identität hinsichtlich der Offenbarung persönlicher Lebenssachverhalte und die möglichen Erkenntnisse aus

186 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 76, 88.
187 *Masing*, NJW 2012, 2305 (2306); *Schliesky*, ZRP 2015, 56 (57).
188 *Ders.*, ZRP 2015, 56 (57); *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 181.
189 *Grimm*, JZ 2013, 585 (588).

dem Kommunikationsverhältnis geschützt. Sobald die offenbarten persönlichen Informationen zum Gegenstand umfangreicher Datensammlungen werden, steigert sich der Schutz gegenüber den generierbaren Persönlichkeitsprofilen und der Kontrollierbarkeit von personalen Identitäten. Darin liegt ein hohes Differenzierungsmaß zum Schutz personaler Identitäten im online-Kontext, da das Recht auf informationelle Selbstbestimmung sich neben den Daten auf die möglichen Erkenntnisse erstreckt und damit auch auf das erwartbare Fremdbild. Das gesteigerte Risiko hinsichtlich des bloßen Nutzungsverhaltens im online-Kontext gegenüber personalen Identitäten wird mit dem IT-Grundrecht geschützt, da sich die Persönlichkeitsentfaltung zunehmend auf informationstechnische Systeme erstreckt und einen erweiterten Schutz verlangt. Demnach schützt das IT-Grundrecht als „digitale Handlungsfreiheit“[190] die personalen Identitäten aus den informationstechnischen Systemen und das Ergebnis aus einem Kommunikationsprozess in Gestalt eines Bildes der personalen Identität. Folglich wird aus den grundrechtlichen Betrachtungen deutlich, dass die personale Identität in ihrem statischen *Idem*-Anteil und dynamischen *Ipse*-Anteil im offline- und online-Kontext gleichermaßen geschützt wird. Somit entfaltet auch das Auffangrundrecht der allgemeinen Handlungsfreiheit seine Schutzwirkung auf den *Ipse*-Anteil der personalen Identität.

Dieses Schutzregime wird den Bedingungen ubiquitärer Datenverarbeitungen gerecht und schafft Rechte, mit denen sich der Betroffene gegen ungerechtfertigte Verhaltens- und Kommunikationsprofile wehren kann. Dies gilt zwar zunächst gegen staatliche Eingriffe, jedoch sieht die mittelbare Drittwirkung der Grundrechte ebenso den Schutz von Datenverarbeitungen durch Private vor. Dieser kommt in dem Verbot mit Erlaubnisvorbehalt zum Ausdruck und in der grundrechtstypischen Gefährdungslage von Datenverarbeitungen durch marktbeherrschende Intermediäre. Somit könnte ein Gewährleistungsrahmen nicht nur durch den Staat, sondern auch durch Private mit der Identitätsverwaltung realisiert werden. Darin würde eine Übertragung der mittelbaren Drittwirkung aus dem offline- in den online-Kontext erfolgen und eine organisatorische und verfahrensrechtliche Vorkehrung mit der Identitätsverwaltung zur Grundrechtsgewährleistung vorgenommen werden können. Diese sollte die verhandlungsfähigen Bilder und Gegenbilder personaler Identitäten einbeziehen und eine *verhandelbare Identität* ermöglichen.

Gleichwohl wird in der Literatur eine Überforderung des Staates bei Sachverhalten im online-Kontext hervorgehoben, wonach die „analoge

190 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 19.

Rechtsordnung" nicht mehr ausreiche und ein Ausgleich geschaffen werden müsse.[191] So sieht etwa Art. 15 der Verfassung des Landes Schleswig-Holstein ein spezifisches online-Grundrecht vor, das die „digitale Privatsphäre" schützt. Ebenso ist in Art. 14 Landesverfassung Schleswig-Holstein der Zugang zu digitalen Basisdiensten geschützt, worin die Gewährleistung einer „digitalen Daseinsvorsorge" gesehen werden kann. Inwieweit es sich dabei um neue Rechte mit einem weiteren Schutzbereich handelt, erscheint jedoch fraglich. Denn der Wortlaut erfasst zwar den online-Kontext, doch dieser wird auch von dem grundrechtlichen Wortlaut der Art. 2 Abs. 1 GG i. V. m. Art. 1 GG im Wege der Auslegung umfasst, so dass in der Begründung eines Grundrechts über die „digitale Privatsphäre" vielmehr eine Klarstellung zu sehen ist.

Insgesamt lässt sich aus dem grundrechtlichen Schutzregime im online-Kontext ein Modell der Identitätsverwaltung zur Gewährleistung des Grundrechtsschutzes ableiten. Damit wäre die Identitätsverwaltung nicht ausschließlich über den Markt zu realisieren, sondern findet eine grundrechtliche Verankerung im Rahmen der staatlichen Daseinsvorsorge. In Anbetracht der grundrechtlichen Abwehrdimension gegenüber staatlichem Handeln kommen hybride Formen der Identitätsverwaltung in Betracht, bei denen ein Nebeneinander von staatlicher und privater Identitätsverwaltung denkbar wäre.[192]

III. Personale Identität im amerikanischen Recht

Das liberale Verfassungskonzept zum Schutz der Privatheit im amerikanischen Rechtsraum könnte für das Verständnis des Begriffs der personalen Identität und des Identitätsverwaltungsmodells in Anbetracht internationalisierter Datenverarbeitungen aufschlussreich sein. Dabei soll nach der rechtlichen Begründung des „*right to privacy*" der Blick auf die Ausprägungen des „*right to be let alone*", der „*reasonable expectation of privacy*" und des „*informational privacy*" gerichtet werden.

Für die Begründung des „*right to privacy*" werden als rechtshistorische Quelle einerseits der Aufsatz von *Warren/Brandeis*[193] und andererseits das Urteil *Whalen v Roe* mit Bezugnahme auf den Aufsatz von *Warren/Brandeis*

191 *Schliesky*, ZRP 2015, 56 (58).
192 *Hornung*, in: Roßnagel (Hrsg.), Wolken über dem Rechtsstaat?, 2015, 189 (206).
193 *Warren/Brandeis*, Harv. L. R. 1890, 193.

angeführt.[194] Dabei ging es um den Schutz des Rechts am eigenen Bild, welches als ein Kontrollkonzept beschrieben wurde und als Ursprung für das im vierten Verfassungszusatz anerkannten „*right to privacy*" gilt.[195] Das „*right to privacy*" dient demnach als Schutzkonzept gegenüber Voyeurismus und der damals neuartigen Verbreitung der „*Yellow Press*". Dazu gehöre das von *Thomas Cooley* beschriebene „*right to be let alone*", wonach der maßgebliche Anknüpfungspunkt der Schutz vor „*mental pain*" und „*distress*" infolge des hohen Verbreitungsgrades der „*Yellow Press*" und der darin enthaltenen Trivialitäten sei.[196] Weitergehend werde der Schutz des individuellen Körpers, des individuellen Emotionsgefüges und der Reputation gegenüber der Sozialisation erfasst.[197] Gegen solche Eingriffe in private Belange etwa durch die Darstellung einer Person „im falschen Licht" wirkt das Rechtsmittel des „*remedy*" als Schutzmechanismus.[198]

Als weitere Ausprägung komme die „*reasonable expectation of privacy*" aus der Entscheidung *Katz v United States* in Betracht, die dem Schutz des Bürgers gegen die Offenlegung von Informationen diene.[199] Nach diesem Recht müssten die Kriterien der subjektiven Privatheitserwartung, der objektiven Vernünftigkeit und Legitimität dieser erfüllt sein.[200] Demgegenüber umfasst das „*right to be let alone*" den Schutz gegenüber staatlichen Beschränkungen.[201] Aus diesen Schutzausprägungen ist dagegen das Recht auf „*informational privacy*" nur im geringen Maß ausgeprägt und der „*Supreme Court*" hat in der Entscheidung *NASA v Nelson* die Existenz eines Rechts auf „*informational privacy*" ausdrücklich offengelassen.[202]

Insgesamt basiert das amerikanische Verständnis über die Privatheit auf einem liberalen verfassungsrechtlichen Regelungsgefüge, welches zwar vereinzelt auch auf die Menschenwürde zurückgeführt wird, im Gesamten jedoch als Schutzregime auf das Abwehrrecht als „*remedy*" gegenüber öf-

194 *Black*, Cornell Int'l LJ 34 (2001), 397, (414 f.), Fn. 87, 101; *Whalen v. Roe*, 429 U.S. 589 (1977).
195 *Whitman*, Yale L. J. 2004, 1151 (1213).
196 *Warren/Brandeis*, Harv. L. R. 1890, 193 (194–196): „Triviality destroys at once robustness of thought and delicacy of feeling. No enthusiasm can flourish, no generous impulse can survive under its blighting influence."
197 *Dies.*, Harv. L. R. 1890, 193 f.
198 *Prosser*, Cal. Law Review 1960, 383 (398 f).
199 *Wittmann*, ZaöRV 73 (2013), 373 (386); *Katz v. United States*, 389 U.S. 347 (1967).
200 *Ders.*, ZaöRV 73 (2013), 373 (387).
201 Section 23 der Verfassung von Florida, *ders.*, ZaöRV 73 (2013), 373, (407) Fn. 208.
202 *Ders.*, ZaöRV 73 (2013), 373 (383); *NASA v. Nelson*, 562 U.S. 134 (2011).

fentlichen Darstellungen zurückgeht. Im Einzelnen sind die Gefährdungslagen durch neue Technologien gegenüber der Privatheit zum Gegenstand höchstrichterlicher Rechtsprechung geworden, wie es in der Entscheidung *United States v Maynard* sichtbar wurde. Darin wurde die *Mosaik-Theorie* angewendet, bei der es um den Schutz gegen Profilbildungen geht, die mit der Zusammenführung von GPS-Standortdaten ein ausdifferenziertes Bild der Persönlichkeit ermögliche und entsprechenden Schutzbedarf auslöse.[203] Denn im Gegensatz zu der kurzfristigen Überwachung, die nicht vom vierten Verfassungsgrundsatz umfasst sei, stünde die „*reasonable expectation of privacy*" einer langfristigen und kumulativen Überwachung individueller Bewegungen entgegen. Gleichwohl vertrat die Richterin *Sotomayor* in dem „*Supreme Court*"-Fall *United States v Jones* ein Sondervotum, wonach die kurzfristige GPS-Überwachung in der Öffentlichkeit auch zu Persönlichkeitsprofilen führen könne und daher ein verfassungsrechtlich bedenkliches Missbrauchspotential begründe.[204]

Indem von der „*Federal Trade Commission*" im Hinblick auf die Profilerstellung der Bedarf nach „*Data Brokern*" und Transparenzregeln zum Schutz von Verbrauchern als Kontrollmöglichkeit empfohlen wurde, wird ein Schutzbedarf teilweise anerkannt.[205] Weiter wird die Kontrolle als Schutzmaßnahme für den Verbraucher in der vom Weißen Haus unter der Regierung *Obama* im Jahr 2011 vorgelegten Strategie für „*Trusted Identities in Cyberspace – Enhancing Online Choice, Efficiency, Security, and Privacy*"[206] ebenfalls anerkannt. In dieser Strategie erscheinen implizite Bezugnahmen auf europäische Datenschutzprinzipien, mit denen die Ausübung individueller Freiheitsrechte über ein ausdifferenziertes, transparentes und interoperables Identitäts- und Accountverwaltungssystem als ein (online) „*Identity Ecosystem*" gefördert werden soll. Gleichzeitig liegt einem solchen System ein liberales Privatheitsverständnis zugrunde, wonach ein grundsätzliches Verbot der Datenverarbeitung, wie es sich aus dem europäischen Verbot mit Erlaubnisvorbehalt ergibt, fehlt. Obwohl die rechtskulturellen Divergenzen hinsichtlich des Schutzes der Privatheit augenscheinlich sind, fällt das Schutzinteresse an Identitäten und Profilen im online-Kontext

203 *Ders.*, ZaöRV 73 (2013), 373 (393) Fn. 109; *United States v. Maynard*, Nr. 08–3030 (2009); *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 61.

204 *United States v. Jones*, 565 U.S. 400 (2012), Sondervotum *Sotomayor*, S. 3.

205 *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2016, 535 (544).

206 *White House*, National Strategy for Trusted Identities in Cyberspace, 2011, S. 21 f.

auf, wie es mit dem Sondervotum der Richterin Sotomayor und der Initiative des Weißen Hauses nachgewiesen wurde.

Insgesamt wird aus der amerikanischen Perspektive der Kontrollbegriff über das eigene Bild eingesetzt und der Bedarf an Interoperabilität zum Schutz der Privatheit angeführt, welches aufschlussreiche Kriterien für ein Identitätsverwaltungsmodell sind. Hinsichtlich einer Konkretisierung des Identitätsbegriffs werden die Schutzdimensionen aus dem „*right to privacy*" über das Bestehen eines absoluten Schutzes der Privatheit ebenfalls deutlich. Gleichwohl konnte ein Schutzregime über den Identitätsbildungsprozess in Gestalt eines Rechts auf Selbstbestimmung und Selbstbewahrung nicht nachgewiesen werden.

IV. Ergebnis

Die Bestimmung des Begriffs der personalen Identität und die Bestimmung der Grundlagen eines Identitätsverwaltungsmodells lassen sich aus der europäischen Grundrechtecharta und den Grundrechten ableiten. Daneben wurden die Annahmen des amerikanischen Rechts zum Schutz der Identität herangezogen, um für das Identitätsverwaltungsmodell weitere Anhaltspunkte generieren zu können. Insgesamt konnte nachgewiesen werden, dass die personale Identität grundrechtlich in ihrem statischen *Idem*- und dynamischen *Ipse*-Anteil geschützt wird. Dabei wurde als Schutzgegenstand die kommunikative Beziehung im Privatleben und die Selbstdarstellung in der Sozialsphäre herausgearbeitet. Es konnte jeweils die Kontrollmöglichkeit über das Bild der personalen Identität als Selbstbild und als Gegenstand der Selbstdarstellung bestimmt werden. Gleichzeitig steht dieses Bild im Verhältnis zum wahrgenommenen Gegenbild, so dass sich diese gegenüberstehen und die Vergegenbildlichung der Gegenstand privater Verhandlung über die Bilder personaler Identitäten werden kann. Dazu lässt sich das Recht auf Neubeginn anführen, wonach das Gegenbild gänzlich in Gestalt eines *tabula rasa*-Rechts für einen Neubeginn weichen muss. Darin lässt sich eine absolute Kontrolle über die Bilder personaler Identitäten erblicken, wohingegen die Informationen über eine Identität im Rahmen des Rechts auf informationelle Selbstbestimmung der relativen Kontrolle im Hinblick auf das wahrgenommene Gegenbild der personalen Identität unterliegen. Daraus geht die Kommunikation über die personale Identität als weiterer Schutzgegenstand hervor, so dass Datensätze, Informationen oder Erkenntnisse in das Identitätsverwaltungsmodell einzubeziehen sind. Weiter ergibt sich für ein Identitäts-

verwaltungsmodell der Bedarf an der Abbildung rechtlicher Schutzmechanismen gegenüber privaten Intermediären mit marktbeherrschender Stellung. Dies würde sich als Ausprägung der mittelbaren Drittwirkung des Rechts auf informationelle Selbstbestimmung und des IT-Grundrechts oder gar aus der unmittelbaren Drittwirkung des europäischen Rechts auf informationelle Selbstbestimmung darstellen können.

Insgesamt bedarf es eines Identitätsverwaltungsmodells, welches die rechtlichen Schutzregime über ein technisch interoperables Konzept miteinander in Verbindung bringt. Dahingehend ist die Strategie des Weißen Hauses, über ein „*Identity Ecosystem*" eine Lösungsmöglichkeit zu bilden, über die amerikanische Rechtskultur hinaus für die europäische Rechtskultur aufschlussreich. Denn gerade in dieser Strategie kommen die wellenförmigen rechtskulturellen Einflüsse durch die Bezugnahme auf Prinzipien des europäischen Datenschutzrechts zum Ausdruck.

B. Personale Identität aus fachübergreifenden Perspektiven

Die personale Identität bedarf in ihrer Begriffsbestimmung und für die *Modellbildung der Identitätsverwaltung* einer über das Recht hinausgehenden Betrachtung. Denn die Annahme einer personalen Identität, die aus dem eingeführten statischen *Idem*-Anteil und dem dynamischen *Ipse*-Anteil besteht, verlangt eine fachübergreifende Einordnung. Mit dieser sollen Phänomene der personalen Identität über das Recht hinaus beleuchtet werden, um maßgebliche Eigenschaften für das Identitätsverwaltungsmodell herauszuarbeiten. Dafür sollen im Folgenden die informationstechnische (I.), die sozialpsychologische (II.) und die kommunikationspsychologische Perspektive (III.) mit einer abschließenden Analyse zur Übertragbarkeit auf die einfachrechtliche personale Identität (IV.) einbezogen werden.

I. Informationstechnische Perspektive

Die personale Identität aus der informationstechnischen Perspektive kommt allein in der digitalen Ausprägung vor und besteht aus dem Informationsgehalt der „Bits und Bytes". Maßgeblich aus der informationstechnischen Perspektive ist dabei, dass die Funktionalität der Authentifizierung und Identifizierung im Vordergrund steht und nachrangig die kon-

krete Ausgestaltung der kontextspezifischen digitalen Identität,[207] was ausschließlich den *Idem*-Anteil der personalen Identität betrifft. Mit der Identifizierung unter Einsatz eines *Identifizierers* („*Identifier*") wird durch die Verknüpfung an einen Namen der Zugang gewährt. Demgegenüber wird bei der Authentifizierung der Zugang an den Inhaber der Zugangsdaten gewährt. Nach beiden Vorgängen wird die Zugriffskontrolle eingeräumt, die mit spezifischen Rechten einer Person verbunden sein kann und sich daraus eine digitale Identität begründen lässt.[208] Die Einräumung der Zugriffskontrolle erfolgt meistens mit einem *Identifizierer*, der aus Attributen der Person oder einer Zeichenfolge besteht, mit der jeweils eine eindeutige und sichere Identifizierung ermöglicht wird. Damit wird Vertrauen über die Richtigkeit der Identität geschaffen, da nur der Inhaber des *Identifizierers* den Vorgang zur Einräumung der Zugriffskontrolle ausüben können sollte, wie es mit einem Mitarbeiterausweis und einer konkretisierten *Berechtigungsverwaltung* möglich ist.[209] Sobald ein Dritter die Infrastruktur für die Identifizierung und Authentifizierung zur Verfügung stellt, kann das Vertrauen zusätzlich von der Reputation des Dritten beeinflusst werden, wie es bei der Erteilung der elektronischen Signatur der Fall ist.[210] Diese wird von einer zertifizierten Stelle durch die Vergabe von Zertifikaten nach der Identifizierung des Nutzers an diesen ausgegeben. Somit ist Identität aus der informationstechnischen Perspektive in der IT-Sicherheit einzuordnen, da es um die sichere Identifizierung und Authentifizierung und um den Schutz der gespeicherten Attribute geht,[211] wobei die konkrete inhaltliche Ausgestaltung der Identität nachrangig bleibt.

Gleichwohl herrscht aus der informationstechnischen Perspektive kein statisches Verständnis über den Lebenszyklus einer Identität. Vielmehr können sich die Attribute etwa auf einem Mitarbeiterausweis oder die zugewiesenen Berechtigungen ebenfalls ändern. Damit kommt erweiternd

---

207 *Ralston/Reilly/Hemmendinger* (Hrsg.), Encyclopedia of computer science, 2003, zu „Identity"; *Broy/Spaniol* (Hrsg.), VDI-Lexikon Informatik und Kommunikationstechnik, 1999, zu „Identität"; *Greulich* (Hrsg.), Der Brockhaus Computer und Informationstechnologie, 2003, zu „Bezeichner".

208 *Greulich* (Hrsg.), Der Brockhaus Computer und Informationstechnologie, 2003, zu „Authentifizierung" und „Identifikation"; *Windley*, Digital identity, 2005, S. 50.

209 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 127; *Windley*, Digital identity, 2005, S. 9–13.

210 *Bidgoli*, Handbook of information security, 2006, Volume 2, S. 232; *Windley*, Digital identity, 2005, S. 15–20.

211 *Ders.*, Digital identity, 2005, S. 11.

der Lebenszyklus von Identitäten hinzu, der die Begründung einer Identität, ihre Speicherung zur Abrufbarkeit, ihre Verwendung und ihre Löschung umfasst, was in einer vertrauenswürdigen Identitätsverwaltungsstruktur zu berücksichtigen wäre.[212] Damit lässt sich ein Wandel von dynamischen *Ipse*-Anteilen einer personalen Identität aus dem Lebenszyklus in *Idem*-Anteile vollziehen, wenn das vorübergehende Attritbut einer Zugangsberechtigung etwa als gewähltes Vorstandsmitglied zu vertraulichen Dokumenten zum statischen Identifizierungsmerkmal wird.

Im Rahmen des Lebenszyklus einer personalen Identität sieht die informationstechnische Perspektive neben der vertrauenswürdigen Identifizierung auch die übergreifende Verbindung und Teilung von Attributen und digitalen Identitäten vor,[213] was gerade das *Big Data*-Phänomen ausmacht. Damit ist die personale Identität begrifflich aus der informationstechnischen Perspektive nachrangig gegenüber dem Vorgang der sicheren Identifizierung und Authentifizierung. Das Konzept einer digitalen Identität, das sich aus kontextabhängigen Attributen einer Person zusammensetzt, steht daher in direkter Verbindung mit der *Berechtigungsverwaltung*.

II. Sozialpsychologische Perspektive

1. Personale Identität im offline-Kontext

Die personale Identität aus sozialspsychologischer Perspektive unterliegt gesamtgesellschaftlichen Veränderungen und dem Wandel der aktuell wirkenden sozialpsychologischen Schulen. Dabei können die Theorien zur Identität und die Identitätsfrage in besonderem Maße vom gesamtgesellschaftlichen Wandel und kulturellen Ausgangssituationen geprägt sein. In der von *Erikson*[214] geprägten Theorie zur Identität werden etwa acht Phasen der Identitätsbildung angenommen, die kausal für die spätere Persönlichkeit und mögliche Konfliktlagen sein können. Darin kommt das Verständnis eines „inneren Kapitals" zum Ausdruck, welches sich aufgrund der Entwicklungsphasen in der frühen Kindheit bis zur Adoleszenzphase bildet, die zu der Annahme einer Einheitlichkeit und Kontinuität von Identität führt.[215] Der personalen Identität komme nach dieser Theorie ab

212 *Ders.*, Digital identity, 2005, S. 29–34.
213 *Bidgoli*, Handbook of information security, 2006, Volume 2, S. 231.
214 *Erikson*, Identität und Lebenszyklus, 2015, S. 150 ff.
215 *Keupp*, Identitätskonstruktionen, 1999, S. 28 f. mit Verweis auf *Erikson.*

einer bestimmten Lebensphase die Eigenschaft einer „unitären Identität“[216] zu, die sich anschließend in der Realwelt bewege. Dem steht ein theoretisches Verständnis der personalen Identität gegenüber, welches sich durch Kontinuität der Identitätsbildung auszeichnet und keiner Begrenzung auf Lebensphasen in einer Biographie unterliegt. Die Identität als *homo identicus*[217] wird danach unabhängig von der Lebensphase und dem Lebensalter in einem Beziehungsgefüge zwischen den inneren Strukturen und äußeren sozialen Strukturen gesehen, so dass in der modernen funktional differenzierten Gesellschaft sogar das „Problem der personalen Identität“ auftauchen könne.[218]

Nach der vorliegend gefolgten Schule unterliegt die Identität einem inneren und äußeren Dialog, der eine kontinuierliche Konstruktion der Identität ermöglicht, so dass Identität aus fortschreitenden Handlungen und Narrationen besteht.[219] Diese Betrachtung ermöglicht einen zeit- und kontextbezogenen Identitätsbegriff und legt die Vorstellung von mehreren Identitäten nahe. Entsprechend wird in der Identitätsforschung auch von „Patchwork-Identitäten“ gesprochen, die kontinuierlichen Veränderungen und den Wandlungen der narrativen Identitätsdarstellung unterliegen, so dass die Identität „aus einem Guß“ empirisch nicht nachweisbar sei.[220] Folglich finden Identitätsrealisierungen in einem inneren und äußeren Dialog statt, der sich unter dem Obersatz „Ich bin viele“ zusammenfassen und differenzieren lässt. Danach wird die personale Identität in ein berufliches Ich („Ich arbeite also bin ich“), ein soziales Ich („Ich liebe, also bin ich“), ein physisches Ich („Ich bin da, also bin ich“), ein materielles Ich („Ich habe, also bin ich“) und ein religiöses Ich („Ich glaube, also bin ich“) unterteilt.[221] Gleichzeitig unterliegen diese Teile der Identitäten keinem separierten Verhältnis, sondern stehen im Dialog zueinander, entfalten untereinander Wechselwirkungen und unterliegen so kontinuierlichen Veränderungen. Darin kommen neben der personalen Identität weitere Teilidentitäten als kontextspezifische Ausprägungen zum Ausdruck, aus denen

216 *Turkle*, Leben im Netz – Identität in Zeiten des Internet, 1999, S. 422.
217 *Shapiro*, Negotiating the nonnegotiable, 2017, S. 10 f.
218 *Meuter*, in: Kolmer/Wildfeuer/Krings u.a. (Hrsg.), Neues Handbuch philosophischer Grundbegriffe, 2011, Bd. 2, S. 1213.
219 1. Teil, C., II., 2.; *Keupp*, Identitätskonstruktionen, 1999, S. 99–103, 215.
220 *Ders.*, Identitätskonstruktionen, 1999, S. 74, 110.
221 *Lippmann*, Identität im Zeitalter des Chamäleons, 2014, S. 31 ff.; ebenso *Kieck*, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe, 2019; *Meuter*, in: Kolmer/Wildfeuer/Krings u.a. (Hrsg.), Neues Handbuch philosophischer Grundbegriffe, 2011, Bd. 2, S. 1213.

sich die einheitliche personale Identität in Gestalt einer dynamischen Identitätsbildung darstelle.[222]

Die personale Identität verkörpert demnach aus sozialpsychologischer Perspektive eine beständige alltägliche Identitätsarbeit, die von Selbst- und Identitätskonstruktionen gekennzeichnet ist und sich kontinuierlich in der Neuentstehung über die Teilidentitäten befindet. Im offline-Kontext führt die Selbstdarstellung etwa in einem berufsorientierten Verein zur Begründung einer Teilidentität mit der entsprechenden fachlichen Selbstdarstellung, die jedoch mit der Beendigung der Mitgliedschaften ebenso in ihrer Existenz und Wirkkraft abgeschlossen wird. Damit kommt der personalen Identität ein amöbenartiger Charakter zu, der von einer kontextbezogenen Darstellung der personalen Identität geprägt ist und von dem Betrachtungswinkel abhängt.

2. Personale Identität im online-Kontext

Aus sozialpsychologischer Perspektive werden spezifische Ausprägungen der personalen Identität im online-Kontext beschrieben. Dabei lässt sich grundsätzlich die Übertragbarkeit der personalen Identität auf den online-Kontext feststellen, wenn die sozialen Beziehungen und wirtschaftlichen Handlungen im offline- und im online-Kontext gleichermaßen wahrgenommen werden. Gleichzeitig wird aus der psychologischen Perspektive eine online-spezifische Verschiebung bei der Identitätsforschung festgestellt. In den sozialen Medien wird die Selbstdarstellung in ihrer Reichweite durch die Entterritorialisierung erheblich erleichtert, so dass die Begründung sozialer Kontakte und Freundschaften im online-Kontext ungehemmter als im offline-Kontext erfolge.[223] Die Hintergründe derartiger Phänomene können in psychologischen Wahrnehmungsverzerrungen liegen, die dazu führen, dass die Selbstdarstellungen im online-Kontext als reale Identitäten wahrgenommen werden, obwohl es sich um virtuelle Identitäten auf Probe handelt.[224] Darüber hinaus können die Rahmenbedingungen des online-Kontextes dafür genutzt werden, dass das Individuum leichter eine Selbstmaskierung mit falschen Eigenschaften über die ei-

222 *Lippmann*, Identität im Zeitalter des Chamäleons, 2014, S. 33; *Shapiro*, Negotiating the nonnegotiable, 2017, S. 19–23.

223 *Kneidinger-Müller*, in: Schmidt/Taddicken (Hrsg.), Handbuch Soziale Medien, 2017, S. 2.

224 *Turkle*, Leben im Netz – Identität in Zeiten des Internet, 1999.

gene Identität vornehmen und sich in den „multiplen Identitäten" ausprobieren kann, was sich wiederum auf die Persönlichkeitsentwicklung auswirken könne.[225] Damit könne ein Identitätsexperiment vorgenommen werden, indem etwa die geschlechtliche Identität als „erwünschte digitale Identität" im online-Kontext in Erscheinung tritt.[226] Aus diesen Phänomenen über die Darstellung der personalen Identität im online-Kontext lassen sich spezifische Gestaltungsmöglichkeiten und Gefährdungslagen ableiten, die in einem Identitätsverwaltungsmodell einzubeziehen sind.

Demnach lässt sich aus der sozialpsychologischen Perspektive die enge Verbindung über das Verständnis der personalen Identität mit den jeweiligen theoretischen Schulen abbilden. Nach heutigen Erkenntnissen stellt sich ein dynamischer Identitätsbegriff als vorherrschend dar, der sich über die Biographie kontinuierlich konstituiert und bei dem sich die personale Identität in kontextbezogenen Teilidentitäten realisiert. Gleichzeitig unterliegt die personale Identität im online-Kontext anderen Bedingungen, welche sich in ihrer Realisierung und Konstituierung auf die personale Identität auswirken und in Wechselwirkung[227] zur personalen Identität im offline-Kontext stehen können.

III. Kommunikationspsychologische Perspektive

Mit einem in der Sozialpsychologie herrschenden dynamischen Identitätsbegriff, der sich biographisch kontinuierlich und konstituierend realisiert, bedarf es der Einbeziehung der kommunikationspsychologischen Perspektive. Denn der personalen Identität kommt zwar eine statische Dimension zu, diese wird jedoch aus philosophischer und sozialpsychologischer Perspektive mit einer dynamischen Dimension über die sich realisierenden Teilidentitäten erweitert. Diese Ausprägungen der personalen Identität sind nicht solipsistisch einzuordnen, sondern stehen in einer kommunikativen Beziehung. Die personale Identität steht im Rahmen ihrer Biographie in kommunikativen Beziehungen, was die kommunikationspsychologischen Betrachtungen rechtfertigt.

---

225 *Dies.*, Leben im Netz – Identität in Zeiten des Internet, 1999, S. 286–289, 329; ebenso das Phänomen „identitätsbildender Selfies" beschreibend, *Dreier*, Bild und Recht, 2019, S. 197.

226 *Herrmann/Federrath*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 131 (133); zur Selbstmaskierung, *Kneidinger-Müller*, in: Schmidt/Taddicken (Hrsg.), Handbuch Soziale Medien, 2017, S. 3.

227 *Turkle*, Leben im Netz – Identität in Zeiten des Internet, 1999, S. 15.

Danach ist die im Rahmen der Biographie bestehende Verbindung zum Kommunikationspartner durch eine unendliche Folge von Interpunktionen geprägt, in denen der Anfang und das Ende des Mitteilungsaustausches nicht feststellbar sind, sich aber über Rückkoppelungen in der Kommunikation[228] über die entstandenen Bilder personaler Identitäten abbilden lassen. Die digitale und technische Kommunikation findet auf der syntaktischen Ebene statt, wohingegen die menschliche Kommunikation die Beziehungsebene und damit semantische Ebene umfasst. Auf beiden Kommunikationsebenen könne der Empfänger die Mitteilung bestätigen, verwerfen oder entwerten,[229] was sich auf die Kommunikation über die Bilder personaler Identitäten erweitern lässt und die Frage nach *Instruktionen* für die Kommunikation aufwirft.

Gleichermaßen gilt für den offline- und online-Kontext, dass der Zweck von Kommunikation in der Restaurierung der Kommunikation liegen kann, die mit der Steigerung von zwischenmenschlicher Koordination und der Herbeiführung von Konsens erfolgt.[230] Dennoch gibt es paradoxe zwischenmenschliche Kommunikationen, die mit einer realen Wahlmöglichkeit, aus dem System austreten zu können, oder mit der Einführung von Regeln[231] als *Instruktionen* aufgelöst werden können. Denn algorithmusbasierte Profile können ebenfalls eine echte Wahlmöglichkeit und *Instruktionen* zur Profilerstellung verlangen. Der Schutz gegen diese Fremdbilder personaler Identitäten in Gestalt von Profilen kann entweder in einer Beendigung des Dienstes als „Ausstieg aus dem System" oder aber aus modifizierten *Instruktionen* über die Erstellung von Profilen bestehen.

Demnach bedarf es der Unterscheidung zwischen unmittelbaren Erkenntnissen und der instruierten Erkenntniserlangung als „Kalkül"[232]. Denn mit den vorher festgelegten *Instruktionen* lassen sich die Erkenntnismöglichkeiten begrenzen. Insofern ermöglichen die *Instruktionen* eine Kanalisierung der Erkenntnisse und stellen eine Metakommunikationsebene dar. Dabei kommen drei Ordnungen[233] der Kommunikation zum Ausdruck, die sich auf ein Modell der Identitätsverwaltung auswirken können. Als erste Ordnung kommt der Informationsgehalt über das Bild der personalen Identität in Betracht, als zweite Ordnung die Bedeutung dieser als

228 *Watzlawick/Beavin/Jackson*, Menschliche Kommunikation, 2016, S. 144 f.
229 *Dies.*, Menschliche Kommunikation, 2016, S. 70.
230 *Schmidt*, in: Haft/Schlieffen (Hrsg.), Handbuch Mediation, 2016, § 8 Rn. 7, 31.
231 *Watzlawick/Beavin/Jackson*, Menschliche Kommunikation, 2016, S. 50.
232 *Dies.*, Menschliche Kommunikation, 2016, S. 46–50; *Reisinger*, Rechtsinformatik, 2016, S. 70–71.
233 *Dies.*, Menschliche Kommunikation, 2016, S. 287 f.

Erkenntnisgehalt auf der Metaebene und in der dritten Ordnung das Wissen über die zwei Ordnungen und eine intuitiv geprägte Perspektive auf die personale Identität als Gesamtheit. Maßgeblich sind die erste und zweite Ordnung für die Modellbildung, da mit ihnen die personalen Identitäten und die Erkenntnisse über diese unter Einbeziehung von *Instruktionen* erfolgt.

IV. Zusammenfassung

In den fachübergreifenden Darstellungen wurden die informationstechnische, sozialpsychologische und kommunikationspsychologische Perspektive einbezogen, um Eigenschaften für das Identitätsverwaltungsmodell bestimmen zu können. Dabei lässt sich die personale Identität aus der informationstechnischen Perspektive schwerlich definieren, sondern unterliegt vorrangig dem Ablauf der Identifizierung und der Authentifizierung. Gleichwohl können die dafür eingesetzten *Identifizierer* und die digitalen Attribute der Person als digitale Identitäten über die *Berechtigungsverwaltung* in Erscheinung treten. Für die Bestimmung der digitalen Identität können die Attribute statisch und dynamisch im Rahmen des Lebenszyklus mit der personalen Identität verbunden sein. Diese technische Ausprägung steht in Übereinstimmung mit dem sozialpsychologischen Verständnis einer dynamischen personalen Identität, die sich kontinuierlich und kontextspezifisch realisiert. Dabei konnte dieses für den offline-Kontext geltende Phänomen der personalen Identität auch auf den online-Kontext übertragen werden. Gleichwohl erfolgte der Nachweis, dass die Rahmenbedingungen im online-Kontext eine Selbstmaskierung und das Ausprobieren „multipler Identitäten" erleichtern. Damit ist in der Differenzierung zwischen der personalen Identität im online- und im offline-Kontext zugleich eine Wechselwirkung zwischen diesen Kontexten festzustellen.

Dass der Begriff der personalen Identität auch in einem Kommunikationsvorgang einzuordnen ist, wird mit diesen Wechselwirkungen und den Verhandlungen über die Bilder personaler Identitäten augenscheinlich, so dass die Einbeziehung kommunikationspsychologischer Betrachtungen gerechtfertigt ist. Es kommen für den Kommunikationsprozess übergeordnete *Instruktionen* für die Bilder personaler Identitäten in Betracht, so dass diese auch den „Konstruktionsarbeiten"[234] über die personale Identität die-

234 *Kieck*, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe, 2019, S. 33

nen und damit als Meta-Modell[235] einzuordnen sind. Darin kann ein Verfahren zur Kanalisierung[236] der personalen Identitäten für ein Identitätsverwaltungsmodell liegen und einen kontinuierlichen Aushandlungsprozess über die personale Identität ermöglichen.

C. Ergebnis: Statische und dynamische personale Identitäten

Die personale Identität als zentraler Gegenstand eines Identitätsverwaltungsmodells kann aus Art. 8 GRC über den Schutz der personenbezogenen Daten und dem Kombinationsgrundrecht nach Art. 7, 8 GRC mit der personalen Identität als Ausprägung der Privatheit begründet werden.[237] Dabei kommen in dem Konzept der personalen Identität eine innere und eine äußere Dimension zum Ausdruck, die sich im Rahmen des allgemeinen Persönlichkeitsrechts in dem Recht auf Selbstbestimmung und dem Recht auf Selbstdarstellung auf der einen Seite und in der allgemeinen Handlungsfreiheit auf der anderen Seite abbilden. Daneben erfolgte die Einordnung in dem Recht auf informationelle Selbsbestimmung. Die personale Identität differenziert sich demnach in einen solipsistischen Teil und einen kommunikativen Teil, wie es in dem Modell nach *Ricœur* seine philosophische Verankerung[238] findet.

Folglich ist die personale Identität von einer Dynamik geprägt, die sich in der informationellen Selbstbestimmung auch in den darin geregelten Betroffenenrechten, Art. 8 Abs. 2 GRC, und dem grundrechtlichen Recht auf Neubeginn sowie dem Recht am eigenen Bild nachweisen lässt. Gleichzeitig ist dabei der Bedarf erkennbar, einen Einfluss in Gestalt von Kontrolle über die Datensätze und Erkenntnisse der kontextspezifischen Datenverarbeitung ausüben zu können. Davon umfasst sind die Kontrolle am eigenen Bild und das mögliche Gegenbild zur personalen Identität.[239] Ferner lässt sich aus dem angloamerikanischen Recht ebenfalls ein Kontrollrecht über den Schutz der Privatheit ableiten.

Die Anerkennung eines im Verfassungsrecht verwurzelten dynamischen Identitätsbegriffs lässt sich auch auf die Erkenntnisse fachübergreifender

---

235 *Steinmüller*, Information, Modell, Informationssystem, S. 51. Als Meta-Modell kommen die Problemlösungen von Informationsverarbeitungen in Betracht, die in Software mit *Instruktionen* überführt werden könnten.
236 *Luhmann*, Legitimation durch Verfahren, 2017, S. 12.
237 2. Teil, A., I., 4.
238 1. Teil, C., II., 2., b).
239 2. Teil, A., II.

Betrachtungen stützen. Denn neben der informationstechnischen Perspektive zur Identitätsverwaltung als *Berechtigungsverwaltung* nimmt die sozialpsychologische Perspektive eine Differenzierung zwischen dem online- und offline-Kontext vor und versteht die personale Identität als eine sich situativ realisierende Ausprägung eines Individuums.[240] Demnach besteht die Bildung der Identität aus einem lebenslangen Prozess und wird von *Kieck* als ein „Puzzle von Teilidentitäten" beschrieben.[241] Maßgeblich ist dabei die Ablehnung eines statischen Identitätsbegriffs, bei dem die Identität als ein Produkt oder ein Ergebnis der Identitätsbildung in Erscheinung tritt.[242] Folglich muss für die Modellbildung die spiegelbildliche Übertragung der Identitätsverwaltung vom offline-Kontext in den online-Kontext vorgenommen werden. Zudem soll in dem Modell die Verhandlung zwischen dem dargestellten Bild und dem entstandenen Gegenbild als Ergebnis eines Kommunikationsprozesses unter *Instruktionen* im online-Kontext[243] abgebildet werden.

240 2. Teil, B., I. – II.
241 *Kieck*, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe, 2019, S. 33.
242 *Dies.*, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe, 2019, S. 93.
243 2. Teil, B., III.

3.Teil: Anforderungen an die Identitätsverwaltung

Die grundrechtliche und fachübergreifende Verankerung der personalen Identität im Hinblick auf ein Identitätsverwaltungsmodell bedarf ebenso der einfachrechtlichen Einordnung des Begriffs der personalen Identität. Diese ist für die Begründung eines Identitätsverwaltungsmodells erforderlich, um die personale Identität in ihren dynamischen *Ipse*-Anteilen und in ihren statischen *Idem*-Anteilen abbilden zu können. Dafür müssen die einfachrechtlichen Typologien zur personalen Identität (A.) herausgearbeitet werden, da diese den unmittelbaren Anknüpfungspunkt für die Modellbildung darstellen. Weiter ist für das Identitätsverwaltungsmodell die Ebene der Erkenntniserlangung über die personale Identität einzubeziehen, was mit dem Modell über Daten-Informationen-Wissen (B.) erfolgt. Ebenso verlangt die Identitätsverwaltung die Steuerung der personalen Identitäten, die mit dem Konzept der Kontrolle über die Erkenntnismöglichkeiten der personalen Identität (C.) abgeleitet werden soll. Dabei kommt als Kontrollgegenstand in der Identitätsverwaltung der (elektronische) Agent in Betracht, der anschließend eingeführt wird (D.) und schließlich in die Grundannahmen für die Modellbildung über die kontrollierbaren Erkenntnisse zu personalen Identitäten überführt werden soll (E.).

A. Personale Identität in einfachrechtlichen Typologien

Die personale Identität in einfachrechtlichen Typologien lässt sich primär mit dem Namen einer Identität in Verbindung bringen, mit dem die Zuordnung der personalen Identität möglich wird. Dies gilt für den offline-Kontext und für den online-Kontext gleichermaßen, da etwa der elektronische Personalausweis als eine Anknüpfung für die „digitale Identität“[244] im online-Kontext gilt und der Name in einem Identitätsverwaltungsmodell als Anknüpfungspunkt heranzuziehen ist (I.). Weiter ist mit der kommunikativen Ausprägung der personalen Identität das Recht im elektronischen Rechtsverkehr einzubeziehen, welches in seinem statischen *Idem*-Anteil

244 *Hornung*, Die digitale Identität, 2005; ebenso auf die statische *Idem*-Dimension der Identität abstellend, *Warnecke*, Identitätsmanagement und Datenschutz, 2019, S. 14.

aus der elektronischen Signatur und in seinem dynamischen *Ipse*-Anteil aus der vertraulichen und sicheren Kommunikation besteht (II.). Diese einfachrechtlichen Regelungen über die elektronische Kommunikation sind Anknüpfungspunkte für das Identitätsverwaltungsmodell im online-Kontext, welches das kontextspezifische Vertrauens- und Sicherheitsniveau bei der Identifizierung der personalen Identität umfasst. Diese Ausprägungen der personalen Identität können primär der Identitifizierung und Authentifizierung mit einem *Identifizierer* und sekundär dem schutzwürdigen Vertrauen des Kommunikationspartners über die tatsächliche Identität in einem spezifischen Kontext dienen. Dabei würde der Schutzbereich der informationellen Selbstbestimmung zunächst unberührt bleiben, gleichzeitig werden aber die Schnittmengen zum Datenschutzrecht aufgezeigt (III.).

I. Personale Identität als Name

Der Name als *Idem*-Anteil der personalen Identität des Individuums bildet einen Anknüpfungspunkt für die kontextübergreifende Identitätsverwaltung. Damit ist der Name in seiner statischen *Idem*-Dimension der personalen Identität in die Modellbildung einzubeziehen und fungiert als zentraler Anker. Gleichwohl kann auch der Name Änderungen unterliegen und in direkter Verbindung zu den Ausprägungen der personalen Identität stehen, so dass die einfachrechtlichen Vorgaben aus dem Namensrecht für die einfachrechtliche Konkretisierung des Identitätsbegriffs und die Modellbildung heranzuziehen sind.

Zunächst dient der Name aus der öffentlich-rechtlichen und privatrechtlichen Perspektive der Identifizierung der natürlichen Person und wirkt sich auf die Selbstdarstellung ebenso aus wie auf das wahrnehmbare Bild der personalen Identität. Der Name gemäß § 12 BGB kann der bürgerliche Name kraft Gesetzes gemäß § 1757 BGB oder ein Wahlname etwa als Deckname oder auch ein Pseudonym sein.[245] Dabei dient der Name der Unterscheidung und der Identifizierung und gilt in diesen Funktionen als schutzwürdig.[246] Gleichzeitig gilt gemäß § 1616 BGB der Gleichlauf der Namensführung zur Gewährleistung der Kontinuität der Namensführung, worin eine staatliche Fürsorge über die Namensgebung erkennbar ist. Daher kann die Eintragung von Namen mit unzureichender Identifizierungs-

245 *Palandt*, Kommentar, BGB, 2020, § 12 BGB Rn. 4.
246 *Ders.*, Kommentar, BGB, 2020, § 12 BGB Rn. 1, 11.

und Unterscheidungsfunktion, die im Widerspruch zu einer mit dem Vornamen einhergehenden Identitätsfindung stehen, abgelehnt werden.[247]

Vom Namensrecht nicht erfasst sind akademische Grade, obgleich diese als Namenszusätze im Personalausweis stehen können, §§ 5 Abs. 2 Nr. 3, 9 Abs. 3, 18 Abs. 3 Nr. 3 PAuswG, § 4 Abs. 1 Nr. 3 PassG.[248] Ebenso wird über § 132a StGB der Missbrauch von Titeln, Berufsbezeichnungen und Abzeichen unter Strafe gestellt, denn der allgemeine Rechtsverkehr verlangt die Lauterkeit der Titelführung und das Vertrauen in die Echtheit der Titel von Berufsträgern auch für die Funktionsfähigkeit dieser Berufsgruppen.[249] Weiter kommen als Namenszusätze die Adelsprädikate als Teile des bürgerlichen Namens in Betracht, auch wenn sie nicht mehr verliehen werden dürfen.[250] Daraus wird erkennbar, dass der Name als Bestandteil der personalen Identität neben der Identifizierungsfunktion im Rechtsverkehr eine Beschreibungsfunktion der personalen Identität erfüllt. Gleichwohl bleibt festzuhalten, dass der Titel auf das Verhalten der natürlichen Person zurückzuführen ist, so dass sich im Namen und in den Titeln verhaltensunabhängige *Idem*-Anteile und verhaltensbezogene *Ipse*-Anteile widerspiegeln.

Als weiteres Identifikationsmittel kommen biometrische Daten gemäß § 18 PAuswG hinzu, womit der Schutzbereich des Rechts auf informationelle Selbstbestimmung eröffnet ist.[251] Gleichwohl wird bei der Verwendung biometrischer Daten zur alleinigen Authentifizierung kein Verstoß gegen die Menschenwürdegarantie und das Recht auf informationelle Selbstbestimmung gesehen, da Überschussinformationen etwa über gesundheitliche Merkmale technisch ausgeschlossen werden.[252] Insgesamt ist gerade im öffentlichen Recht, wie auch im Privatrecht, der zum Einsatz kommende elektronische Identitätsnachweis maßgeblich,[253] so dass für die Identifizierung eine Beschränkung der übermittelten Identifizierungsdaten

247 *Ders.*, Kommentar, BGB, 2020, Einf § 1616 BGB Rn. 10; so wurde „Waldmeister" als männlicher Vorname für unzulässig erklärt.
248 *Ders.*, Kommentar, BGB, 2020, § 12 BGB Rn. 7.
249 *Sternberg-Lieben*, in: Schönke/Schröder/Eser u.a. (Hrsg.), Strafgesetzbuch, 2019, § 132a StGB Rn. 3.
250 Art. 109 Abs. 3 S. 2 WRV i. V. m. Art. 123 GG; *Palandt*, Kommentar, BGB, 2020, § 12 BGB Rn. 6.
251 *Hornung/Möller*, Passgesetz, Personalausweisgesetz, 2011, Einf Rn. 31–33.
252 *Dies.*, Passgesetz, Personalausweisgesetz, 2011, Einf Rn. 34 f.; § 16a PassG Rn. 8 f.
253 *Dies.*, Passgesetz, Personalausweisgesetz, 2011, Einf Rn. 87.

erfolgt,[254] und damit dem Grundsatz der Datenminimierung Rechnung getragen wird. Folglich erkennt das Personalausweiswesen die personale Identität im offline- und im online-Kontext gleichermaßen an. Mit dem elektronischen Personalausweis wird die Identitätsverwaltung im online-Kontext ermöglicht, wobei sich diese auf den Namen und die zusätzlichen Informationen gemäß § 18 Abs. 3 PAuswG beschränkt, was überwiegend der personalen Identität in ihrem *Idem*-Anteil gleichkommt.

Insgesamt geht es bei den rechtlichen Schutzdimensionen um den Namen und Familiennamen selbst, seinen Zusätzen in Gestalt von akademischen Graden und Adelsprädikaten. So hat der Name in der Biographie der personalen Identität eine statische Dimension, es sei denn, er wird über das Namensänderungsrecht (NamÄndG) geändert. Weiter kann mit dem Eheschluss der Familienname eines Ehepartners geändert oder beibehalten werden, worin wieder eine dynamische Dimension im Namensrecht zum Ausdruck kommt, § 1355 Abs. 1 BGB.

Für den Begriff der personalen Identität lässt sich daraus ableiten, dass mit dem Namen und seiner Änderung sich eine Identität begründen lässt, mit der eine rechtssichere Zuordnung zu einer natürlichen Person ermöglicht wird. Schließlich kann damit für das Identitätsverwaltungsmodell der Name als maßgeblicher Anknüpfungspunkt der personalen Identität festgehalten werden, der mit Zusätzen in Gestalt von Titeln oder Adelsprädikaten versehen sein kann, die sich als dynamische Realisierungen im Rahmen der individuellen Biographie darstellen können. Gleichzeitig kann der Name im Rahmen des Identifizierungsprozesses hinter dem Authentifizierungsprozess stehen und als *Identifizierer* für einen weiteren kontextbezogenen Datensatz eingesetzt werden.

II. Personale Identität im elektronischen Rechtsverkehr

Ein Identitätsverwaltungsmodell, basierend auf den grundrechtlichen Ausprägungen der personalen Identität, verlangt einerseits den statischen *Idem*-Anteil und andererseits den dynamischen *Ipse*-Anteil auch im online-Kontext. Diese Ausprägungen sollen aus dem einfachen Recht des elektronischen Rechtsverkehrs hergeleitet werden, um daraus weitere Grundlagen für die Modellbildung ableiten zu können. Dazu werden die statische *Idem*-Dimension der personalen Identität im Recht der elektronischen Si-

254 BT-Drucks. 16/10489, S. 40: In der Gesetzesbegründung wurde ausdrücklich auf die Möglichkeit des „persönlichen Identitätsmanagements“ hingewiesen.

gnatur (1.) und bei der gestuften sicheren Identifizierung (2.) dargestellt. Beide lassen sich auf den Namen zurückführen, der für die Erteilung einer elektronischen Signatur und der Identifizierung im elektronischen Rechtsverkehr erforderlich ist, so dass sie für die Modellbildung eine direkte rechtliche Grundlage bilden. Demgegenüber ist der *Ipse*-Anteil der personalen Identität in ihrer Dynamik im Recht zum Schutz der vertraulichen Email-Kommunikation nach dem De-Mail-G abbildbar und stellt eine weitere einfachrechtliche Grundlage für die Modellbildung dar (3.).

1. Qualifizierte elektronische Signatur, §§ 11, 12 VDG

Die personale Identität in Gestalt des Namens tritt im Recht der Vertrauensdienste in verschiedenen Phasen auf. Dazu gehören die Identitätsprüfung bei dem Vertrauensdienstanbieter, die Identifizierung und die Gewährleistung der rechtssicheren Durchführung des Vertrauensdienstes, damit der Kommunikationspartner mit einer hohen Sicherheit auf die Richtigkeit der Identität vertrauen kann. Die Identitätsprüfung wird gemäß § 11 VDG als Nachfolgegesetz des SigG über die „Personenidentifizierungsdaten" gemäß Art. 3 Nr. 3 eIDAS-VO durchgeführt. Dabei können weitere Attribute, wie etwa Angaben über die Vertretungsmacht, im qualifizierten Zertifikat gemäß § 12 VDG aufgenommen werden. Mit der Identitätsprüfung erfolgt die Ausstellung eines qualifizierten Zertifikates, welches beim Inhaber gespeichert wird und mit einem Passwort zugänglich ist. Dieses ausgestellte Zertifikat stellt einen *Idem*-Anteil der personalen Identität dar, da mit ihm der Kommunikationspartner auf die statische Dimension der Identität vertrauen kann. Denn mit dem Zertifikat kann die Schriftform als Identitätsnachweis mit der Unterschrift durch die elektronische Signatur ersetzt werden, §§ 126, 126a BGB, Art. 25 Abs. 2 eIDAS-VO. Darin kommen gerade die Funktionen der Formregeln in der Abschluss-, Kontroll- und Beweisfunktion zum Ausdruck. Zwar richten sich diese an den Rechtsverkehr, jedoch kommen darin die rechtlichen Wertungen über die Gewährleistung eines hohen Sicherheits- und Vertrauensniveaus über die Identität zum Vorschein, was gleichermaßen für personale Identitäten in der Identitätsverwaltung erforderlich ist. Denn mit der qualifizierten elektronischen Signatur lässt sich für einen spezifischen Kontext ein hohes Vertrauens- und Sicherheitsniveau herstellen.

In technischer Hinsicht wird die Signatur mit dem Verfahren der asymmetrischen Kryptographie erstellt, wonach Verschlüsselung und Entschlüsselung jeweils mit zwei Schlüsseln erfolgen, einem öffentlichen und einem

privaten Schlüssel, sog. „*Public-Key-Infrastructure*“ (PKI). Dem Signieren jedes Dokuments geht ein technisches Verfahren voraus, mit dem ein Hashwert als Element für das spezifische Dokument erzeugt wird, welches mit dem privaten Schlüssel generiert wird.[255] Der Empfänger des Dokuments nutzt wiederum seinen privaten Schlüssel und anschließend erfolgt die Prüfung der Schlüssel mit dem Abgleich zu den öffentlichen Schlüsseln. Erst mit dem Zertifikat werden der private und öffentliche Schlüssel miteinander in Verbindung gebracht.[256] Damit ist in technischer Hinsicht die reale Kontrolle durch den Zertifikatinhaber mit einem hohen Sicherheits- und Vertrauensniveau gegeben. Gleichwohl können Angriffe und damit ein Identitätsmissbrauch oder Identitätsdiebstahl[257] nicht ausgeschlossen werden, jedoch besteht ein gesteigertes Sicherheitsniveau.

Insgesamt lässt sich das Kontrollkonzept über die personale Identität aus der qualifizierten elektronischen Signatur ableiten, EWG 51, 52, 53 eIDAS-VO. Denn es wird in Art. 26 c) eIDAS-VO geregelt, dass die Umgebungen zur Verwendung der elektronischen Signaturen der alleinigen Kontrolle des Unterzeichners unterliegen. Gleichzeitig kann der Einsatz eines spezifischen Zertifikates zeitlich begrenzt werden und ein neues Zertifikat als *Idem*-Anteil der personalen Identität ausgestellt werden, was einer „Beendigung von Identitäten“[258] und einer Neubegründung dieser gleichkommt.

2. Gestufte sichere Identifizierung, Art. 8 eIDAS-VO

Das Vertrauens- und Sicherheitsniveau von elektronischen Identifizierungssystemen unterliegt Abstufungen, die sich in der Regelung des Art. 8 Abs. 2 eIDAS-VO widerspiegeln. Danach sind *drei Sicherheitsstufen* in niedrig, substantiell und hoch für die Identifizierung vorgesehen, worin bereits ein eigenes Identitätsverwaltungsmodell erblickt werden kann. Bei der Identifizierung mit einem niedrigen Sicherheitsniveau genügt zur Authen-

255 *Bergfelder*, Der Beweis im elektronischen Rechtsverkehr, 2006, S. 97.

256 *Ders.*, Der Beweis im elektronischen Rechtsverkehr, 2006, S. 98 f.

257 Es kommen Angriffe auf das Trägermedium etwa den Laptop, auf das zu signierende Dokument oder eine Manipulation bei Erstellung des Hashwertes in Betracht. Ebenso kann das Verhalten der Passworteingabe über „*social engineering*“ oder Schwachstellen im Betriebssystem der Gegenstand von Angriffen werden, so dass die Unmöglichkeit einer absoluten Sicherheit und damit Kontrolle über die Signatur ausgeschlossen ist, *ders.*, Der Beweis im elektronischen Rechtsverkehr, 2006, S. 95 f., 199 f.

258 *Hornung*, in: Roßnagel (Hrsg.), Wolken über dem Rechtsstaat?, 2015, 189 (198).

tifizierung der Einsatz von Passwörtern, auf der zweiten Stufe sind für das substantielle Sicherheits- und Vertrauensniveau etwa Zertifikate vorgesehen und auf der dritten Stufe mit einem hohen Sicherheitsniveau wird der Schutz vor Duplizierungen gewährleistet, indem die Identifizierung ausschließlich von einer Person etwa über den elektronischen Personalausweis vorgenommen werden kann. Danach verlangt die Identifizierung des Bürgers gegenüber einer staatlichen Institution ein hohes Sicherheits- und Vertrauensmaß, Art. 8 Abs. 2 c) eIDAS-VO, wohingegen gegenüber einem notifizierten Dienstanbieter für die Rechtsbeziehung unter Privaten[259] die Authentifizierung über ein Passwort ausreichend sein kann, Art. 8 Abs. 2 a) eIDAS-VO. Aus diesen drei verschiedenen Sicherheitsniveaus geht der Grad der Vertrauenswürdigkeit des elektronischen Identifizierungsmittels hervor, mit dem das Vertrauensmaß zwischen festgelegter Identität und der damit zugewiesenen Identität beschrieben wird, EWG 16 S. 1. Die Anknüpfung dieses Vertrauensmaßes richtet sich nach dem Registrierungsumfang für die Ausstellung des Passwortes, Zertifikates oder etwa des elektronischen Personalausweises. Denn von der Identifizierung durch persönliches Erscheinen bei einer „*Trusted Third Party*" als notifizierten Vertrauensdienstanbieter mit den „Personenidentifizierungsdaten" gemäß Art. 3 Nr. 3 eIDAS-VO, geht eine hohe Beweiswirkung aus, die einer Identifizierung mit der bloßen Email-Adresse gegenübersteht.

Aus den gestuften Sicherheits- und Vertrauensniveaus lässt sich innerhalb des jeweiligen Niveaus eine kontextübergreifende Identifizierung abbilden, wie sie ein differenziertes Identitätsverwaltungsmodell voraussetzen würde. Erweiternd ist für ein Identitätsverwaltungsmodell die Anforderung maßgeblich, eine grenzüberschreitende Interoperabilität gemäß Art. 12 eIDAS-VO zu gewährleisten, die innerhalb eines Sicherheits- und Vertrauensniveaus gelten würde. Darin kommt die Beseitigung der Hindernisse zur grenzüberschreitenden Verwendung des gleichen elektronischen Identifizierungsmittels zur Authentifizierung bei öffentlichen Diensten zum Ausdruck, EWG 12 S. 1. Der technische Interoperabilitätsrahmen ist gemäß Art. 12 Abs. 3 a) eIDAS-VO technologieneutral und kann durch Kommunikationsschnittstellen realisiert werden. Dabei besteht der zu regelnde Interoperabilitätsrahmen aus Bezugnahmen auf die Sicherheitsniveaus nach Art. 8 eIDAS-VO, technischen Mindestanforderungen, Verfahrensregelungen und Regelun-

259 Die eIDAS-VO ist grundsätzlich für die Identifizierung und Authentifizierung gegenüber öffentlichen Diensten vorgesehen, jedoch soll gemäß EWG 57, 2 und Art. 3 Nr. 7, 30 eIDAS-VO auch der Rechtsverkehr unter Privaten einbezogen werden.

gen zur Streitbeilegung, Art. 12 Abs. 4 a, c–f) eIDAS-VO. Mit dem Interoperabilitätsrahmen für eine grenzüberschreitende Identifizierung in dem jeweiligen Sicherheitsniveau gemäß Art. 8 Abs. 2 eIDAS-VO kann jedoch einhergehen, dass das Risiko einer kontextübergreifenden Identifizierbarkeit steigt und die Trennung der Sicherheitsstufen faktisch aufgehoben wird.

Damit lässt sich die rechtliche Überschneidung zwischen dem Vertrauensdiensterecht und den datenschutzrechtlichen Vorgaben gerade an der Datenminimierung aufzeigen. Denn das Vertrauensdiensterecht soll die sichere Identifizierung ermöglichen und zugleich gemäß Art. 5 Abs. 1 eIDAS-VO datenschutzrechtliche Maßgaben einhalten. Im Rahmen des Selbstdatenschutzes können dabei Zielkonflikte mit der Sicherstellung der kontextbezogenen Identifizierung auf der einen Seite und der faktischen kontextübergreifenden Re-Identifizierbarkeit als Ausprägung des *Big Data*-Phänomens auf der anderen Seite entstehen. Insoweit erscheint die konsequente Einhaltung des kontextspezifischen Sicherheitsniveaus aus datenschutzrechtlicher Hinsicht fraglich, wenn die Identifizierung auf einem niedrigen Sicherheitsniveau gemäß Art. 8 Abs. 2 a) eIDAS-VO erfolgt und die damit verbundenen Erkenntnisse kontextübergreifend herangezogen werden können, wobei damit das höhere „substantielle" Schutzniveau gemäß Art. 8 Abs. 2 b) eIDAS-VO herangezogen werden müsste. Um gegen dieses Risiko vorgehen zu können, wäre der zeitlich beschränkte Einsatz der Identifizierungsmittel denkbar, indem etwa die Wirksamkeit einer Signatur an den Erstellungszeitpunkt anknüpft, zeitlich begrenzt ist und nach Zeitablauf automatisch gelöscht wird.

3. Vertrauliche sichere Kommunikation, § 1 De-Mail-G

Das Konzept der Kontrolle als Beherrschbarkeit kann ebenso die Kommunikation umfassen, da der Kommunikationsvorgang durch eine der Kontrolle unterliegenen Handlung ausgelöst wird. Indem die personale Identität neben dem statischen *Idem*-Anteil über einen kommunikativen und damit dynamischen *Ipse*-Anteil verfügt, kann in den einfachrechtlichen Regelungen zur vertraulichen und sicheren Kommunikation ein wesentlicher Anknüpfungspunkt für das Identitätsverwaltungsmodell liegen.

Mit dem De-Mail-G wird gerade die sichere, vertrauliche und nachweisbare Kommunikation geregelt und dabei die Vertraulichkeit der Kommunikation als Kernelement des De-Mail-G begründet, § 1 Abs. 1 De-Mail-G. Darin sollte eine Antwort auf die bislang unausgeprägten elektronischen Kommunikationsmöglichkeiten zwischen dem Bürger und staatlichen Institutionen

etwa für Bürgerdienste oder die elektronische Post liegen. Die Voraussetzung ist wiederum, parallel zum Erhalt einer qualifizierten elektronischen Signatur, die Registrierung bei einem akkreditierten Dienstanbieter unter Vorlage eines Personalausweises, wodurch wiederum ein hohes Sicherheits- und Vertrauensniveau gewährleistet wird. Dies wird im besonderen Maße sichergestellt, indem die Identitätsdaten in angemessenen zeitlichen Abständen auf ihre Richtigkeit geprüft werden, §§ 1 Abs. 2, 3 Abs. 3 Nr. 1 a), 3 Abs. 5 S. 2 De-Mail-G. Maßgeblich sind nach dem De-Mail-G der Schutz vor Manipulation der Identität des Kommunikationspartners und auch die rechtssichere inhaltliche Zustellung elektronischer Dokumente gegen unkooperative Kommunikationspartner.[260] Damit werden über die Identitäten des Senders und Empfängers hinaus die Inhalte der Kommunikation durch die verschlüsselte Kommunikation geschützt, §§ 4 Abs. 3, 5 Abs. 3 De-Mail-G, und über die inhaltliche Zustellung eine Beweiserleichterung begründet, die als Anscheinsbeweis über die Richtigkeit des Absenders und den Inhalt der Nachricht fungiert, § 371a Abs. 2 ZPO.[261]

In dieser Erweiterung der Beweisvermutung, die sich auf den Inhalt der Nachricht erstreckt, liegt ein wesentlicher Erkenntniswert für die Identitätsverwaltung. Denn nach der Wertung des Gesetzgebers kommt es im online-Kontext nicht allein auf die rechtssichere elektronische Identifizierung in Gestalt einer Signatur an, sondern auf den Schutz der rechtssicheren inhaltlichen Kommunikation gegenüber staatlichen Institutionen und zwischen Privaten. Mit dem Schutz der Identität des Kommunikationspartners auf der einen Seite und dem Schutz des Inhaltes der Kommunikation auf der anderen Seite ist für den online-Kontext aus dem De-Mail-G ein aufschlussreiches Regelungsregime für die Identitätsverwaltung ableitbar. Denn es wird neben der statischen Dimension der personalen Identität über eine Signatur die dynamische Dimension der schützenswerten Kommunikation in die gesetzgeberische Wertung einbezogen. Zwar kann die Kommunikation einem eigenständigen grundrechtlichen Schutz aus dem Fernmeldegeheimnis, Art. 10 Abs. 1 GG, und der allgemeinen Meinungsfreiheit, Art. 5 Abs. 1 GG, unterliegen, jedoch bezieht sich die vorliegende Betrachtung auf die enge Verbindung zur Identität des Kommunikationspartners. Diese strahlt unmittelbar auf das Schutzniveau der inhaltlich vertraulichen Kommunikation aus. Die personale Identität in ihrer verhaltensbezogenen Dimension findet damit im online-Kontext eine unmittelbare einfachrechtliche Abbildung, welches für ein Identitätsverwaltungsmodell zu einer Aner-

260 *Roßnagel*, CR 2011, 23 (29).
261 *Ders.*, CR 2011, 23 (29).

kennung der personalen Identität im Rahmen der Identifizierung und der damit verbundenen inhaltlichen Kommunikation führt. Damit sind die Grundlagen für ein Identitätsverwaltungsmodell im online-Kontext gelegt, weil ein einfachrechtliches Schutzkonzept für die personale Identität und ihre inhaltliche kommunikative Ausprägung besteht.

4. Bewertung

Das Recht der Vertrauensdienste und das Recht über die sichere, vertrauliche elektronische Kommunikation knüpfen an die Identifizierung der personalen Identität an, was über das Registrierungsverfahren und anschließend die Anwendung einer Signatur oder des De-Mail-Kontos erfolgt. Darin kommt die statische Dimension der personalen Identität in ihrem *Idem*-Anteil über den Namen zum Ausdruck, erfährt aber durch die Kommunikation mit diesem eine dynamische Erweiterung in ihrem *Ipse*-Anteil. Denn über die Gewährleistung des Schutzes der Identität und der inhaltlichen Kommunikation kommt im online-Kontext ein dynamisches Schutz- und Ausgleichskonzept in direkter Verbindung zur personalen Identität zum Ausdruck.

Gleichzeitig stellt sich bei der IT-sicherheitsrechtlichen Prägung die Frage nach der Gewährleistung datenschutzrechtlicher Vorgaben, um eine umfassende Überführung der Maßgaben in ein rechtlich gestütztes Identitätsverwaltungsmodell vornehmen zu können. Gemäß Art. 5 Abs. 1 eIDAS-VO wird auf die Datenschutzrichtlinie verwiesen, was nunmehr einem Verweis auf die DSGVO gleichkommt. Eine konkretisierte Regelung erfolgt in Art. 5 Abs. 2 eIDAS-VO und § 5 Abs. 2 De-Mail-G, wonach die Benutzung von Pseudonymen nicht untersagt werden darf. Darin und in § 15 De-Mail-G liegt eine Konkretisierung der Datenminimierung nach Art. 5 Abs. 1 c) DSGVO, wonach zum Schutz der personenbezogenen Daten eine Beschränkung der Datenverarbeitung auf das notwendige Maß geregelt wird. In den nur punktuellen Bezugnahmen[262] auf datenschutzrechtliche Vorgaben wie etwa „*privacy by design*“, Art. 12 Abs. 3 c) eIDAS-VO, ohne jedoch die differenzierten Interdependenzen zwischen Datenschutz und IT-Sicherheit aufzugreifen, wird ein Regelungsgefüge gesehen, welches „unterkomplex“ sei.[263] So sieht etwa Art. 8 Abs. 2 c) eIDAS-VO für die Identifizierung mit dem elektronischen Personalausweis ein hohes Schutzniveau vor, ohne jedoch in

262 Art. 12 Abs. 3 c), d), Art. 19 Abs. 2, Art. 20 Abs. 2, Art. 24 Abs. 2 b) und j) eIDAS-VO.

263 *Roßnagel*, NJW 2014, 3686 (3687).

der eIDAS-VO ein Regelungsgefüge für die Verarbeitung besonderer Kategorien personenbezoger Daten nach Art. 9 DSGVO zu enthalten. Darin kommen die noch unzureichende Verknüpfung zwischen dem Vertrauensdienste- und Datenschutzrecht und das Fehlen eines ausdifferenzierten Schutzgefüges für die informationelle Selbstbestimmung zum Ausdruck. Folglich wäre eine differenzierte Einbeziehung der Datenverarbeitungsgrundsätze gemäß Art. 5 Abs. 1 DSGVO wünschenswert und könnte einen gesteigerten Schutz für die informationelle Selbstbestimmung bedeuten.

Insgesamt lässt sich aus den bestehenden Regelungen dennoch ein Schutzgefüge zur Gewährleistung der Datenminimierung nachweisen, welches bei der Modellierung heranzuziehen ist. Dieses könnte mit einem zeitlich beschränkten Identifizierungsvorgang umgesetzt werden, damit das Risiko von Erkenntnissen zu einer personalen Identität über die jeweiligen Stufen des Sicherheits- und Vertrauensniveaus hinweg gemindert wird.

Mit der Verbindung der IT-sicherheitsrechtlichen und der datenschutzrechtlichen Regelungen würde einem Identitätsverwaltungsmodell mit statischen und dynamischen Ausprägungen entsprochen werden können. Dabei sind die Zielkonflikte, einerseits eine rechtssichere Identifikation des *Idem*-Anteils einer personalen Identität zu ermöglichen und andererseits das Risiko der Re-Identifizierbarkeit in einem anderen Kontext mit einem höheren Sicherheitsniveau zu mindern, miteinander in Einklang zu bringen. Insofern verlangt das Identitätsverwaltungsmodell eine Differenzierung des Sicherheitsniveaus bei der rechtssicheren Identifizierung und einen Schutzmechanismus für die rechtssichere Gewährleistung der Interoperabilität innerhalb des Schutzniveaus.

III. Zusammenfassung

Aus dem einfachen Recht wurden die Konkretisierungen der verfassungsrechtlichen Vorgaben zur personalen Identität für das Identitätsverwaltungsmodell abgeleitet. Dazu gehört, dass der Name als übergreifender Bezugspunkt im einfachen Recht fungiert und kontextspezifisch das Vertrauens- und Sicherheitsmaß der personalen Identität und Kommunikation variiert. Dies kommt in der zivilrechtlichen Regelung des Namensrechts in § 12 BGB zum Ausdruck und dem damit einhergehenden Schutz im Rechtsverkehr hinsichtlich der Unterscheidbarkeit und Identifizierbarkeit der natürlichen Person. Gleichzeitig erlangt der Name in der Rechtsbeziehung zwischen Bürger und Staat besonders durch das PAuswG ein hohes Vertrauens- und Sicherheitsmaß hinsichtlich der Identifizierbarkeit. Dieses wird für

den elektronischen Rechtsverkehr über die eIDAS-VO für den öffentlich-rechtlichen und privatrechtlichen Kontext gleichermaßen geregelt. Danach erfolt die Registrierung zum Erhalt eines Zertifikates für die elektronische Signatur mit den Personenidentifizierungsdaten und für den Erhalt eines De-Mail-Kontos muss der Personalausweis vorgelegt werden, §§ 3 Abs. 3 a), c), 4 Abs. 2 De-Mail-G.

Gleichzeitig wird ein gestuftes System zur Identifizierung nach Art. 8 Abs. 2 eIDAS-VO anerkannt, woraus die Grundstruktur eines Identitätsverwaltungsmodells dahingehend abzuleiten ist, dass dieses abhängig von dem jeweiligen Kontext ein niedriges, substantielles oder hohes Vertrauens- und Sicherheitsniveau enthält. Dieses richtet sich auf die statische Identifizierung und den über das De-Mail-Konto gewährleisteten Schutz der Identität und der Kommunikation gleichermaßen. Daraus ergibt sich für die personale Identität und das Identitätsverwaltungsmodell das Erfordernis von kontextbedingten Vertrauens- und Sicherheitsabstufungen. Damit werden die Identifizierung und die inhaltliche Kommunikation geschützt. Aus diesen rechtlichen Phänomenen lässt sich ein einfach- und sekundärrechtliches Grundmodell ableiten. Dabei würde sich die digitale Identität über den elektronischen Personalausweis als ein Bestandteil in dem Gesamtgefüge der personalen Identität im online-Kontext erweisen.

B. Erkenntnismodell

Die *Modellbildung der Identitätsverwaltung* verlangt darüber hinaus die Bestimmung des Gegenstands der personalen Identitäten, der sich aus dem Erkenntnismodell ableiten lässt. Danach können die Anknüpfungspunkte für die personale Identität die Daten, die Informationen und das Wissen über die Identität sein (I.). Dabei sind die vielfältigen Erkenntnismöglichkeiten über personale Identitäten kontextbezogen und flexibel, was in die Modellbildung einzubeziehen ist, um einen wirksamen Schutz- und Ausgleichsmechanismus begründen zu können. Daneben kommt der dynamische *Ipse*-Anteil einer personalen Identität über die Kommunikation im Rahmen der Datenverarbeitung und dem damit verbundenen Datenzyklus einer personalen Identität als Schutzgegenstand zum Ausdruck. Dieser kann mit einer übergeordneten Metakommunikation durch *Instruktionen* in einem Verfahren über das Wissen zu einer personalen Identität maßgeblich sein (II.). Schließlich geht es um die Konkretisierung der Gegenstände für das Identitätsverwaltungsmodell, die an die Informationen und das verfahrensbedingte Wissen über personale Identitäten anknüpfen und einen Schutz- und

Ausgleichsmechanismus über die entstandenen Bilder personaler Identitäten bilden können (III.).

I. Daten-Informationen-Wissen

Im Verfassungsrecht und im einfachen Recht sind als Schutzgegenstände zur personalen Identität die Daten und die semantischen Bedeutungsgehalte über die personale Identität erfasst. Bei einem Identitätsverwaltungsmodell stellt sich die Frage, welche dieser Erkenntnisgehalte zur personalen Identität zum Gegenstand der Kontrolle werden können. Denn es kommt nicht nur der Schutz der Signale als Daten über eine personale Identität in Betracht, sondern auch die damit verbundenen Interpretations- und Erkenntnismöglichkeiten. Daraus ergibt sich der Bedarf, den Gegenstand des Schutzes einer näheren Differenzierung zu unterziehen, damit sich der Kontrollgegenstand spezifizieren lässt.

Nach dem Erkenntnismodell wird eine Untergliederung in Daten, Informationen, Wissen und dem Vorgang der Entscheidung vorgenommen, die in einem Identitätsverwaltungsmodell jeweils zum Gegenstand der Kontrolle werden können. Diese aus Daten bestehenden Zeichenfolgen erlangen einen Bedeutungsgehalt erst durch den Vorgang der Interpretation, woraus sich aus den Daten die semantischen Informationen über die personale Identität ergeben. Mit der Interpretation werden die Daten aus der „Schattenwelt der Informationstechnik" in ein sozialwirksames Folgensystem überführt.[264] Der Interpretationsvorgang unterliegt einem bestimmten Zweck und ist damit perspektivisch, so dass es sich nicht um wertfreie, objektive Informationen handeln könne.[265] Dabei beschreibt *Steinmüller* diesen Vorgang eigens als Übermittlungsvorgang, bei dem es auch zu einem Übermittlungsirrtum kommen könne und die Informationen – vergleichbar mit einer Amöbe – dem räumlichen und zeitlichen Wandel unterliegen.[266] Wiederum können aus den Informationen und ihrer Bündelung weitere Erkenntnisebenen wirken und einen eigenständigen kontextspezifischen Bedeutungsgehalt als „konsolidiertes Wissen"[267] entfalten, wobei das kon-

264 *Steinmüller*, Information, Modell, Informationssystem, S. 48.
265 *Ders.*, Information, Modell, Informationssystem, S. 37 f.; *Albers*, Informationelle Selbstbestimmung, 2005, S. 92–94.
266 *Ders.*, Information, Modell, Informationssystem, S. 5, 32–35.
267 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (23); ebenso *Gasser*, Kausalität und Zurechnung von Information als Rechtsproblem, 2002, S. 74.

krete Wissen von der Wandlungsfähigkeit der Informationen abhänge (Abbildung 2).[268] Somit ist Wissen in einem System flexibel und könne nicht objektiv sein, aber einem kontextbedingten Wahrheitssystem entsprechen.[269] Sobald das Wissen aber als ableitbare Schlussfolgerung festgestellt wurde, kann dem erlangten Wissen die Eigenschaft eines Agenten zukommen,[270] so dass dem Wissen über eine personale Identität in einem spezifischen Kontext die Agenteneigenschaft zugeschrieben werden kann. Damit wird das Bild der personalen Identität in Gestalt eines Agenten zum Gegenstand der Kommunikation.

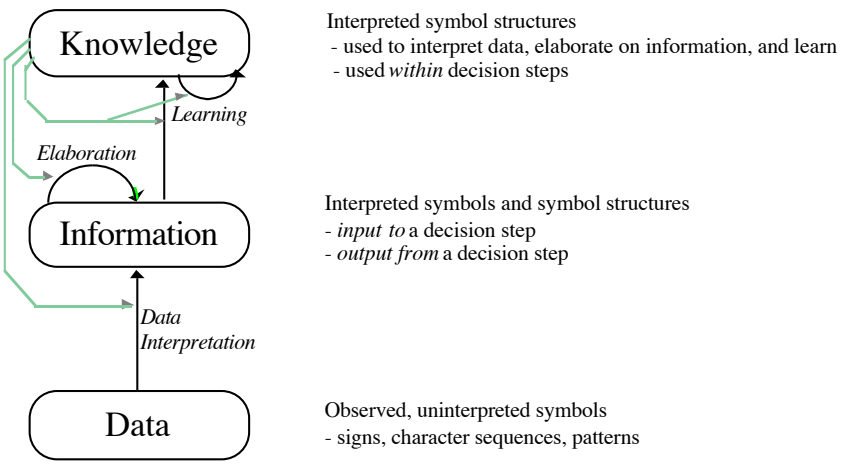

Abbildung 2: Aamodt/Nygård[271]

Dies setzt den Vorgang des Entscheidens voraus, der von *Steinmüller* als Aggregatzustand über die Informationen beschrieben wird, denn Informationen verlangen einen dynamischen Informationserzeugungsvorgang, der eines *strukturierten Entscheidungsverfahrens* etwa als „iteratives Entschei-

268 *Aamodt/Nygård*, Data & Knowledge Engineering 16 (1995), 191 (199); *Reisinger*, Rechtsinformatik, 2016, S. 75.
269 *Dies.*, Data & Knowledge Engineering 16 (1995), 191 (200); *Steinmüller*, Information, Modell, Informationssystem, S. 67; zudem hänge das Wissen von möglichem *Vorwissen* ab, *Gasser*, Kausalität und Zurechnung von Information als Rechtsproblem, 2002, S. 77.
270 *Dies.*, Data & Knowledge Engineering 16 (1995), 191 (204).
271 *Dies.*, Data & Knowledge Engineering 16 (1995), 191 (198).

dungsmodell“ bedarf.[272] Darin könnte eine Begegnung von missverständlichen, falschen oder manipulierten Informations- und Wissensergebnissen über die Bilder personaler Identitäten liegen, die gerade bei der Profilerstellung oder in Scoringverfahren in Erscheinung treten können. Demnach geht es bei dem Wissen in *Big Data*-Zeiten nicht allein um das Erlernen aus Informationen an sich, sondern um die Validierung der Informationen nach bestimmten Regeln, damit sinnlose, überholte oder widerlegte Informationen für eine wirksame Beschränkung des Wissens ausgeschlossen werden.[273] Dies setzt ein strukturiertes Entscheidungsverfahren voraus, das aus *Instruktionen* für die Entscheidungsfindung besteht und ein wesentlicher Anknüpfungspunkt für die Identitätsverwaltung sein kann, um die aus Wissen erstellten Bilder personaler Identitäten tatsächlich kontrollieren zu können.

II. Datenzyklus

Der Datenzyklus im Zusammenhang mit der personalen Identität umfasst die Datenverarbeitung der personenbezogenen Daten in ihren Ausprägungen der Erfassung, der Organisation, der Speicherung oder Veränderung, der Einschränkung, des Löschens oder der Vernichtung der personenbezogenen Daten, Art. 4 Nr. 2 DSGVO, EWG 39 S. 2. Demnach wirkt sich das Recht auf Vergessenwerden im Datenzyklus als ein entscheidendes Schutzrecht im Hinblick auf das verfassungsrechtliche Recht auf Neubeginn für die personale Identität aus. Mit einem Identitätsverwaltungsmodell sind auf der Ebene der Realphänomene die biographischen Kontexte maßgeblich, denn das Individuum steht in einer kontinuierlichen kommunikativen Beziehung zu der sozialen Umgebung.

Für den Schutz der personalen Identität innerhalb des Datenzyklus kann die Einteilung in die Phasen vor der Datenverarbeitung, der Begründung der Rechtmäßigkeit und der Phase nach der Rechtfertigung der Datenverarbeitung vorgenommen werden. An dieser Stelle sollen jedoch im Rahmen des dargestellten Erkenntnismodells die Relevanz des Datenzyklus für die personale Identität und der Identitätsverwaltung analysiert

272 *Steinmüller*, Information, Modell, Informationssystem, S. 76; ebenso zur Information als Zustand, vgl. *Gasser*, Kausalität und Zurechnung von Information als Rechtsproblem, 2002, S. 26.

273 *Weyh*, Philosophie in der digitalen Welt - DigiKant oder: Vier Fragen, frisch gestellt.

werden. Unter der Maßgabe, dass ein Identitätsverwaltungsmodell über die Verwaltung von Teilidentitäten hinaus einem Kommunikationsgefüge unterliegt und der Bedarf einer übergeordneten Kommunikationsstruktur bestehen kann, soll im Folgenden der Datenzyklus als Kommunikation (1.) und als Metakommunikation (2.) dargestellt werden.

1. Datenzyklus als Kommunikation

Der Datenzyklus unterliegt einem Kommunikationsprozess, der aus einer Vielzahl von Interpunktionen besteht. Dabei wird angenommen, dass sich die aus der Kommunikationspsychologie stammenden Erkenntnisse fragmentarisch auf die digitale Kommunikation in einem Datenzyklus übertragen lassen.[274] Denn es handelt sich um einen Datenzyklus, der personenbezogene Daten zum Gegenstand hat und bei dem in der Kommunikation neben der Informationstechnik der Mensch beteiligt ist, was sich auf die Bilder personaler Identität auswirkt. Demnach ist zwischen Sender, Empfänger, Nachricht und Vermittler als technische Umsetzer in einem Kommunikationsverhältnis zu differenzieren.[275] Ein Identitätsverwaltungsmodell verlangt diese Bestandteile eines technischen Systems, wonach es über die identitätsrelevanten Daten, Informationen und das Wissen[276] hinaus eines Senders, Empfängers und Vermittlers zum Schutz der personalen Identität bedarf. Damit sind die wesentlichen Bestandteile eines Identitätsverwaltungsmodells beschrieben, mit dem die Bilder personaler Identität als Erkenntnisse aus Daten entstehen und im räumlichen und zeitlichen Zusammenhang kontrolliert werden können.

Dahingehend wird von einer „Lebenszyklusverwaltung" über produktive, archivierte, gesperrte oder gelöschte Daten als Ausprägung des „*Infor-*

274 *Steinmüller* hat in der Begründung des Grundbegriffs der Kommunikation in der Informatik die Annahmen von *Watzlawick* einbezogen und festgestellt, dass die psychologische Facette der Kommunikation in der Begriffsfindung der informationstechnischen Kommunikation als Erkenntnisquelle für die Informatik unzureichend diskutiert werde, *Steinmüller*, Information, Modell, Informationssystem, S. 2 Fn. 6, S. 4 Fn. 32.

275 *Ders.*, Information, Modell, Informationssystem, S. 2 f.

276 Nach *Watzlawick* wird das Konzept des Wissens über die andere Partei in der menschlichen Kommunikation sogar in Frage gestellt und er geht vielmehr davon aus, dass sich Parteien vertrauen oder misstrauen können, jedoch nicht „Wissen" können; *Watzlawick/Beavin/Jackson*, Menschliche Kommunikation, 2016, S. 249 f.

mation lifecycle Management" ausgegangen, welches dem Regelungsregime der DSGVO unterliegt.[277] Daraus lässt sich für die Bilder personaler Identitäten die Annahme eines Datenzyklus über das kontextspezifisch generierte Wissen ableiten, welches dem Wandel der Zeit unterliegt. Demnach erscheint die Forderung nach regulatorischen und technischen Maßnahmen für ein Identitätsverwaltungsmodell von *Froomkin* folgerichtig, mit dem eine Kombination aus dem Verwalten, Synchronisieren, Sammeln und Verwenden von personenbezogenen Daten zur Kontrolle kontextspezifischer personaler Identitäten erfolgen würde.[278]

2. Datenzyklus als Metakommunikation

Ein Identitätsverwaltungsmodell könnte eine übergeordnete Kommunikationsebene als Metakommunikation darstellen. Dem liegt die Annahme zugrunde, dass nach dem Erkenntnismodell das Wissen nicht absolut und objektiv ist, sondern mehrere Versionen von Wissen zur Verfügung stehen können und eine Differenzierung des Wissens notwendig ist, was den rationalen Umgang mit personenbezogenen Daten voraussetze.[279] Folglich geht es um das *Wissen über das Wissen* und die damit verbundene Wissensverwaltung,[280] wie es mit den *Instruktionen* zur Generierung von Wissen über das Bild der personalen Identität erforderlich ist. Entsprechend kann das Verfahren das Wissen konsolidieren, wie es mit dem Verwaltungsverfahren, den Regeln der Beweislastverteilung und der Durchsetzung von Entscheidungen geregelt wird.[281]

In einem Datenzyklus geht es demnach um ein Verfahren, mit dem die Identitätsverwaltung erfolgen kann, welches eine weitere Ordnung über die Daten, Informationen und das Wissen zur personalen Identität begründet. Dabei geht es weniger um die Kontrolle über die Daten-, Informations- und Wissensströme, als um die Einbeziehung einer Metaebene der Kommunikation in Gestalt von *Instruktionen*. Auf dieser Metaebene kann ein Verfahren die *Instruktion* zur Steuerung über die Regeln der Informations- und Wissenserlangung von Bildern personaler Identitäten umfassen.

277 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 142; *Veil*, ZD 2015, 347 (350).
278 *Froomkin*, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, S. 8.
279 *Cohen*, JTHTL 2012, 242 (242 f.).
280 *Steinmüller*, Information, Modell, Informationssystem, S. 69.
281 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (24 f.).

III. Übertragung auf das Identitätsverwaltungsmodell

Das Erkenntnismodell ermöglicht die Differenzierung der Identitätsverwaltung hinsichtlich der Daten, Informationen und des Wissens über eine personale Identität. Diese Erkenntnisebenen variieren in einem Datenzyklus und hängen von dem jeweiligen Betrachtungswinkel ab. Darin kommt zum Ausdruck, dass im Laufe einer Biographie der personalen Identität kontextbedingte Änderungen entstehen, die sich im Datenzyklus widerspiegeln können und den Bedarf einer Anpassung auslösen, was in einem Identitätsverwaltungsmodell einzubeziehen ist. Dieser Datenzyklus ist nach dem Erkenntnismodell geprägt von den Daten, den Informationen und dem Wissen, wobei die Informations- und Wissenserlangung als Kommunikationsvorgänge einzuordnen sind.[282] Dem folgend wird die Bezeichnung des „Datenschutzes" als unzutreffend gesehen, denn es gehe um den Schutz vor Informationen und Wissen über natürliche Personen, damit Fehlentwicklungen von Informationen und Erkenntnissen erkannt und korrigiert werden können.[283] Demnach kann mit der Perspektive auf das datenschutzrechtliche Phänomen der Kommunikation möglicherweise ein Paradigmenwechsel mit einem Identitätsverwaltungsmodell vorgenommen werden, der in einer Verlagerung des datenbasierten Ansatzes auf ein Verfahren der Erkenntniserlangung über die personale Identität liegt.

Es kommt insgesamt nicht allein auf die mit der personalen Identität verbundenen Daten, Informationen und das Wissen an, sondern auf die damit verbundenen Kommunikationsvorgänge mit ihren Regeln und *Instruktionen* zur Erkenntniserlangung. Darin würde die für ein Identitätsverwaltungsmodell erforderliche Metaebene einbezogen werden. Dabei ginge es um *Instruktionen* zur Informations- und Wissenserlangung in einem Verfahren, welches für die Herbeiführung eines Ergebnisses als Bild der personalen Identität eingesetzt werden könnte. In dieser Metaebene in einem Identitätsverwaltungsmodell könnte eine Antwort auf die von Dataisten festgestellte Umkehrung der Erkenntnispyramide liegen, wonach die Dominanz der Daten für den menschlichen Erkenntnisprozess dem Einsatz intelligenter Algorithmen weicht, denn diese würden einen „höheren Er-

282 „Jede Information ist vielmehr Kommunikation", vgl. *Veil*, NVwZ 2018, 686 (687); *Albers*, Informationelle Selbstbestimmung, 2005, S. 88.

283 *Spiecker gen. Döhmann*, in: Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, 263 (265); *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 3 mwN.; *Haft*, Einführung in die Rechtsinformatik, 1977, S. 16; ebenso den Schutz des Erkenntnisgehalts von Daten betonend, *Drexl*, JIPITEC 2017, 257 (263) Rn. 24.

kenntniswert“ generieren und die Bedeutung der Daten verdrängen.[284] Demnach können übergeordnete *Instruktionen* den algorithmusbasierten Erkenntnisprozessen entgegengehalten werden, so dass mit den *Instruktionen* eigenständige Bilder personaler Identitäten generiert können. Diese sollen als Gegenbild in die Kommunikation einbezogen werden. Mit den festgelegten Verfahrensregeln und *Instruktionen* könnte die Kontrolle über die Interpretations- und Erkenntnisprozesse zu den Bildern personaler Identitäten in einem Identitätsverwaltungsmodell implementiert werden.

IV. Zwischenergebnis

Für die Identitätsverwaltung ist das Erkenntnismodell maßgeblich, um den Kontrollgegenstand bestimmen zu können. Zunächst ließe sich annehmen, dass die Kontrolle über Daten-Informationen-Wissen zu personalen Identitäten entscheidend sei. Jedoch stehen in Anbetracht des amöbenartigen kontextspezifischen Informations- und Erkenntnisgehaltes die *Instruktionen* im Vordergrund. Mit den *Instruktionen* wird der Schutz über kontextspezifische Wahrheitsgehalte gewährleistet, da Informationen und Erkenntnisse in Systemen nicht absolut und objektiv sind. Die Identitätswaltung sollte daher den Aggregatzustand von Informationen einbeziehen und sich über den Datenzyklus erstrecken. Damit liegt ein Paradigmenwechsel insofern vor, dass sich die Identitätsverwaltung auf die Kommunikation und die Metakommunikation in Gestalt der *Instruktionen* erstrecken soll. Folglich bedarf es der Kontrolle personaler Identitäten unter Einbeziehung der Kommunikation und der *Instruktionen*.

C. Kontrolle personaler Identitäten

Das Konzept der Kontrolle über die personale Identität kann aus den Grundrechten und dem einfachen Recht abgeleitet werden (I.). Die Kontrolle soll dabei in eine absolute (II.) und relative Kontrolle (III.) unterteilt werden, wobei sich das Konzept der Kontrolle als Paradoxon (IV.) gegenüber dem Schutz der informationellen Selbstbestimmung erweist. Die Wirkungen des Kontroll-Paradoxons sollen bei der Übertragung der Kontrolle auf das Identitätsverwaltungsmodell (V.) näher untersucht werden.

---

284 *Harari*, Homo Deus, 2017, S. 498–500.

I. Einführung

Der Kontrollbegriff für ein Identitätsverwaltungsmodell lässt sich bereits aus dem Volkszählungsurteil herleiten, welches den Schutzbedarf gegen „unkontrollierbare Persönlichkeitserfassung“[285], unkontrollierbare Nebenfolgen mit der Weitergabe des Namens[286] und den Bedarf nach Kontrolle über Persönlichkeitsbilder, die aus Datensammlungen zusammengefügt wurden, beschreibt[287]. Weiter lässt sich der Kontrollbegriff direkt aus der Datenschutzgrundverordnung ableiten, indem die Kontrolle über die eigenen Daten in den Erwägungsgründen (EWG) 7 S. 2; 13, S. 1; 68 S. 1; 75 benannt wird und der Kontrollverlust über die personenbezogenen Daten als mögliche Grundlage für einen Schadensersatzanspruch nach dem EWG 85 S. 1 vorgesehen ist. Daraus lässt sich ein Verständnis über den Kontrollbegriff ableiten, wonach es um das bewusste Einwirken, Beherrschen, Gestalten und Beaufsichtigen der personenbezogenen Daten geht. Gleichzeitig realisiert sich in diesem einfachrechtlichen Kontrollbegriff das grundrechtliche Konzept der informationellen Selbstbestimmung und der Schutz, dass die Handlungen in der privaten und öffentlichen Sphäre über die Informationen und Bilder zur Identität beherrschbar sind. Gegen den Begriff der Beherrschbarkeit von Informationen führt *Marsch* auch unter Einbeziehung des Begriffs der Kontrolle jedoch die fehlende Beherrschbarkeit von Interpretationsvorgängen an.[288] Demgegenüber wird aus einer rechtskulturellen Perspektive die Kontrolle als Bestandteil des kontinentaleuropäischen Privatheitskonzepts angesehen,[289] was die Entscheidungsmöglichkeit über die Offenlegung von Informationen über die Begründung und Entwicklung des eigenen Bildes[290] umfasst. Folglich geht es bei den Begriffen der Kontrolle und Beherrschbarkeit von Informationen nicht allein um ein absolutes Verständnis, sondern es kommt ebenso die relative Be-

285 BVerfGE 65, 1 (4).
286 BVerfGE 65, 1 (18).
287 BVerfGE 65, 1 (42).
288 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 99 f.
289 *Whitman*, Yale L. J. 2004, 1151, (1161, 1199): Insgesamt könne es nicht um ein Konzept der absoluten Kontrolle gehen, sondern immer nur um die relative Kontrolle.
290 *Dreier*, Bild und Recht, 2019, S. 60, 68, ebenso den Begriff der „Kontrolle über das eigene (Lebens)Bild“ und der „Kontrolle über das eigene Selbstbild“ verwendend; *Albers* geht von der Chance aus, das Wissen oder das „Bild“ anderer zu beeinflussen, vgl. *Albers*, Informationelle Selbstbestimmung, 2005, S. 576.

herrschbarkeit und Kontrollierbarkeit von Bildern personaler Identitäten in Frage.

Der für das Identitätsverwaltungsmodell anzuwendende Begriff der Kontrolle soll daher als Synonym für das Herrschaftsrecht über die personenbezogenen Informationen verstanden und folgend differenziert werden. Demnach wird die Kontrolle über die Entscheidung, was zum Privaten gehöre und was gegenüber einem Dritten zu eröffnen ist, angenommen.[291] In diesem absolut privaten Kontext wird gerade die „kontrollierte Unzugänglichkeit" als Kriterium des Privaten beschrieben.[292] Dazu gehört die räumliche und die informationelle Abgeschiedenheit, die den Kern der Selbstbestimmung ausmacht und die Kontrolle über private Entscheidungen und Handlungen umfasst.[293]

Gleichzeitig ist die Kontrolle nicht solipsistisch ausgestaltet, sondern die Kontrolle hat den Zugang, die Offenlegung und die Verwendung von persönlichen Informationen zum Gegenstand, so dass es sich bei der Kontrolle auch um ein Konzept der kommunikativen Privatheit handelt.[294] Mit der kommunikativen Ausprägung der Kontrolle soll von einer relativen Kontrolle ausgegangen werden. Danach kann über den Zugang und die Offenlegung persönlicher Informationen die Kontrolle ausgeübt werden, aber die Auswirkungen bei dem Kommunikationspartner liegen außerhalb des Kontrollierbaren und sind daher relativ. Dennoch unterliegt nach der Rechtsprechung des Bundesverfassungsgerichts auch dieser Bereich dem grundrechtlichen Schutz, denn es wird auch geschützt, dass das erlangte Wissen der Kommunikationspartner für das Individuum einigermaßen einschätzbar ist.[295] Darin kommt zum Ausdruck, dass die relative Kontrolle innerhalb der Kommunikation besteht und eine Vorhersehbarkeit von Gegenbildern geschützt wird. Entsprechend wird die Relativität der Kontrolle durch die rechtlichen Regelungen über den Schutz vor Beleidigungen und dem Recht am eigenen Bild etwa über das Einwilligungserforder-

---

291 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 21; von „Einflusschancen" und „Einflussmöglichkeiten" ausgehend, *Albers*, Informationelle Selbstbestimmung, 2005, S. 114, 122.

292 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 34–37.

293 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 37.

294 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 162; *DeHert/Gutwirth*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 61 (74 f.)

295 BVerfGE 65, 1 (43).

nis nach § 23 KUG geschützt, so dass von einem Konzept der absoluten Kontrolle über die Privatheit nicht ausgegangen werden könne.[296]

Demnach soll in das Identitätsverwaltungsmodell die Kontrolle über die personale Identität in relativer Hinsicht einbezogen werden. Denn die Informationen über die personale Identität unterliegen der relativen Kontrolle, wohingegen die Datensätze zu dieser absolut kontrollierbar sein können. Aufgrund des mit dem Phänomen *Big Data* einhergehenden Bedarfs, die Kontrollierbarkeit über Profilinhalte und Scoringwerte wiederherzustellen, erscheint die grundrechtlich begründete Beherrschbarkeit und absolute Kontrolle mit Hilfe eines Eigentumsrechts an Daten naheliegend, aber möglicherweise nicht problemlösend. Im Folgenden soll demnach ein Konzept der absoluten und relativen Kontrolle nachvollzogen werden.

II. Absolute Kontrolle

Die absolute Kontrolle über die personalen Identitäten kann sich aus einem Konzept des Dateneigentums in Gestalt eines Verfügungsrechts über die Bilder personaler Identitäten ableiten lassen (1.). Ein solches Konzept könnte zu einem rechtlichen Schutzmechanismus führen, der den *Big Data*-Phänomenen am ehesten Rechnung trägt. Gleichwohl fügt sich eine Kommerzialisierung des allgemeinen Persönlichkeitsrechts in Anbetracht der absolut wirkenden informationellen Selbstbestimmung in das bestehende Datenschutzrecht schwerlich ein, so dass sich die absolute Kontrolle in Gestalt eines Zugangsrechts zu personalen Identitäten für das Identitätsverwaltungsmodell als geeignet erweisen kann (2.).

1. Eigentumsrecht an Daten?

Der Kontrollbegriff in der DSGVO lässt sich mit einem Konzept des Eigentumsrechts an Daten in Verbindung bringen, zumal in der englischsprachigen Fassung des EWG 68 S. 7 der Begriff „*own*" verwendet wird. Gerade unter Einbeziehung der *Big Data*-Phänomene und des Internets der Dinge wird das Konzept des Dateneigentums als ein Lösungsmechanismus gegenüber bestehenden Schutzeinbußen gesehen.[297] Grundsätzlich haftet

296 *Whitman*, Yale L. J. 2004, 1151 (1169, 1199).
297 *Janeček*, CLSR 2018, 1039 (1040 f).

jedoch einem Eigentumsrecht über personenbezogene Daten ein fragwürdiger Gehalt an, da mit dem Versuch der Kommerzialisierung von Daten auch die Kommerzialisierung des allgemeinen Persönlichkeitsrechts und der Unantastbarkeit der Menschenwürde einhergeht. Gleichzeitig ist die Verfügung über absolute grundrechtliche Positionen im Zivilrecht anerkannt, so dass eine eigentumsähnlich ausgestaltete Position über Daten als sonstiges Recht nach § 823 Abs. 2 BGB angenommen wird und das praktische Bedürfnis nach einem umfassenden Schutz des Rechts auf informationelle Selbstbestimmung diese Einordnung rechtfertige.[298] Weiter wird das Dateneigentum als Konstruktion des Treuhandeigentums diskutiert, wonach über die Einwilligung hinaus eine Treuhandabrede geschlossen werden könnte und der Verantwortliche die personenbezogenen Daten als vermögenswertes Gut gewinnbringend einsetzen müsste, so dass zwischen einem effektiven Kontrollrecht über Daten aus ökonomischer Perspektive („*economic property right*") und dem rechtlich zugewiesenen Verfügungsrecht („*legal property right*") differenziert werden würde.[299] Dagegen lässt sich jedoch anführen, dass Daten nicht automatisch ein Wert zukommt, was aber die Voraussetzung für ein Konzept des Dateneigentums wäre. So lässt sich anhand eines Berechnungsbeispiels über den Wert von personenbezogenen Daten in sozialen Medien ein geringer Wert feststellen: Denn die Übernahme etwa von *Whats-App* durch *Facebook* für ca. 18 Milliarden Dollar hätte einen Datenwert von 42 Dollar pro Nutzer-Konto zur Folge und der Wert von Benutzerdaten auf dem Schwarzmarkt würde wenige Cent für ein Email-Konto betragen.[300] Nach diesem Beispiel erscheint der Auszahlungsbetrag für die Verarbeitung personenbezogener Daten nicht ansprechend genug, um damit eine Schutzsteigerung für die informationelle Selbstbestimmung der Betroffenen insgesamt herbeiführen zu können.

Weiter sieht das von *Janeček* entwickelte Konzept über ein Eigentumsrecht an Daten einen aktiven Teil, der die Kontrolle umfasst, und einen passiven Teil, der den Schutz der Daten umfasst, vor.[301] Hinsichtlich des zu kontrollierenden Gegenstandes stellt sich die Frage nach der Bestim-

298 *Wagner*, in: Säcker (Hrsg.), Münchener Kommentar – BGB, 2015, Bd. 5, § 823 BGB Rn. 294–297.

299 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 138–140. Ebenso ein Ausschließlichkeitsrecht an Daten zugunsten des wirtschaftlich verantwortlichen Datenerzeugers in Gestalt von Nutzungsrechten begründend, vgl. *Specht*, CR 2016, 288.

300 *Bernau*, FAS vom 10.02.2019, 23.

301 *Janeček*, CLSR 2018, 1039 (1042).

mung des Kontrollgegenstandes. Dies stößt bei personenbezogenen Daten jedoch deswegen auf Schwierigkeiten, weil zum einen der Übergang von Daten zu Informationen fließend und zum anderen die Personenbeziehbarkeit kontextspezifisch ist, so dass die Daten allein als Eigentumsgegenstand in Betracht kämen.[302] Daher wird eine Regelung über ein Eigentumsrecht an Daten als unzureichende Lösung gesehen und vielmehr auf ein Dateneigentumskonzept abgestellt, nach dem auf die faktische Kontrollmöglichkeit etwa über das Recht auf Datenportabilität nach Art. 20 DSGVO abgestellt werde, der sog. *Bottom up*-Ansatz.[303] Dennoch ist bei diesem Ansatz die Abbildbarkeit der Kontrolle kaum realisierbar, da bei Systemen mit einem hohen Vernetzungsgrad und redundanten Speichersystemen die faktische Kontrollmöglichkeit kaum umzusetzen und der faktisch kontrollierte Datensatz kaum zu ermitteln ist.[304] Erschwerend kommt hinzu, dass bei der Annahme eines kontrollierbaren Datensatzes die Zuordnung zu einem Eigentümer erfolgen müsste. Dieser könnte sich nach dem Grundsatz des Erstbesitzes und nach den Grundsätzen der Publizität ableiten lassen, was aber aufgrund der kaum feststellbaren Publizität und der fehlenden Haptik und Visualität von Daten kaum realisierbar sei.[305] Neben den dogmatischen Hürden, ein Eigentumsrecht an Daten zu begründen, kommt das Wesen der informationellen Selbstbestimmung hinzu, einen Kommunikationsprozess als Grundbedingung der Persönlichkeitsbildung vorauszusetzen. Denn die Anknüpfung an den Kommunikationsprozess verhindert die eindeutige Zuordnung der faktischen Kontrolle, da die Kontrolle über Informationen relativ ist. Weiter könnten Daten nicht als Partikel des Selbst an Dritte überlassen und nach Belieben wieder zurückgegeben werden.[306]

Darin kommt gerade die von *Marsch*[307] angeführte dogmatische Problematik zum Ausdruck, dass im einfachen Recht keine Unterscheidung zwischen den Datenverarbeitungen durch die öffentliche und private Stelle vorgenommen werde. Denn die Datenverarbeitung durch öffentliche Stellen kann durch eine Ermächtigungsgrundlage gerechtfertigt sein, ohne dass es eines Momentes der Kontrolle in Gestalt einer Einwilligung durch den Betroffenen bedurfte. Ferner wird festgestellt, dass Informationsord-

302 *Ders.*, CLSR 2018, 1039 (1043, 1052).
303 *Ders.*, CLSR 2018, 1039 (1051).
304 *Ders.*, CLSR 2018, 1039 (1045).
305 *Ders.*, CLSR 2018, 1039 (1048–1050); *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 8
306 *Masing*, NJW 2012, 2305 (2307).
307 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 103 f.

nungen nicht eigentumsanalog ausgestaltet sein können, da die Vielschichtigkeit von Informationsströmen und ihre gesellschaftlichen und ökonomischen Wirkungen mit einem Verfügungsrecht nicht ausreichend abbildbar sind.[308] Zudem könne ein Eigentumsrecht an Daten zu einer Steigerung der Marktmacht führen, wenn Intermediäre über einen hohen Datenbestand verfügen, was gerade aus wettbewerbsrechtlicher Perspektive zu vermeiden sei.[309] Insgesamt werde die Anknüpfung an den Begriff der Kontrolle des Betroffenen über seine Daten in der DSGVO daher mehr als rechtspolitische PR gesehen als die tatsächliche rechtliche Einräumung einer Kontrollmöglichkeit.[310]

Schließlich kann die Diskussion über ein Eigentumsrecht auch auf rechtskulturelle Einflüsse aus dem angelsächsischen oder angloamerikanischen Privatheitskonzept einer „*reasonable expectation of privacy*" zurückgeführt werden,[311] wonach ein Verfügungsrecht über die Preisgabe von persönlichen Informationen nahezuliegen scheint. Es kommt daher anstelle eines Verfügungsrechts über personenbezogene Daten das Zugangsrecht in Betracht, denn auch der strafrechtliche Schutz gegen das Ausspähen von Daten nach § 202a StGB setzt einen Schutz gegen den unbefugten Zugang zu Daten voraus.[312] Ein mögliches Verfügungsrecht an Daten kann demnach mit dem Zugangsrecht abgebildet werden, so dass das Zugangsrecht der Gegenstand absoluter Kontrolle wird. Somit sieht *Kühling* gegenüber einem Dateneigentumsrecht den Steuerungsbedarf auf der Ebene der Zugänglichkeit zu Informationen, denn zu der Freiheit, die eigenen Daten weiterzugeben, gehöre spiegelbildlich, dies genau nicht zu tun und keinen Zugang zu gewähren.[313]

2. Zugang als absolute Kontrolle

Dem Konzept der absoluten Kontrolle folgend, geht es um das Bestehen eines Zugangs zu den personenbezogenen Daten und der daraus ableitba-

308 *Reinhardt*, AöR 142 (2017), 528 (535 f.); *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 9; *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 40; *Graf von Westphalen*, IWRZ 2018, 9 (13 f.).

309 *Drexl*, JIPITEC 2017, 257 (266) Rn. 36; *Bundeskartellamt*, Fallbericht vom 15.02.2019, Az.: B6-22/16.

310 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 105.

311 *Jay*, Data protection law and practice, 2012, Rn. 2.66.

312 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 13 f.

313 *Dies.*, Rechte an Daten, 20. November 2018, S. 20.

ren personalen Identität. Dabei ist zu differenzieren zwischen der inneren Dimension als Kontrollentscheidung[314] über die Zugangsgewährung und der äußeren Dimension als tatsächlichen Zugang über das Wissen eines Passwortes oder den Besitz eines Schlüssels. Von der äußeren Dimension des Zugangs ist die räumliche Dimension umfasst, nach der zwischen Privatheit und Öffentlichkeit zu differenzieren ist. Es kann darum gehen, Dritte vom Zugang zu privaten Räumen in örtlicher und informationeller Hinsicht auszuschließen.[315] Die innere Dimension umfasst die Entscheidung über die informationelle Selbstbestimmung in Gestalt der Gewährung des Zugangs zu den personenbezogenen Daten und der personalen Identität durch Dritte.

Das Konzept der absoluten Kontrolle über den Zugang in seiner äußeren Dimension ist im Folgenden maßgeblich und umfasst den Zugang durch Wissen oder Besitz. Ein Zugangssystem über Wissen erfolgt etwa durch die Kenntnis eines Passwortes, wohingegen der Zugang auch mit dem Besitz eines Schlüssels möglich ist und sich auf die Kontrolle der Informationsflüsse erstrecken kann.[316] Am Beispiel des Zahlungsverkehrs wird der Zugang mit Wissen und Besitz eingeräumt, wie es beim Einsatz der Bankkarte vereint wird und beim Online-Banking über das TAN-Verfahren die Transaktion durch Wissen des Passwortes und der TAN authorisiert wird. Daraus lässt sich die jeweilige Zugangsmöglichkeit zu einem Identitätsverwaltungssystem ableiten, bei dem der Zugang durch Wissen und Besitz gemeinsam angewendet und mit den Attributen der personalen Identität in Verbindung gebracht werden kann. Als technisches Zugangssystem in einem Identitätsverwaltungsmodell kommen insbesondere der elektronische Personalausweis als Authentifizierungssystem, ein Pseudonym zur persönlichen Identifikation und die elektronische Signatur in Betracht.[317] Entsprechend wurde in Südafrika ein Identitätsverwaltungssystem implementiert, welches für öffentliche und private Einrichtungen genutzt und als Authentifizierungs-, Identifizierungs- und Zahlungsmittel eingesetzt werden könne, ohne dass der Nutzer sein Kontroll- und Korrek-

314 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 82

315 *Ders.*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 33 f.

316 *Smedinghoff*, Introduction to Online Identity Management, S. 7; *Sorge/Wethoff*, DuD 2008, 337; *Eichenhofer/Gusy*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 65 f.; ingesamt zum Datenzugang, *Albers*, Informationelle Selbstbestimmung, 2005, S. 112.

317 *Sorge/Wethoff*, DuD 2008, 337 (338–341).

turrecht verliere, sog. „*smart cards*".[318] In dieser Art von Identitätsverwaltungskonzepten erscheint jedoch die Einbeziehung datenschutzrechtlicher Maßgaben fraglich. Entsprechend wird aber bei dem elektronischen Personalausweis die Stärkung der informationellen Selbstbestimmung durch die Möglichkeit eines kontrollierten Umgangs mit den Attributen durch den Ausweisinhaber angenommen.[319]

Darüber hinaus sei eine sektorspezifische Realisierung von einem Zugangsrecht möglich, wobei ein entsprechender Anspruch auf Zugang zu Intermediären mit marktbeherrschender Stellung wünschenswert wäre.[320] Folglich wurde das Zugangsrecht als Kontrolle und Informationsmöglichkeit gegenüber dem Intermediär „*Facebook*" in einer jüngeren erbrechtlichen Entscheidung des Bundesgerichtshofes[321] anerkannt. Danach wurden auch nicht-vermögensrechtliche Zugangsrechte zu einem *Facebook*-Benutzerkonto für vererblich erklärt. Hervorzuheben ist dabei, dass der Zugang zu dem gesamten Inhalt, einschließlich der inhaltlichen Kommunikationsdaten des Benutzerkontos, auf die Erben übergegangen ist und ein eingeschränkter Zugang zu dem im Gedenkzustand befindlichen „Datenfriedhof" dem erbrechtlichen Grundsatz der Universalsukzession nicht entspräche.[322] Dabei wird in der Urteilsbegründung der Vergleich zu einem Girovertrag vorgenommen, der ebenfalls im Wege der Gesamtrechtsnachfolge auf die Erben übergehe.[323] Folglich können als Zugangssysteme das Wissen über das Passwort und der Besitz eines Schlüssels auf die Erben übergehen.[324] Maßgeblich sei die Vererblichkeit des Zugangsrechtes und nicht der Umstand, dass auf dem Benutzerkonto personenbezogene Daten und Kommunikationsdaten aus der Privatsphäre gespeichert sind, denn das Erbrecht erfasst nicht den Schutzgehalt der informationellen Selbstbestimmung, wie es der BGH über die nicht Vererblichkeit von Geldentschädigungsansprüchen bei der Persönlichkeitsverletzung bereits entschieden habe.[325]

Weiter berührt die absolute Kontrolle über den Zugang zu personenbezogenen Daten und damit der personalen Identität in inhaltlicher Hinsicht

318 *Black*, Cornell Int'l LJ 34 (2001), 397 (431).
319 *Hornung/Möller*, Passgesetz, Personalausweisgesetz, 2011, § 18 PAuswG Rn. 5.
320 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 22; *Drexl*, JIPITEC 2017, 257 (276) Rn. 101.
321 BGH, Urt. v. 12.07.2018 – III ZR 183/17.
322 BGH, Urt. v. 12.07.2018 – III ZR 183/17 Rn. 17–30.
323 BGH, Urt. v. 12.07.2018 – III ZR 183/17 Rn. 36.
324 BGH, Urt. v. 12.07.2018 – III ZR 183/17 Rn. 49–50.
325 BGH, Urt. v. 23.05.2017 – VI ZR 261/16.

die grundsätzliche Frage, *ob* der Zugang von den Intermediären eingeräumt wird. Weiter wird sich die Frage stellen, *wie* im Einzelnen die Zugangsgewährung ausgestaltet sein wird, und welches Bild der personalen Identität das Individuum einsehen darf. Folglich wird die Kontrolle über personenbezogene Daten und der Zugang zu den personalen Identitäten von den wirtschaftlichen Interessen des Intermediärs geprägt sein und kann im Einzelnen durch die Interessen der Intermediäre, wie es die oben genannte *Facebook*-Entscheidung belegt, erschwert werden. Weiter lässt sich dies im Zusammenhang mit personalisierter Werbung nachweisen, da sich mit der Werbung eine Wertsteigerung der personenbezogenen Daten für den Verantwortlichen herbeiführen lässt, den Betroffenen jedoch der Zugang zu den entsprechenden Profilen oder Geschäftsmodellen verwehrt bleibt.[326] Auch hierbei lässt sich eine Diskrepanz zwischen den generierbaren Erkenntnissen aus den personenbezogenen Daten und dem tatsächlichen Zugang zu diesen konstatieren.

3. Zwischenergebnis

Die absolute Kontrolle über personenbezogene Daten kann weder aus dem bestehenden Recht noch aus dem Eigentumsrecht an Daten begründet werden. Damit können Daten als Kontrollgegenstand ausgeschlossen werden, es sei denn, sie fungieren als Schlüssel mit dem der Zugang zu personenbezogenen Daten gewährt wird. Denn die absolute Kontrolle in einem Identitätsverwaltungsmodell lässt sich hinsichtlich des Zugangs zu der personalen Identität und ihren Teilidentitäten abbilden. Danach kann die absolute Kontrolle über das Wissen und den Besitz die Zugangserlangung ermöglichen, wie es etwa bei beim Einsatz des elektronischen Personalausweises, der elektronischen Signatur oder bei Bankgeschäften mit dem Einsatz einer Karte oder eines Passwortes der Fall ist.

III. Relative Kontrolle

Die relative Kontrolle ist aus dem kommunikativen Vorgang der Interpretation und der Erkenntniserlangung aus Daten nach dem Erkenntnismodell abzuleiten. Danach besteht zwar eine absolute Kontrolle über die Da-

326 Zur Methode der Score-Bestimmung als Geschäftsgeheimnis, BGHZ 200, 39 (47) – SCHUFA.

ten, die Interpretation dieser und die Erkenntniserlangung in Gestalt von Wissen unterliegt aber der Perspektive und den *Instruktionen* des interpretierenden und lernenden Kommunikationspartners. Demnach liegt die Kontrolle in informationeller Hinsicht vor, wenn über die Erkenntnisse von Dritten und die Gegenbilder eine Einflussnahmemöglichkeit besteht. Diese Einflussnahmemöglichkeit stelle eine Ausprägung des selbstbestimmten Verhaltens über die informationelle Privatheit dar.[327]

Dennoch sind einmal offengelegte Informationen in ihren Interpretationsmöglichkeiten kaum mehr beherrschbar, denn die Offenlegung der Informationen gegenüber dem Kommunikationspartner bewirkt den Verlust der Einflussmöglichkeiten auf diese Informationen und Erkenntnisse. Vergleichbar mit einem Brief, können Nachrichten kontrolliert versendet werden, demgegenüber unterliegt nicht der Kontrolle, wer die Inhalte zur Kenntnis nimmt und seine Rückschlüsse daraus zieht. Demnach kann mit der Einwilligung nach Art. 6 Abs. 1 a) DSGVO zwar die absolute Kontrolle über die Erklärung ausgeübt werden, aber die damit einhergehende Rechtfertigung über die Verarbeitung personenbezogener Daten erlaubt zugleich die vielfältigen Interpretationsmöglichkeiten durch den Verantwortlichen. Mit der Einwilligung werden daher Informationen preisgegeben, die irreversibel in ihren Auswirkungen bis hin zur möglichen Ausübung der Betroffenenrechte sein können. Somit ist ab dem Vorliegen der Rechtfertigung über den Datenverarbeitungsvorgang der Datenzyklus über die personale Identität begründet und es können folglich für diesen Zeitraum im Rahmen der Zweckmäßigkeit die Informationen über die Person generiert werden, ohne dass eine Kontrollmöglichkeit besteht.

Im Rahmen der relativen Kontrolle über die Informationen und das Wissen bleibt die Möglichkeit der Kontrolle durch *Instruktionen* über die konkrete Ausführung des Interpretations- und Lernvorgangs. Denn nicht jedes Erlernen in einem Kontext ist zulässig, wie es die *Instruktionen* aus § 81g StPO zur DNA-Identitätsfeststellung belegen, wonach aus der DNA allein das Identifizierungsmuster und das Geschlecht als Erkenntnis generiert werden dürfen und darüber hinaus keine weiteren Erkenntnisse gerechtfertigt wären. Somit gilt für die relative Kontrolle personaler Identitäten der Schutzmechanismus über *Instruktionen*, der für das Identitätsverwaltungsmodell herangezogen werden soll.

327 *Maus*, Der grundrechtliche Schutz des Privaten im europäischen Recht, 2007, S. 40.

IV. Kontroll-Paradoxon

Dem Konzept der Kontrolle personaler Identitäten für das Identitätsverwaltungsmodell könnte entgegenstehen, dass die Einräumung der Kontrolle nicht zwingend zu einer Steigerung, sondern möglicherweise zu einer Gefährdung des Schutzes der informationellen Selbstbestimmung führt.

Mit verhaltensökonomischen Untersuchungen zur Kontrolle des Nutzers bei der Verarbeitung personenbezogener Daten konnte ein Paradoxon festgestellt werden, wonach die Begründung der Kontrolle über personenbezogene Daten zu einer Einbuße des Schutzes führe.[328] Es wurde mit statistischen Untersuchungen nachgewiesen, dass differenzierte Privatheitseinstellungen und die damit einhergehende Kontrolle, eine gesteigerte Bereitschaft beim Nutzer auslöse, Informationen offenzulegen.[329] Dieses Phänomen wurde besonders deutlich, wenn zuvor das Bestehen der Kontrollmöglichkeit zugesichert wurde.[330] Aufgrund dieser Untersuchungen könne eine Schutzsteigerung durch die Erweiterung oder Begründung eines Kontrollkonzeptes nicht angenommen werden, vielmehr liege ein Kontroll-Paradoxon vor.[331]

Sobald dieses Ergebnis auf die Einwilligung übertragen wird, lässt sich mit dem Vorgang der Einwilligung bereits die Gefahr einer die Privatheit einschränkenden Handlung erblicken, die zu einer Absenkung des individuellen Privatheitsniveaus führen kann. Denn nach den dargestellten Untersuchungen von *Brandimarte/Acquisti/Loewenstein* könne die Einwilligung eine gesteigerte Bereitschaft auslösen, Informationen offenzulegen oder überhaupt einzuwilligen. Folglich soll festgehalten werden, dass mit einer Steigerung des Kontrollniveaus nicht gleichzeitig die Steigerung des Schutzes der Privatheit einhergeht, vielmehr folgt mit der Kontrollmög-

328 *Brandimarte/Acquisti/Loewenstein*, Social Psychological and Personality Science 4 (2013), 340.

329 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (344, 346) mit Verweis auf einen „Post" von Marc Zuckerberg mit dem Titel „*Giving you more control of your privacy*". Es konnte festgestellt werden, dass mit der suggerierten Kontrollmöglichkeit durch die Privatheitseinstellungen tatsächlich der Eindruck von Kontrolle erweckt werden könne, dieser aber irreführend sei, da das Kontroll-Paradoxon bei der eingeräumten Schutzmöglichkeit mit Privatheitseinstellungen wirken könne.

330 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (344).

331 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (346).

lichkeit eine Überschätzung der tatsächlichen Einflussmöglichkeit.[332] Denn aufgrund der Relativität von Informationen und Wissen, kann die absolute Kontrolle allein über Daten ausgeübt werden. Die ausdrückliche Einbeziehung eines Kontrollkonzeptes lenkt folglich von dem tatsächlichen Risiko für den Schutz der personenbezogenen Daten ab. Denn es wird die Illusion über die faktische Kontrollmöglichkeit von Interpretationen und Erkenntnissen aus Datenverarbeitungen geschaffen.

V. Übertragung auf das Identitätsverwaltungsmodell

In einem Identitätsverwaltungsmodell bedarf es der Kontrolle über die Realisierung der personalen Identität und ihrer Teilidentitäten, damit das Individuum seine informationelle Selbstbestimmung ausüben kann. Dabei bedeutet ein Kontrollkonzept die Vorverlagerung des Schutzes der personalen Identität, mit dem einer Verselbstständigung des Selbstbildes durch Fremdbilder begegnet und damit dem datenschutzrechtlichen Vorfeldschutz entsprochen wird. Dem ist immanent, dass bei einem Identitätsverwaltungsmodell das Individuum im Zentrum stehen muss, sog. „*user centric identity management*“[333]. Entsprechend kommen verschiedene Ausprägungen der Identitätsverwaltung in Betracht.

Es kann um die Kontrolle von Benutzerkonten mit der Authentifizierung oder Identifizierung des Nutzers im Sinne einer *Berechtigungsverwaltung* gehen. Weiter kommt aus der Perspektive des Verantwortlichen die Verwaltung von Profilen und Kommunikationsdaten in Betracht.[334] Schließlich kann ein kontextabhängiges Rollen- und Pseudonym-Management etwa mit biometrischen Daten oder *Single Sign-On*-Lösungen als Identitätsverwaltungskonzept dienen.[335] Gleichwohl lässt sich in diesen Ausprägungen jeweils der Datensatz als Gegenstand der Kontrolle im Identitätsverwaltungssystem über das Wissen eines Passwortes als *Idem*-An-

---

332 *Dies.*, Social Psychological and Personality Science 4 (2013), 340 (346).

333 *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 30.

334 *Schallaböck*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 103 (121): Dabei wird auf die Identitäts-*Managementsysteme* der US-amerikanischen und britischen Geheimdienste verwiesen.

335 *Ders.*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 103 (107–109); *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 19; *Hornung/Engemann* (Hrsg.), Der digitale Bürger und seine Identität, 2016, S. 18.

teil einer personalen Identität feststellen, ohne die Ausprägungen einer personalen Identität in ihrem dynamischen *Ipse*-Anteil im online-Kontext einzubeziehen. Danach soll im Identitätsverwaltungsmodell die Realisierung der Interpretations- und Erkenntnisgehalte zum Gegenstand eines Kontrollkonzeptes im online-Kontext werden. Dies würde einen gesteigerten Einfluss auf die Bilder personaler Identitäten aus Profilbildungen ermöglichen. Folglich würden die generierbaren Erkenntnisse aufgrund ihrer Rück- und Auswirkungen auf das Individuum einbezogen werden und der Selbstbestimmung unterliegen.

Daraus lässt sich der Bedarf nach einer Übertragung des Kontrollgegenstandes auf den Zugang zu den Daten, Informationen und dem Wissen über eine personale Identität ableiten. Denn die Analysen über ein Eigentumskonzept an Daten haben dargelegt, dass ein Eigentumsrecht an Daten nicht zu einer Schutzsteigerung führt und rechtlich schwerlich abzubilden ist. Folglich soll ein Kontrollkonzept als ein Zugangsrecht für ein Identitätsverwaltungsmodell eingesetzt werden, um die Kontrolle über die personale Identität in absoluter und relativer Hinsicht zu ermöglichen. Damit würde die Kritik an einem Kontrollkonzept, dass aufgrund redundanter Speichermöglichkeiten *de facto* über die Datensätze keine Kontrolle ausgeübt werden könne,[336] ins Leere laufen. Denn es ginge nicht um die Kontrolle über die Daten, sondern um die Kontrolle über den Zugang zu Daten und den mit ihnen verbundenen Erkenntnissen.

Gleichwohl konnte aufgrund verhaltensökonomischer Untersuchungen belegt werden, dass die Kontrollmöglichkeit zu einer gesteigerten Bereitschaft der Offenlegung von Informationen führe und das Kontroll-Paradoxon wirke. Demnach könne bei einem ausdifferenzierten Kontrollkonzept von einem neuen Risiko ausgegangen werden, da mit der Einwilligung zwar die Kontrolle ausgeübt wird, aber damit eine gesteigerte Bereitschaft zur Offenlegung privater Informationen einhergehen kann. Danach wäre von einem „vollständigen Kontrollverlust“[337] auszugehen, der über ein differenziertes Zugangs- und Iterationskonzept kompensiert werden könnte. Damit wird dem Einzelnen die Möglichkeit eingeräumt, in einem iterativen und dialogischen Verfahren infolge des Zugangs zu den personenbezogenen Daten und personalen Identitäten, Einfluss auszuüben. Demnach würde es der informationellen Selbstbestimmung im online-Kontext entsprechen, eine erhöhte Differenzierung möglicherweise mit einem iterati-

336 *Veil*, NVwZ 2018, 686 f.; *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 20.

337 BVerfGE 120, 274 (336 f.).

ven und dialogischen Prozess vorzunehmen, welches der weitere Gegenstand dieser Untersuchung sein soll.

VI. Zwischenergebnis

Die Kontrolle personaler Identitäten erfolgt in absoluter Hinsicht über den Zugang und in relativer Hinsicht in einem dialogischen Verfahren. Dabei sollte die Kontrolle personaler Identitäten ein differenziertes Zugangs- und Iterationskonzept umfassen, um eine Schutzsteigerung herbeizuführen. Demnach ist ein dialogisches Verfahren erforderlich, was über *Instruktionen* für die Informations- und Wissenserlangung verfügt. Damit soll ein differenzierter Schutz der informationellen Selbstbestimung gewährleistet werden.

Insgesamt ist in dem Identitätsverwaltungsmodell das Kontroll-Paradoxon einzubeziehen, wonach die Kontrollmöglichkeit zu einer Überschätzung der Einflussmöglichkeit führen kann. Somit bedarf es der Differenzierung von personalen Identitäten, um Gegenstände der relativen Kontrolle und der *Instruktionen* für das Identitätsverwaltungsmodell bestimmen zu können.

D. Agenten personaler Identitäten

Zu den personalen Identitäten gehört das Verhalten des Individuums,[338] so dass sich die Frage nach der Handlungsträgerschaft im einfachen Recht stellt. Diese wirkt sich darauf aus, dass sich das Verhalten als identitätsbildend einordnen lässt und die Zurechnung des Verhaltens zu dem Individuum voraussetzt. Indem das Recht mit Fiktionen arbeitet, wird dem Individuum nach den zivilrechtlichen Vorschriften zur Rechtssubjektivität die Rechts- und Geschäftsfähigkeit gemäß §§ 1, 105 ff. BGB verliehen und das Individuum erlangt im Rechtsverkehr die Handlungsfähigkeit, was auch über Stellvertretungsregeln erfolgen kann.[339] Darin kommt eine Prinzipal- und Agentenstruktur zum Ausdruck, bei der das Individuum als Prinzipal über die rechtlich anerkannte Handlungsträgerschaft wirkt. Vorliegend sollen für ein Identitätsverwaltungsmodell die Handlungsträgerschaften herausgearbeitet werden, unter denen sich eine Übertragung der bestehen-

338 2. Teil, A., II., 2.
339 *Zippelius*, Das Wesen des Rechts, 62012, S. 27.

den Prinzipal- und Agentenstruktur auf den online-Kontext vornehmen lässt. Dabei sollen die bestehenden Prinzipal- und Agentenstrukturen aus den rechtlichen Konzepten im offline-Kontext herangezogen werden.

Für die Begründung einer graduellen Handlungsträgerschaft sind die zivilrechtlichen Stellvertretungsregeln und das Strafprozessrecht als Grundlage für einen Transfer zu einer elektronischen Handlungsträgerschaft heranzuziehen. Nach dem zivilrechtlichen Stellvertretungsrecht kann eine graduelle Steigerung der Kontroll- und Steuerungsmöglichkeit des Prinzipals ausgehend von dem Boten, dem Verrichtungsgehilfen (§ 831 BGB), dem Erfüllungsgehilfen (§ 278 BGB) hin zu dem Stellvertreter (§§ 164 ff. BGB) erfolgen, wobei für deren Einordnung das Offenkundigkeitsprinzip und die Verkehrsanschauung maßgeblich sind. Ein Bote unterliegt hinsichtlich des *Ob* und *Wie* seiner Handlung dem höchsten Kontroll- und Steuerungsmaß durch den Prinzipal. Dieses nimmt beim Verrichtungsgehilfen ab, der in seiner Erfüllung weisungsgebunden ist, aber über einen Ausführungsspielraum verfügt. Demgegenüber ist der Erfüllungsgehilfe bei der Erfüllung des Schuldverhältnisses nicht weisungsgebunden. Das Kontroll- und Steuerungsmaß ist bei der Stellvertretung wiederum geringer, wobei der Umfang im Einzelnen von der gesetzlichen oder vertraglichen Vertretungsmacht abhängt und sich ebenfalls nach der Verkehrsanschauung richtet.

In strafprozessualer Hinsicht stellen klassische Prinzipal- und Agentenstrukturen solche aus § 110a StPO dar, wonach verdeckte Ermittler mit einem sich steigernden Identitätsveränderungsgrad in Ermittlungsverfahren eingesetzt werden. Mit der qualifizierten Legende nach § 110a StPO wird etwa eine neue Identität mit den entsprechenden Ausweispapieren und dem Lebenslauf begründet, wohingegen der gelegentlich nicht offen ermittelnde Polizeibeamte situativ ohne Legende auftritt.[340] Weiter wird zum Schutz von gefährdeten Zeugen oder deren Angehörigen eine vorübergehende Tarnidentität § 5 Abs. 3 ZSHG erstellt, wobei ausdrücklich keine Identitätsänderung vorgesehen ist.[341]

Aus diesen einfachrechtlichen Regelungsstrukturen lässt sich eine Differenzierung der personalen Identität ableiten, bei der das Individuum als Prinzipal den Agenten des Bildes der personalen Identität kontrolliert und steuert. Das Bild der personalen Identität als Agent wird dem Individuum als Prinzipal zugerechnet, so dass das Identitätsverwaltungsmodell aus

340 *Meyer-Goßner/Schmitt*, Kommentar, Strafprozessordnung, 2019, § 110a StPO Rn. 7 f., 4.

341 *Soiné/Engelke*, NJW 2002, 470 (474).

mehreren Agenten in Gestalt von Bildern personaler Teilidentitäten des Individuums besteht. Demnach verlangt die Identitätsverwaltung die Annahme, dass sie von einem Prinzipal als natürliche Person durchgeführt wird, wobei der Agent in Gestalt des Bildes der Identität über keine Rechtssubjektivität verfügt und aus einem elektronischen Ausführungsmechanismus besteht. Somit liegt eine kontextspezifische Steuerungs- und Kontrollmöglichkeit gegenüber dem elektronischen Agenten als Handlungsträger vor, die entsprechend den Regeln der Handlungsträgerschaft graduell erfolgen kann.[342]

Die Eigenschaften des Agenten können dahingehend variieren, dass der elektronische Agent intelligent reaktiv oder proaktiv handeln kann. Ein *proaktiver Agent* wäre lernfähig und könnte dem Prinzipal Entscheidungen vorschlagen, wohingegen ein reaktiver Agent ausführend wäre.[343] Wobei *Aamodt/Nygård* zwischen aktiven und passiven Agenten bei der Entscheidungsunterstützung danach differenzieren, ob eine passive assistierende Funktion oder eine aktive Unterstützung in der Entscheidungsfindung wahrgenommen werde.[344] Beide Umschreibungen sind von der graduellen Autonomie und Abhängigkeit zum Prinzipal gekennzeichnet, jedoch soll der Klarheit wegen im Folgenden der aktive und passive Agent als Begriffspaar angewendet werden. Von einem elektronischen Agenten, der aktiv ausgestaltet ist und hinsichtlich des *Ob* und *Wie* über einen dem Stellvertreter entsprechenden Entscheidungsspielraum verfügt, kann ein hohes Risiko für den Prinzipal ausgehen, welches ihm zugerechnet werden würde.

Die Einheit, die aus dem Prinzipal und elektronischen Agenten besteht, wird von *Teubner* als „Hybrid" bezeichnet, dem wiederum eine Rechtssubjektivität zukommen könne, wenn diese über eine eigene Intelligenz verfüge.[345] Damit könnte die Vorstellung einbezogen werden, dass bereits Informationsströmen unter bestimmten Bedingungen eine Personalität zukommt, was eine eigenständige rechtliche Schutzwürdigkeit begründen könnte. Dabei könne der elektronische Agent auch eine fragmentierte Rechtssubjektivität als Teilrechtsfähigkeit mit begrenzter Handlungskompetenz darstellen.[346] Demnach solle die graduelle Charakteristik der Prin-

342 *Sester/Nitschke*, CR 2004, 548 (550).
343 *Dies.*, CR 2004, 548; *Hoffmann-Riem*, AöR 142 (2017), 1 (30) mwN.
344 *Aamodt/Nygård*, Data & Knowledge Engineering 16 (1995), 191 (195).
345 *Teubner*, Zeitschrift für Rechtssoziologie 2006, 5 (14).
346 *Ders.*, Zeitschrift für Rechtssoziologie 2006, 5 (10–12).

zipal- und Agenten-Beziehung und ihre Lebensdauer in eine fragmentierte Rechtssubjektivität überführt werden.[347]

Folglich lässt sich für die Ausprägungen der personalen Identität im online-Kontext und die dazugehörenden Informationsströme eine separate fragmentierte Subjektivität zusprechen, die für das Identitätsverwaltungsmodell als weiteres Element in Gestalt eines elektronischen Agenten maßgeblich sein könnte. Dabei soll die rechtstheoretische Einordnung, ob es sich um eine neu begründete Rechtssubjektivität handelt, dahinstehen, denn vorliegend soll die Differenzierung der personalen Identität in eine Prinzipal- und Agenten-Struktur mit ihren Bestandteilen im online-Kontext für die Modellbildung entscheidend sein. Demnach können sich die statischen *Idem*-Anteile und dynamischen *Ipse*-Anteile einer personalen Identität in einem elektronischen Agenten abbilden. Weiter würde die elektronische Ausgestaltung des Agenten den Bedarf nach Transparenz über die Funktionalität auslösen, was über die Wahrung der Transparenzanforderungen gemäß Art. 12 Abs. 7 S. 2 DSGVO in maschinenlesbarer elektronischer Form erbracht werden könnte. Ebenso kommt der elektronische Agent als Vermittler auf der Mikroebene in Betracht und könnte über Software oder einen „*Smart Contract*" realisiert werden. Schließlich kann ein Agent in einem Identitätsverwaltungsmodell auf der Makroebene eingesetzt werden, wenn es um mögliche kontextspezifische Realisierungen personaler Identitäten geht.

E. Ergebnis: Kontrollierbare Erkenntnisse zur personalen Identität

Die Anforderungen an die Identitätsverwaltung richten sich primär nach den verfassungsrechtlichen und einfachrechtlichen Vorgaben, aus denen sich die Eigenschaften und Kriterien für ein Identitätsverwaltungsmodell ableiten lassen. Maßgebliche Anknüpfung für die Identität im einfachen Recht ist der Name, der im Zusammenhang mit dem elektronischen Rechtsverkehr um die elektronische Signatur ergänzt wurde. Folglich stellt die einfachrechtliche Regelung zur gestuften und sicheren Identifizierung gemäß Art. 8 Abs. 2 eIDAS-VO eine statische Dimension über kontextspezifische Vertrauens- und Sicherheitsniveaus von personalen Identitäten dar. Weiter wird die *vertrauliche und sichere Kommunikation* nach dem De-Mail-G geschützt, so dass die personale Identität in ihrem dynamischen *Ipse*-Anteil im Rahmen der Kommunikation einen rechtlichen Schutz im on-

347 *Ders.*, Zeitschrift für Rechtssoziologie 2006, 5 (24).

line-Kontext erfährt.[348] Ferner umfasst das verfassungsrechtliche und einfachrechtliche Schutzregime über die personale Identität das Erkenntnismodell, welches sich auf die personale Identität innerhalb eines Datenzyklus über eine Biographie anwenden lässt. Dabei ist einem Identitätsverwaltungsmodell immanent, dass es im Rahmen der informationellen Selbstbestimmung eine Steuerungs- und Kontrollmöglichkeit über die Daten, Informationen und das Wissen zu einer personalen Identität vorsehen muss. Gleichwohl ist nach dem Erkenntnismodell eine absolute Kontrolle ausgeschlossen, denn zwischen den Kommunikationspartnern ist der Datensatz der Gegenstand von kontextspezifischen Interpretations- und Lernprozessen, da in der Kommunikation das Gegenbild über die personale Identität nur bedingt beeinflusst werden kann und damit der relativen Kontrolle unterliegt.[349] Aus dem Erkenntnismodell lässt sich der mögliche Bedarf an einer prozeduralen Konkretisierung über die Entstehung der Bilder personaler Identitäten ableiten, damit der dynamische Charakter der biographischen personalen Identität und den damit verbundenen Erkenntnissen in das Identitätsverwaltungsmodell überführt werden kann.

Als erweiternde Dimension kommt die systemische Perspektive der Kommunikation hinzu, nach der die kontextspezifische Kommunikation in einem System erfolgt und sich der Bedarf an der Beobachtung des Systems stellt. Mit der Beobachtung des Systems wird dieses mit der Metaebene über den Datenzyklus erweitert und ermöglicht die übergeordnete Bewertung der Erkenntnisse über personale Identitäten. Dazu gehört die Einbeziehung der *Instruktionen* in das Identitätsverwaltungsmodell, damit die Erkenntnisse über eine personale Identität einem eigenen Schutzregime unterliegen und nicht beliebig generiert werden können. Die Gestaltung des Identitätsverwaltungsmodells verlangt demnach ein iteratives Modell etwa mit der Erteilung mehrerer Einwilligungen in einem Datenzyklus und der Einbeziehung von *Instruktionen* über die Bildung der personalen Teilidentitäten.[350]

Schließlich ist für die Identitätsverwaltung die Handlungsträgerschaft über die personale Identität maßgeblich. Diese lässt sich entsprechend zum Stellvertretungsrecht in einen Prinzipal, dem die Handlung zugerechnet wird, und den Agenten, der als Handlungsträger fungiert, differenzieren. Weiter können sich die statischen *Idem*-Anteile und dynamischen *Ipse*-Anteile einer personalen Identität in einem elektronischen Agenten vereinen

348 3. Teil, A., II.
349 3. Teil, A., III.
350 3. Teil, B., I. – II.

und den datenschutzrechtlichen Transparenzregeln unterliegen.[351] Ferner wurde eine Differenzierung der Agentenstruktur auf der Mikro- und Makroebene vorgenommen, bei der ein Agent auf der Mikroebene aus Software oder einem *Smart Contract* besteht und auf die Bildung personaler Identitäten einwirkt und auf der Makroebene eine Vermittlungsstruktur zur Verwaltung personaler Identitäten in Betracht kommt.

351 3. Teil, D.

4.Teil: Begründung der Identitätsverwaltung im IKT-Recht

Für die Identitätsverwaltung im IKT-Recht soll eine differenzierte Analyse der maßgeblichen Rechtsregeln vorgenommen werden. Nach dem OSI-Schichtenmodell[352] ist die Anknüpfung auf der höchsten Ebene an die Dienste als Anwendungsebene vorgesehen, so dass die Datenschutzgrundverordnung, das Telemedienrecht und anschließend das Telekommunikationsrecht zum Gegenstand der Analysen werden. Zunächst sollen die Gegenstände der Identitätsverwaltung im online-Kontext aus der Datenschutzgrundverordnung abgeleitet werden, um daraus die Grundlagen für stipulative Definitionen zur Bewertung des IKT-Rechts herauszuarbeiten (A.). Dabei sollen die Schutzebenen innerhalb der Identitätsverwaltung bestimmt werden und gleichzeitig die Risiken für den Schutz der personalen Identität und der Erkenntnisse über diese nachvollzogen werden. Demnach soll sich die *Modellbildung der Identitätsverwaltung* aus der Datenschutzgrundverordnung an dem Datenzyklus und den damit verbundenen Risiken orientieren. Dies erfolgt anhand der datenschutzrechtlichen Grundidee eines phasenorientierten Datenschutzes[353] bei der Verarbeitung personenbezogener Daten. Folglich wird in den zeitlichen Dimensionen *ex ante* zur begründeten Rechtmäßigkeit der Datenverarbeitung (B.), der Rechtmäßigkeitsbegründung (C.) und *ex post* zur begründeten Rechtmäßigkeit (D.) unterschieden. Dabei werden die maßgeblichen datenschutzrechtlichen Vorschriften für die Identitätsverwaltung nachvollzogen. Diese Betrachtungen zur Datenschutzgrundverordnung werden mit den personalen Teilidentitäten aus dem Telemedien- und Telekommunikationsrecht ergänzt (E.), um die IKT-rechtlichen Ausprägungen der personalen Identität zu vervollständigen. Insgesamt sind dabei die konkreten Anforderungen an ein Identitätsverwaltungsmodell nach dem IKT-Recht herauszuarbeiten und anhand des stipulativen Identitätsverwaltungsmodells zu bewerten.

352 *Schmidt/Pruß*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 2018, § 3 Rn. 62–64.

353 *Steinmüller*, RDV 2007, 158 (159).

A. Identitätsverwaltung in der Datenschutzgrundverordnung

I. Personale Identität in der Datenschutzgrundverordnung

1. Personale Identität aus personenbezogenen Daten, Art. 4 Nr. 1 DSGVO

Bereits die Bestimmung des Schutzbereiches nach Art. 8 GRC nimmt Bezug auf die sekundärrechtliche Definition der personenbezogenen Daten. Danach sind personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Eine Person ist bestimmbar, wenn diese direkt oder indirekt identifiziert werden kann über die Personalausweis-, Telefon-, Konto- oder sonstige Nummer oder durch Elemente, die *Ausdruck* der physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sonstigen Identität sind.[354] Im Gegensatz zu dem im Kommissionsentwurf der DSGVO in Art. 4 Nr. 1 enthaltenen Wortlaut, „personenbezogene Daten (sind) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen", stellt der darauf folgende Entwurf des europäischen Rates ein Bekenntnis zum Identitätsbegriff dar und wurde auch in der Endfassung der DSGVO aufgenommen. Denn in Art. 4 Nr. 1 DSGVO werden personenbezogene Daten als Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität von natürlichen Personen beschrieben, die der Schutzbereichsbestimmung zu Art. 8 GRC entsprechen. In der Definition der personenbezogenen Daten ist keine abschließende Aufzählung über die möglichen Identitäten enthalten, sondern diese sind exemplarisch zu verstehen, wie es sich aus dem Wortlaut „Ausdruck" ergibt, dem die Bedeutung des Erscheinens gleichkommt. Ferner überschneiden sich die aufgezählten Identitätsausprägungen und können nicht unabhängig voneinander stehen, wie es bei der sozialen und kulturellen Identität augenscheinlich wird. Dies spricht insgesamt für die Annahme einer exemplarischen Aufzählung der Identitätsausprägungen in Art. 4 Nr. 1 DSGVO.

Weiter unterliegen personenbezogene Daten und die damit zum Ausdruck kommenden Identitäten einem geringeren Schutzniveau als die besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, an deren Verarbeitung höhere Anforderungen geknüpft sind. Zu den besonderen Kategorien personenbezogener Daten gehören die rassische und eth-

354 *Jarass*, Kommentar, Charta der Grundrechte der EU, 2016, Art. 8 GRC Rn. 5.

nische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit und genetische Daten (Art. 4 Nr. 13 DSGVO), biometrische Daten (Art. 4 Nr. 14 DSGVO) und Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) von natürlichen Personen. Diese besonderen Kategorien personenbezogener Daten können als Attribute[355] zu der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität in Erscheinung treten, so dass sie ungeachtet der Form der Daten als digital oder analog, Bild oder Ton[356] von dem Begriff und Schutz der personalen Identität umfasst sind. Dabei unterliegen die besonderen Kategorien personenbezogener Daten einem besonderen Risikogehalt für die Rechte und Freiheiten natürlicher Personen, wie es auch aus der Zuordnung als Risikokriterium in Art. 35 Abs. 3 b) DSGVO hervorgeht.

Ebenfalls kommen als Attribute die Standortdaten, online-Kennungen und die Telefonnummer in Betracht.[357] Daraus ergibt sich aus dem zentralen datenschutzrechtlichen Begriff der „personenbezogenen Daten" die rechtliche Annahme von verschiedenen nicht abschließend aufgezählten Identitäten, die einer natürlichen Person zugeordnet werden. Die einzelnen zum Ausdruck kommenden Identitäten sollen im Folgenden als *Teilidentitäten*, die zu einer personalen Identität gehören, bezeichnet werden und können aus dem IKT-Recht herausdifferenziert werden. Dem liegt die Annahme zugrunde, dass in IKT-Systemen verschiedene personale Teilidentitäten entstehen, die einem IKT-rechtlichen Regelungsbereich unterliegen und in diesem beschrieben werden können. Die Gesamtheit der personalen Teilidentitäten bildet die personale Identität und würde sich in ihrem Informations- und Erkenntnisgehalt der natürlichen Person annähern oder dieser entsprechen. Gleichzeitig soll die immanente Differenzierung in der DSGVO zwischen Identität und natürlicher Person dahingehend aufgegriffen werden, dass hinter der personalen Identität ein Indivi-

355 Die Zuordnung als Attribute basieren auf dem Wortlaut der Legaldefinitionen zu Art. 4 Nr. 13 DSGVO „genetische Daten": *Eigenschaften* einer natürlichen Person; Art. 4 Nr. 14 DSGVO „biometrische Daten": *Merkmalen* einer natürlichen Person; Art. 4 Nr. 15 DSGVO „Gesundheitsdaten": *Beziehen*, *Hervorgehen*.

356 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 Nr. 1 DSGVO Rn. 9.

357 Nach EWG 30 gehören zu den Online-Kennungen die IP-Adressen, Cookie-Kennungen, die das Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern und solche, die Spuren hinterlassen und die Profilerstellung ermöglichen.

duum als natürliche Person steht und der Ausdruck der personalen Identität dieser zugerechnet wird.

2. Personale Teilidentität aus Profilen, Art. 4 Nr. 4 DSGVO

Das „Profiling" als automatisierte Verarbeitung personenbezogener Daten besteht darin, bestimmte persönliche Aspekte einer Person zu bewerten, zu analysieren oder vorherzusagen, Art. 4 Nr. 4 DSGVO. Dabei werden als Bewertungsaspekte die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel in Art. 4 Nr. 4 DSGVO genannt. Aus diesen verhaltensbezogenen Bewertungsaspekten, die als personenbezogene Daten eigene profilrelevante Attribute begründen und besondere Kategorien personenbezogener Daten darstellen können, lassen sich neue Identitäten als Teilidentitäten begründen. Durch das Verfolgen („*Tracking*") und die Markierung von Datensätzen können im Laufe der Zeit unbemerkt Profilidentitäten entstehen. Diese im Datenschatten entstehenden *Konstruktionen und Dekontextualisierungen* eines Bildes der personalen Identität basieren auf Kriterien, die aus einer Kohorte begründet wurden. Demnach wird ein Kriterium durch ein erhöhtes Auftreten in einer Kohorte gebildet. Mit diesem Kriterium wird eine Korrelation verbunden, die eine Wahrscheinlichkeitsaussage über das Vorliegen bestimmter Attribute ermöglichen soll. So kann die Teilnahme an einem bestimmten Musikfestival mit der politischen Einstellung korrelieren und zu einer entsprechenden Zuschreibung führen, obwohl die Teilnahme am Musikfestival nicht mit der politischen Einstellung in einem Kausalitätsverhältnis steht.[358] Darin liegt die Lückenhaftigkeit der entstandenen Bilder personaler Identitäten aufgrund von Profilen, die das Erfordernis einer nachgelagerten Korrekturmöglichkeit für den Betroffenen auslöst. Weiter kommen beim Tracking personenbezogener Daten solche Werte zum Einsatz, mit denen Prognosen und Wahrscheinlichkeitsaussagen etwa über die Bonität, wie es im SCHUFA-Urteil[359] entschieden wurde, ermöglicht werden. In diesem Urteil wurde der Zugang zu den verarbeiteten personenbezogenen Daten durch den Be-

358 Vgl. *Lanzing*, Ethics and Information Technology 2016, 9 (12 f.); *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (35); *Wischmeyer*, AöR 143 (2018), 1 (13 f.); ebenso im Zusammenhang mit dem Finden und Vergessen von Bildern im Digitalen, *Dreier*, Bild und Recht, 2019, S. 44.

359 BGHZ 200, 39 – SCHUFA.

troffenen bestätigt, zugleich aber die Auskunft an den Betroffenen über die genaue Funktionsweise der Scoreformel abgelehnt.[360]

Die im SCHUFA-Urteil zum Ausdruck kommende Tendenz der Kommerzialisierung von personenbezogenen Daten zur Erlangung eines Wertes („Score") begründet eine Gefährdungslage für die informationelle Selbstbestimmung und lässt sich mit der *Mosaik*-Theorie[361] veranschaulichen, wonach mit der Zusammenführung punktueller Datenverarbeitungen ein ausdifferenziertes Bild einer Persönlichkeit ermöglicht wird. Indem diese Profilidentitäten meist auf Verbraucherdaten basieren, würden die „*Consumer*" zu „*Prosumern*"[362], da die Verbraucher die Daten „*für*" die verantwortliche Stelle zur Verfügung stellen und damit umfangreiche Profilbildungsmöglichkeiten befördert werden. Demnach sind Konzepte des Selbsttrackings in einem „*Tool*" zur Wahrung der Selbstkontrolle naheliegend und könnten in einem Identitätsverwaltungsmodell zur Gewährleistung der Einflussnahme auf die Profilbildung umgesetzt werden, was dem Selbstdatenschutz dienen würde. Dabei wäre das Zweckbindungsprinzip maßgeblich, da mit ihm der Betroffene den Rahmen der Datenverarbeitung und das Risiko von Profilbildungen unmittelbar erkennen würde. Denn jede Profilbildung außerhalb des Zweckbindungsprinzips würde ein neues Risiko schaffen und bedürfte eines eigenen Rechtfertigungsgrundes. Daneben bedarf es der technischen Sicherstellung, dass die Verarbeitung der personenbezogenen Daten zu dem jeweiligen Zweck getrennt erfolgt und die Daten nicht-verkettbar sind. Mit der Nicht-Verkettbarkeit von Datensätzen werden zugleich die Erkenntnismöglichkeiten durch den Verantwortlichen beschränkt. Insoweit würde ein Identitätsverwaltungsmodell die Nicht-Verkettbarkeit der personenbezogenen Daten und die Kontrollmöglichkeit über die Profile und Bilder personaler Identitäten voraussetzen.

Weiter müsse dem faktischen Rückbezug von Profilidentitäten auf personenbezogene Daten aus der Vergangenheit und gerade dem fehlenden Bezug auf das aktuelle und zukunftsbezogene Identitätsbild begegnet werden.[363] Denn die Profilidentitäten setzen sich aus Attributen zusammen, die in der Vergangenheit liegen. Dabei wird die natürliche Person diesem

360 BGHZ 200, 39 (47) – SCHUFA.
361 2. Teil, A., III.; ebenso das Phänomen des Mosaiks beschreibend, *Reisinger*, Rechtsinformatik, 2016, S. 282.
362 *Lanzing*, Ethics and Information Technology 2016, 9 (12).
363 *Hildebrandt*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 43 (51 f.).

„neuen" Profil ausgesetzt und mit ihm rückgekoppelt, worin eine Beeinflussung zurück zu den vergangenen Attributen und Bildern personaler Identität erfolgen könne.[364] Dahingehend lässt sich parallel zu der Meinungsenklave im online-Kontext eine Identitätsenklave über Profilidentitäten konstatieren, welche einen eigenen Schutzbedarf über die informationelle Selbstbestimmung auslöst. Dabei könnte als Schutzmechanismus einerseits ein Identitätsverwaltungsmodell und andererseits die Begründung von Transparenzanforderungen über die hinter der Profilbildung stehenden Algorithmen in der „*Black Box*"[365] in Frage kommen, wie sie bereits für die automatisierte Einzelentscheidung gemäß Art. 13 Abs. 2 f) DSGVO vorgesehen sind. Denn insgesamt geht es bei einem Schutzmechanismus gegen die Profilbildung um die Einbeziehung von Diskriminierungsverboten gegenüber willkürlichen Zuschreibungen innerhalb des Profilings und damit verbundenen verfälschten Bildern personaler Identitäten. Dies gilt besonders in Anbetracht von bestimmten Merkmalen in einer Kohorte, die als Vergleichsmaßstab für die Bildung einzelner Profilidentitäten eingesetzt werden und zu einer Beeinflussung der Bilder personaler Identitäten nach den Kriterien des mehrheitlichen Verhaltens in einer Kohorte führen, ohne dabei den aus der Menschenwürde erwachsenden Individual- und Minderheitenschutz zu gewähren. Demnach kann in dem Profil ebenfalls der kontextspezifische Ausdruck einer personalen Identität angenommen werden, der jedoch in seiner Eigenschaft als Profil einen eigenständigen Schutzbedarf auslöst und zum Gegenstand der Identitätsverwaltung werden sollte.

3. Personale Teilidentität aus Pseudonymen, Art. 4 Nr. 5 DSGVO

Die Pseudonymisierung nach Art. 4 Nr. 5 DSGVO sieht eine Verarbeitung personenbezogener Daten in der Weise vor, dass der Personenbezug der Daten nicht ohne Hinzuziehung zusätzlicher Informationen möglich ist, weil diese zusätzlichen Informationen gesondert aufbewahrt werden. Erst mit dem Einsatz der Kennung ist die Zuweisung zu den personenbezogenen Daten möglich, wobei die Kennung zur Identifizierbarkeit eingesetzt wird und ebenfalls als personenbezogenes Datum gilt, Art. 4 Nr. 1

364 *Dies.*, in: Rannenberg/Royer/Deuker (Hrsg.), The Future of Identity in the Information Society, 2009, 274 (293 f.).

365 *Hoffmann-Riem*, AöR 142 (2017), 1 (29); *Schallbruch*, Schwacher Staat im Netz, 2018, S. 49 f.

DSGVO. Grundsätzlich sollen durch das Pseudonym die personenbezogenen Daten ersetzt werden und die Zuordnung zwischen Pseudonym und Betroffenen erfolgt über eine Zuordnungsregel, die mit einem Passwort ausgelöst werden kann. Dahingehend war der Wortlaut „ersetzen durch" des § 3 Abs. 6a BDSG-alt eindeutig und im Gegensatz zu dem neuen Wortlaut in der Datenschutzgrundverordnung „in einer Weise (…) betroffenen Person nicht mehr zugeordnet werden können" enger. Denn mit dem neuen Wortlaut aus Art. 4 Nr. 5 DSGVO kann man zu dem Ergebnis kommen, dass zur Pseudonymisierung auch die Verschlüsselung gehört. Gemein ist der Verschlüsselung und Pseudonymisierung, dass sie der Datenminimierung und Datensicherheit dienen, wodurch sie als *Maßnahmen der Risikominimierung* fungieren, Art. 32 Abs. 2 DSGVO.[366] Als Erweiterung der Risikominimierung kommen die „Vermischung der Datensätze" und die „Umverteilung" dieser in Betracht, was zu einem Rauschen mit extrahierten Informationen führen und eine Irrtumswahrscheinlichkeit herbeiführen kann.[367] Diese Methoden sind zwischen Pseudonymisierung und Anonymisierung einzuordnen, weshalb sie für ein Identitätsverwaltungsmodell herangezogen werden sollten. Ebenso kommt zur Risikominimierung die Entfernung von Datensätzen als „Kontrolle von Intransparenz"[368] in Betracht, das sog. „*Information Hiding*".[369]

Mit der Zuordnung eines spezifischen Pseudonyms kann weiter die Zuordnung einer Rolle einhergehen. Als Rolle gilt der Verbund von Handlungsmöglichkeiten und Berechtigungen, die für den Handelnden in einem bestimmten Kontext gelten.[370] Diese kontextbezogene Limitierung kann mit einem spezifischen Schutzniveau in Verbindung gebracht werden, so dass sich mit der Rolle die maßgebliche technische Vorgabe für das Pseudonym graduell bestimmen lässt. Hierin kommt bereits die Ausprägung eines Identitätsverwaltungsmodells zum Vorschein. Denn es bedarf eines Treuhänders, der über die Zuordnungsregel zwischen Kennung und dem pseudonymisierten Datensatz verfügt und den Dienst eines (rollen-

366 *Pfitzmann/Köhntopp*, in: Federrath (Hrsg.), Designing Privacy Enhancing Technologies, 2001, 1 (7 f.); *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 1 Rn. 28.

367 *Buchmann*, DuD 2015, 510 (512 f.).

368 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 96.

369 *Buchmann*, DuD 2015, 510 (511); *Pfitzmann*, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology, 2006, S. 10 Fn. 25.

370 *Pfitzmann*, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology, 2006, S. 23.

spezifischen) Schutzes personenbezogener Daten erbringt. Dies lässt sich am Beschäftigtendatenschutz illustrieren, wonach dem Arbeitnehmer die zusätzlichen Rollen als Betriebsrat oder leitender Angestellter (§§ 5 Abs. 3, 9 ff. BetrVG) zukommen können und diese Rollen temporär im IT-System eingerichtet werden müssen.

Insgesamt fungiert die Identifizierung als ein Anknüpfungspunkt für die Identitätsverwaltung, da mit ihr die Kontrolle über die Passworteingabe ausgeübt wird.[371] Wann die Kennung auch die Funktion als *Identifizierer* für den Zugang zu einem pseudonymisierten Datensatz erfüllt, ist eine Frage des Schutzniveaus und kann graduell abhängig vom Kontext und der Rolle des Betroffenen variieren. Dabei kann die Kennung als *Identifizierer* aus Attributen der personalen Identität bestehen, mit denen der Zugang zu einem informationstechnischen System ermöglicht wird. So können Pseudonyme dauerhaft oder temporär ausgestaltet sein und aufgrund eines hohen Schutzniveaus ein nur einmaliger *Identifizierer* eingesetzt werden, wie es bei *Single Sign-On*-Lösungen vorgenommen wird. Abhängig vom Schutzniveau kann das Passwort für den *Identifizierer* bei der verantwortlichen Stelle oder bei der betroffenen Person hinterlegt werden. In einem derartigen Identitätsverwaltungsmodell ginge es primär um den Datensatz als Gegenstand der Kontrolle für die Identifikation und den Zugang, ohne dass die Erkenntnismöglichkeiten zum Gegenstand der Identitätsverwaltung werden. Somit sind Pseudonyme als Kennungen ebenfalls der Ausdruck einer personalen Identität und können aus Attributen der personalen Identität bestehen.

4. Zwischenergebnis

Die DSGVO regelt ausdrücklich in der Definition zu den personenbezogenen Daten den Schutz der Identität in ihren Ausdrucksformen als physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität. Demnach ist die Anknüpfung an die personenbezogenen Daten für die Bestimmung der personalen Identität notwendig, auch für die Beschreibung des Gegenstandes der Identitätsverwaltung. Weiter kommt als Ausprägung der personalen Identität die Profilidentität nach Art. 4 Nr. 4 DSGVO hinzu, die gerade keine Ausprägung des grundrechtlichen Rechts auf Selbstdarstellung ist, sondern algorithmischen De-

371 *Hammer/Knopp*, DuD 2015, 503 (504).

konstruktionen und Kombinationen von Attributen der personalen Identität unterliegt.

Schließlich sieht die DSGVO die Pseudonymisierung vor, die ebenfalls eine Ausprägung der personalen Identität ist. Danach wird eine Kennung über eine Zuordnungsregel mit einem Betroffenen in Verbindung gebracht. Daraus ergibt sich ein eigenes Identitätsverwaltungskonzept, in dem die personale Identität eine Kennung erhält, mit der ein kontextspezifischer Zugang begründet werden kann. Dabei fungiert die Kennung selbst als ein Bild der personalen Identität. Folglich können die für Dritte sichtbaren Kennungen aus Attributen der personalen Identität bestehen und den Zugang zu besonders schützenswerten und risikobehafteten Datenverarbeitungen von besonderen Kategorien personenbezogener Daten gewähren. Gleichzeitig kann in solch einem Identitätsverwaltungskonzept eine Beschränkung des Gegenstands auf diese Datensätze gesehen werden und Konzepte der Kontrolle durch Intransparenz umfassen. Die Kontrolle durch Intransparenz würde sich zunächst auf die Datensätze beziehen und sich zugleich auf den Informations- und Erkenntnisgehalt über eine personale Identität auswirken können. Denn bei einem Identitätsverwaltungsmodell geht es einerseits um die Schutzebenen und andererseits um die jeweiligen Risiken für den Schutz der personalen Identität und die Erkenntnisse über diese.

II. Kontextuelle personale Identitäten

Aus der Feststellung des Bundesverfassungsgerichts im Volkszählungsurteil, dass es „kein ‚belangloses' Datum" gäbe, geht hervor, dass Daten abhängig von ihrem Verwendungskontext an Bedeutung erlangen und diese Bedeutgunsgehalte variieren können.[372] Demnach ergibt sich aus der informationellen Selbstbestimmung ein kontextspezifisches Schutzbedürfnis, welches sich aus den Phasen der Datenverarbeitung im Datenzyklus ergibt und in unterschiedlicher Intensität ausgeprägt sein kann. Entsprechend sind nach dem Erkenntnismodell die Informationen zu einer personalen Identität perspektivisch einzuordnen, so dass die Erkenntnisgehalte variabel sind. Dieser Phänomenologie lässt sich entnehmen, dass die Informationen und Erkenntnisse über eine personale Identität in einer sozialen,

372 BVerfGE 65, 1 (45).

zeitlichen und räumlichen Beziehung stehen.[373] Entsprechend soll mit dieser Kontextbezogenheit eine systemtheoretische Perspektive einbezogen werden. Denn es kann sich bei der Datenverarbeitung zu einer personalen Identität im Kontext um ein autopoietisches Kommunikationssystem ohne eine Intervention der Umwelt handeln.[374] In diesem System ist die Verstärkung von Informationen möglich und kann dazu führen, dass der Erkenntnisgehalt gegenüber anderen Systemen im Widerspruch steht.[375] Dabei können als Kommunikationssystem in einem IKT-Kontext Datenbanken, Informationssysteme und intelligente wissensbasierte Systeme fungieren, wonach verschiedene kontextbezogene Datensätze in einen neuen Kontext überführt und eingeordnet werden können. Gleichzeitig ist das Kommunikationssystem aus systemtheoretischer Hinsicht in der Unterscheidung zwischen der Wahrheit und dem Irrtum indifferent, aber es unterscheidet zwischen System und Umwelt, so dass das Konzept der Beobachtung von Kommunikationssystemen eine Kontrollierbarkeit ermöglichen kann.[376] Denn die Beobachtung und Beobachtungsinstruktionen können als „unsichtbare Hand" wirken, wie es etwa bei Verfahren und Handlungsanweisungen als *Instruktionen* in einem Unternehmen der Fall sein kann.[377]

Für die Identitätsverwaltung kommt die Beobachtung mit *Instruktionen* in Betracht, die übergeordnet als Metakommunikation in Gestalt eines Verfahrens in den Systemen wirkt. Indem diese systembezogenen *Instruktionen* in einem datenschutzrechtlichen Kontext wirken würden, ist zunächst die Kontextbezogenheit der personalen Identität herauszuarbeiten. Folglich werden die Kontexte innerhalb der Datenschutzgrundverordnung (1.) im Hinblick auf eine kontextübergreifende Datenverarbeitung (2.) und das Konzept einer kontextuellen Integrität (3.) und ihre Auswirkung auf ein Identitätsverwaltungsmodell (4.) nachvollzogen.

373 *Solove*, Harv. L. R. 2013, 1880 (1890); *Bender*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 187 (190); *Albers*, Informationelle Selbstbestimmung, 2005, S. 120.
374 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 9 (10 f.).
375 *Ders.*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 9 (10 f.); *Steinmüller*, Information, Modell, Informationssystem, S. 8.
376 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 9 (15–17).
377 *Hoffmann-Riem*, AöR 142 (2017), 1 (31) Fn. 119.

1. Kontexte in der Datenschutzgrundverordnung

a) Persönliche oder familiäre Tätigkeiten, Art. 2 Abs. 2 c) DSGVO

In der Datenschutzgrundverordnung wird die Datenverarbeitung in dem Kontext der ausschließlich persönlichen oder familiären Tätigkeit nach Art. 2 Abs. 2 c) DSGVO aus dem Anwendungsbereich ausgeschlossen. Die Auslegung, was sich als persönliche oder familiäre Tätigkeit einordnen lässt, hat aufgrund des Ausnahmecharakters der Regelung und dem geringeren Schutzniveau über die informationelle Selbstbestimmung restriktiv zu erfolgen. Für die Einordnung in den privaten und geschäftlichen Kontext der Datenverarbeitung ist die Verkehrsanschauung einzubeziehen, wie es bei der eindeutigen Zuordnung eines in der Familie lebenden Kindermädchens in die datenschutzrechtlichen Kontexte besonders deutlich wird. Denn hinsichtlich des Beschäftigungsverhältnisses ist Art. 88 DSGVO maßgeblich, gleichzeitig übt ein Kindermädchen, das in der Familie lebt, auch private Tätigkeiten aus, was vom datenschutzrechtlichen Anwendungsbereich ausgeschlossen wäre. Sobald eine eindeutig private Tätigkeit ausgeübt wird, kommt der zivilrechtliche Schutz des allgemeinen Persönlichkeitsrechts in Betracht (§ 823 Abs. 1 BGB). Damit wird der gesetzlichen Wertung Rechnung getragen, dass die datenschutzrechtliche Abwehrdimension bei informellen Konfliktlagen im persönlichen oder familiären Bereich ungeeignet ist.[378] Gleichwohl wird durch die technischen Überwachungs- und Kontrollmöglichkeiten der Familienmitglieder eine gleichwertige Konfliktlage angenommen, die einen datenschutzrechtlichen Schutzmechanismus auslösen könne.[379] Die Annahme einer Ausweitung des datenschutzrechtlichen Anwendungsbereichs auf private Kontexte erscheint für die datenschutzrechtliche Risikolage im online-Kontext vorzugswürdig, da die Graubereiche zwischen privaten und sozialen Kontexten gerade in sozialen Medien damit unerheblich wären und beide dem Anwendungsbereich der DSGVO unterliegen würden. Dagegen spricht jedoch, dass im privaten Kontext die Pflichten des Verantwortlichen umzusetzen wären, was in Anbetracht der fehlenden fachspezifischen Kenntnisse des privaten Verantwortlichen kaum realisierbar wäre. Damit können zwar die Gefährdungslagen im privaten Kontext der datenschutzrechtlichen Gefährdungslage entsprechen, jedoch sind die zivilrechtlichen Schutzmechanismen dabei als ausreichend einzuordnen.

---

378 *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 10.
379 *Raabe/Lorenz/Pallas u.a.*, CR 2011, 831 (837).

Insgesamt ist der Ausschlussgrund nach Art. 2 Abs. 2 c) DSGVO eng auszulegen, wie es in der Linquist-Entscheidung[380] des EuGHs deutlich wurde. Darin wurde die Rechtsauffassung, dass private Informationen in einer leicht humorigen Weise auf einer Webseite vom datenschutzrechtlichen Anwendungsbereich auszuschließen sind, als unvereinbar mit der Datenschutzrichtlinie angesehen. Demnach liegt es nahe, in Grenzfällen eine Schwerpunktbetrachtung dahingehend vorzunehmen, wo der Schwerpunkt des Verhaltens liegt und welche Gefährdungen für den Schutz personenbezogener Daten bestehen. Das festgestellte Risiko für den Schutz personenbezogener Daten gibt dabei Anhaltspunkte für den Schutzbedarf und die Zuordnung in den datenschutzrechtlichen Anwendungsbereich.

b) Beschäftigungskontext, Art. 88 DSGVO i.V.m. § 26 BDSG

Weiter kommt der Beschäftigungskontext für gesonderte Regelungen über die Datenverarbeitung in Betracht, Art. 88 DSGVO i.V.m. § 26 BDSG. Von dem Beschäftigtendatenschutz sind die Phasen der Bewerbung, der Einstellung, der Durchführung und die Beendigung des Arbeitsverhältnisses mit ihren jeweiligen Zwecken der Datenverarbeitung erfasst.[381] Ebenso kommen die spezifischen technischen und organisatorischen Maßnahmen des Arbeitgebers, der Verantwortlicher in den Phasen des Arbeitsverhältnisses ist, entsprechend zu den Risikolagen der Datenverarbeitung hinzu und verlangen einen gesonderten Schutz der personenbezogenen Daten. Die im Kontext des Beschäftigtendatenschutzrechts geltende Besonderheit von konkretisierenden Regelungen durch Kollektivvereinbarungen können ein differenziertes Regelungsgefüge zur Verfügung stellen, mit dem die Unterkontexte im Beschäftigungskontext geregelt werden und unter einem angepassten Datensicherheitsniveau die personenbezogenen Daten verarbeitet werden können.[382]

Die für die Begründung des Arbeitsverhältnisses erforderlichen Datensätze, etwa die Krankenversicherungsnummer (§ 291 Abs. 2 SGB V), Steueridentifikationsnummer (§ 139b Abs. 1 AO) und Sozialversicherungsnummer (§ 147 Asb. 2 SGB VI) gehören zu der anfänglichen Phase der Einstel-

380 EuGH, Urt. v. 06.11.2003 – C-101/01, Linquist, Rn. 47.
381 *Maschmann*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 88 DSGVO Rn. 14–16.
382 *Ders.*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 88 DSGVO Rn. 24–27.

lung im Beschäftigtendatenschutz und beziehen jeweils die personale Teilidentität in ihrem *Idem*-Anteil im datenschutzrechtlichen Kontext der Beschäftigung ein. In der weiteren Phase der Durchführung des Beschäftigungsverhältnisses können die Identifizierungs- und Zeiterfassungsdaten zu einer personalen Teilidentität gehören. Ebenso kommen rollenspezifische Teilidentitäten des Beschäftigten in Betracht, die aus Zugangsrechten zu bestimmten Datenbanken und aus gesonderten Befugnissen bestehen können. Die Zugangsrechte in Gestalt von Benutzernamen und Passwörtern würden den *Idem*-Anteil einer personalen Identität darstellen und die verhaltensbezogene Ausübung der Befugnisse den *Ipse*-Anteil der personalen Identität.

2. Kontextübergreifende Datenverarbeitung

Neben den kontextspezifischen Datenverarbeitungen in der DSGVO ist die kontextübergreifende Datenverarbeitung als Gegenstand der Identitätsverwaltung einzubeziehen. Dabei geht es um die Datenverarbeitung in zwei zunächst voneinander unabhängigen Kontexten, die miteinander in Verbindung gebracht werden. Dem oben erwähnten Beispiel des im Haushalt einer Familie lebenden Kindermädchens folgend, geht es um die Überschneidung der Datensätze aus der privaten Tätigkeit mit der Tätigkeit im Beschäftigungskontext und der Kontrolle über die jeweiligen personalen Identitäten. Weiter kann bei einem „*smarten*" Arbeitsplatz der Datensatz aus dem „*Smart Home*" von Interesse sein und dem Beschäftigten die Option eingeräumt werden, die aus der privaten Tätigkeit stammenden Datensätze als *Ipse*-Anteil in den Beschäftigungskontext einzubeziehen. Demnach geht es über die Bestimmung des Kontextes hinaus um die Schnittstellen und Interoperabilität von personalen Identitäten zwischen den Kontexten.

Indem beide Konstellationen unterschiedlichen rechtlichen Schutzregimen unterliegen, zugleich aber der Bedarf an der Zusammenführung der Datensätze bestehen kann, stellt sich die Frage nach einer der informationellen Selbstbestimmung gerecht werdenden kontextübergreifenden Kontrolle der Datensätze. So sieht der EWG 54 S. 4 für den *Ipse*-Anteil der personalen Identität vor, dass verarbeitete Gesundheitsdaten aus einem öffentlichen Interesse heraus nicht zu einem anderen Zweck in einem anderen Kontext verarbeitet werden dürfen. Dies macht eine grundsätzliche Nicht-Verkettbarkeit der Datensätze und personalen Identitäten deutlich.

Ebenso führt die Nutzung von sozialen Medien innerhalb eines privaten und familiären Kreises zunächst zu dem Ausschluss des datenschutzrechtlichen Anwendungsbereiches. Gleichzeitig kann die Abrufbarkeit eines Nutzungsprofils unter sog. „Freunden" über den privaten Bereich hinaus dem Regelungsregime der DSGVO unterliegen, so dass Graubereiche bei der Kontextabgrenzung entstehen können.[383]

In Betracht kommt ein steuerbarer Zugriff auf die jeweiligen Datensätze durch erneute Einwilligungen der natürlichen Person. Indem spezifische Risikolagen mit der kontextspezifischen Datenverarbeitung einhergehen, kann sich das Erfordernis einer erneuten Einwilligung für die kontextübergreifende Datenverarbeitung ergeben. Demnach muss im Rahmen der Informationspflichten auf den spezifischen Zweck der kontextübergreifenden Datenverarbeitung hingewiesen werden, Art. 12–14 DSGVO, EWG 32, 39 S. 5, um eine erneute Rechtfertigung einzuholen, Art. 6, 7 DSGVO. Dabei kommt als Rechtfertigung insbesondere die Einwilligung mit der Voraussetzung einer wissensbasierten Entscheidung in Betracht. Maßgeblich ist dabei die Gewährleistung der informationellen Selbstbestimmung in den Kontexten und bei der kontextübergreifenden Datenverarbeitung, so dass die kontextspezifischen *Ipse*-Anteile der personalen Identität über den Datenzyklus hinweg solange separiert bleiben, bis eine kontrollierte kontextübergreifende Zusammenführung gerechtfertigt wird.

3. Kontextuelle Integrität

Aus der angloamerikanischen Perspektive wird von *Nissenbaum* zum Schutz der Privatheit das Konzept der „*kontextuellen Integrität*" vorgeschlagen.[384] In diesem geht es um die kontextbezogenen „Sphären der Gerechtigkeit", die in dem jeweiligen Kontext der behördlichen, der beruflichen und der privaten Kommunikation zu realisieren seien. Dem liegt die Annahme zugrunde, dass Informationen nicht kontextarm sind, sondern aus dem Kontext entstehen. Entsprechend bedarf es eines Schutzregimes, in dem die Kontexte in den Vordergrund treten. Denn bereits die Bestimmung des Kontextes und seiner Grenzen unterliegt der eingenommenen Betrachtungsperspektive, so dass Kontextüberschneidungen ein einheitli-

383 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 76.
384 *Nissenbaum*, Wash. L. Rev. 2004, 119.

ches Schutzniveau erschweren.[385] Folglich besteht die *kontextuelle Integrität* aus vier Prinzipien, die als integraler Bestandteil gelten: Die Abwehrdimension des Schutzes der Privatsphäre, der eingeschränkte Zugang zu sensiblen und vertraulichen Kontexten, die Kontrolle der Informationen als Autonomie und die Sicherstellung von vertraulichen Informationen.[386]

In diesem Konzept der *kontextuellen Integrität* kommt die Beobachtungsdimension von Kommunikationssystemen zum Ausdruck. Dabei wird zwischen dem feststellbaren Öffentlichkeitsgrad der Informationen mit dem jeweiligen Schutzniveau und dem Zugangsniveau unterschieden.[387] Folglich ist in einem Identitätsverwaltungsmodell unter der Wahrung einer *kontextuellen Integrität* zwischen sensiblen und nicht sensiblen, öffentlichen und privaten Informationen zu unterscheiden. Aufgrund der Überschneidungen von Kontexten ist eine Separierung der Informationen nicht immer möglich, so dass die *kontextuelle Integrität* eine kontextuelle Interoperabilität verlangt. Danach geht es um ein gestuftes Sicherheitsniveau, wie es gemäß Art. 8 Abs. 2 eIDAS-VO nachgewiesen wurde, und die Beschränkung der Datensätze auf ein notwendiges Maß für den jeweiligen Kontext. Diese kontextübergreifende Datenverarbeitung mit einem kontextspezifischen Sicherheits- und Risikoniveau würde einem „*Identity Ecosystem*" entsprechen.[388]

Insgesamt lässt sich diesem Konzept der *kontextuellen Integrität* unterstellen, dass es idealistisch sei und dem *Big Data*-Phänomen mit den einhergehenden Informationsasymmetrien unzureichend Rechnung trage. Gleichwohl geht es bei der *kontextuellen Integrität* darum, dass ein gesteigerter Schutz für die personale (Teil-) Identität in dem jeweiligen Kontext begründet wird, und damit der *Selbstdatenschutz* unter verbesserten Bedingungen ausgeübt werden kann. Demnach kommt für den Schutz der *kontextuellen Integrität* ein mediierendes Verfahren zum Ausgleich der bestehenden Informationsasymmetrien in Betracht, welches von den Erfordernissen der Transparenz, Offenheit, Teilhabe und Mitteilungen[389] geprägt ist.

---

385 *Dies.*, Wash. L. Rev. 2004, 119 (122); *Hoffmann-Riem*, AöR 142 (2017), 1 (26 f.); *Steinmüller*, Information, Modell, Informationssystem, S. 45.
386 *Dies.*, Wash. L. Rev. 2004, 119 (131).
387 *Dies.*, Wash. L. Rev. 2004, 119 (151 f.).
388 *White House*, National Strategy for Trusted Identities in Cyberspace, 2011, S. 29 f.
389 *Nissenbaum*, Wash. L. Rev. 2004, 119 (130) mwN.

4. Übertragung auf das Identitätsverwaltungsmodell

In einem Identitätsverwaltungsmodell bedarf es für die personale Identität und ihren Teilidentitäten eines *kontextspezifischen Schutzregimes*, in dem die Phänomene der Kontexte als separiert und zugleich ineinander übergreifend einbezogen werden. Indem die *(kontextuelle) Integrität* als Bestandteil des Schutzes der Privatheit grundrechtlich anerkannt wurde,[390] soll diese in einem Identitätsverwaltungsmodell einbezogen werden. Dafür kommt ein Treuhandmodell in Frage, wonach die Datensätze zur personalen Identität treuhänderisch hinterlegt werden und kontextspezifisch der Zugang gewährt wird. Dabei würde für einen ineinandergreifenden Kontext die Kombination von mehreren Teilidentitäten erfolgen, wie es bei der Zusammenführung der Teilidentitäten über die Steuernummer, Sozialversicherungsnummer und Krankenversicherungsnummer eines Beschäftigten der Fall wäre.

Mit dieser kontextspezifischen Begründung der personalen Identität aus den Teilidentitäten kann dem Verständnis der statischen *Idem*-Identität begegnet werden, indem die personale Identität in einem Kommunikationssystem der Dynamik des Kontextes und seiner Beobachtung unterliegt. Weiter erlaubt das Konzept der kontextspezifischen Integrität eine iterativ, dem Datenzyklus gerecht werdende Neubildung der personalen Identität in ihrem *Ipse*-Anteil. Diese kann von der natürlichen Person im Rahmen der informationellen Selbstbestimmung ausgestaltet werden. Mit diesem *kontextspezifischen Schutz* der personalen Identität würde eine Entwicklungsoffenheit der personalen Identität im online-Kontext gewährleistet werden.

Entsprechend wurde vom Weißen Haus im Jahr 2011 ein „*Identity Ecosystem*“ auf internationaler Ebene vorgeschlagen, in dem das Sicherheitsniveau der Kontexte für die Kontrolle der Datensätze maßgeblich sei. Danach würden etwa die Bankdaten dem gleichen Sicherheitsniveau wie die Gesundheitsdaten unterliegen. In einem kontextübergreifenden interoperablen System würde der Zugang zu den personalen Identitäten entsprechend dem Sicherheitsniveau geregelt werden, wie es in Art. 8 Abs. 2 eIDAS-VO vorgesehen ist.[391]

Diesen Identitätsverwaltungsmodellen ist gemein, dass über die Einwilligung eine *iterative Kontrolle* der Zugangsgewährung ermöglicht wird. Gleichzeitig liegt darin eine Schutzmöglichkeit im Rahmen des *Selbstda-*

390 2. Teil, A., II., 1., b) – c).

391 *White House*, National Strategy for Trusted Identities in Cyberspace, 2011, S. 17 f., 31–35.

tenschutzes, die gegenüber *Big Data*-Phänomenen und den damit einhergehenden Informationsasymmetrien wirken könnte und ein kompensatorisches Verfahren darstellen könnte. Dafür kommt ein mediierendes Verfahren zum Ausgleich der bestehenden Informationsasymmetrien in Betracht, welches von den Erfordernissen der Transparenz, Offenheit, Teilhabe und Mitteilungen[392] geprägt ist.

5. Zwischenergebnis

Die Datenschutzgrundverordnung regelt ausdrücklich die Kontexte der persönlichen und familiären Tätigkeit und der Beschäftigung. Der kontextspezifische Schutz personaler Identitäten verlangt demnach eine *kontextuelle Integrität,* die als Bestandteil der informationellen Selbstbestimmung fungiert. Diese lässt sich mit dem gestuften Vertrauens- und Sicherheitsniveau gemäß Art. 8 Abs. 2 eIDAS-VO abbilden. Für das Identitätsverwaltungsmodell ist folglich ein „*Identity Ecosystem*" aufschlussreich, wonach der Zugang zu dem jeweiligen Sicherheits- und Risikoniveau gewährleistet wird. Damit könnte der *Selbstdatenschutz* wirksam ausgeübt werden und die kontextspezifische iterative Kontrolle der Informationen und Erkenntnisse über personale Identitäten ermöglicht werden. Dies könnte mit einem mediierenden Verfahren erfolgen, das von Teilhabe und Transparenz geprägt ist.

III. Stipulatives Identitätsverwaltungsmodell

Der Identitätsbegriff beschreibt zunächst den Zustand der Gleichheit und könnte demnach auch als undefinierbar gelten. Mit der Beziehung des Begriffs zur Person als personale Identität erlangt der Identitätsbegriff über den Vorgang des Vergleichens hinaus einen inhaltlichen Gehalt, der zum Gegenstand einer stipulativen Definition werden soll. Dennoch verbleibt die Frage nach der definitorischen Ebene, da die personale Identität auf einer niedrigen Stufe ihre individuelle Subjektivität mit den jeweiligen Attributen zum Definitionsgegenstand haben müsste.

Die definitorische Macht für den offline-Kontext ist in den grundrechtlichen und einfachrechtlichen Regelungen verwurzelt, so dass die darin enthaltene reale Essenz in stipulative Definitionen[393] für den online-Kontext

392 *Nissenbaum*, Wash. L. Rev. 2004, 119 (130) mwN.
393 *Pap*, Philosophy of science 1964, 49 (51 f.).

überführt werden soll. Dabei kommen für die Definition der personalen Identität solche Kriterien aus dem offline-Kontext in Betracht, bei denen die Physis, die Sozialisation und die Charakteristik der Person den Anknüpfungspunkt bilden können.[394] Demgegenüber stehen Anknüpfungen an die Attribute einer personalen Identität wie etwa die Email-Adresse bei *Single Sign-On*-Lösungen oder die digitale Identität beim elektronischen Personalausweis, die den Begriff der personalen Identität prägen können.[395]

Insgesamt soll der Begriff der personalen Identität aus den beschriebenen grundrechtlichen und einfachrechtlichen Ausprägungen heraus definiert und damit ein Abstraktionsniveau gewährleistet werden, dass dem offline- und online-Kontext gleichermaßen Rechnung trägt. Zudem sollen die Definitionen dem pluralistischen Verständnis von Individuen gerecht werden und demnach gegenüber verschiedenen Attributen offen sein. Dabei stehen die Definitionen in dem Verhältnis zueinander, wie es in dem Modell zwischen offline- und online-Kontext dargestellt ist (Abbildung 3).

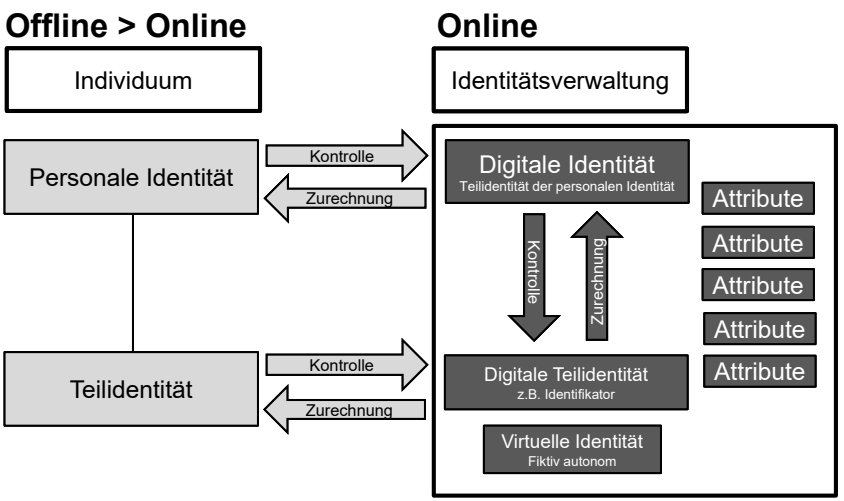

Abbildung 3: System der Definitionen zur personalen Identität

394 *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 1.

395 *Froomkin*, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, S. 6.

1. Definitionen zur personalen Identität

- Die *personale Identität* einer natürlichen Person realisiert sich über die Selbstdarstellung und Darstellung von dynamischen (*Ipse*) und statischen *personalen Teilidentitäten* (*Idem*) als Ausdruck der inneren Selbstbestimmung und Selbstbewahrung innerhalb von IKT-Systemen durch Informationen in interpretierbaren Symbolstrukturen, aus denen Wissen generiert wird.
- Die *personale Teilidentität* einer natürlichen Person ist der personalen Identität zurechenbar und realisiert sich statisch (*Idem*) oder dynamisch (*Ipse*) innerhalb von IKT-Systemen durch kontextspezifische Informationen in interpretierbaren Symbolstrukturen, aus denen Kontextwissen generiert und aus dem Verhalten sichtbar wird.
- Die *digitale Identität* ist einer natürlichen Person über einen Identifikator zurechenbar und realisiert sich innerhalb eines IKT-Systems über ein Zuordnungsobjekt, das aus Teilidentitäten besteht.
- Die *digitale Teilidentität* einer natürlichen Person ist über einen Identifikator zurechenbar und realisiert sich innerhalb eines IKT-Systems über ein Zuordnungsobjekt, das aus Attributen als Datensätze besteht, die zu Informationen und Kontextwissen werden, sowie aus möglichen Zuschreibungen durch Dritte.
- Die *virtuelle (Teil)-Identität* wird durch eine natürliche Person oder künstliche Intelligenz als ein Zuordnungsobjekt in einem IKT-System begründet, ohne dass ein reales Äquivalent mit einem hohen Gleichwertigkeitsgehalt existiert.

2. Definitionen zur Identitätsverwaltung

- Die *Identitätsverwaltung* in einem IKT-System ist die Kontrolle einer natürlichen Person über die Begründung und Annahme von personalen Teilidentitäten, bestehend aus kontextbezogenen Daten, Informationen und generiertem Wissen, sowie die Kontrolle über die Verkettbarkeit von kontextübergreifenden Teilidentitäten.
- Ein *Agent* handelt dauerhaft oder vorübergehend für eine personale Identität durch die Übermittlung von Daten (Bote), durch Tätigwerden für einen Prinzipal (Erfüllungsgehilfe, Verrichtungsgehilfe, Stellvertretung) oder durch autonomes Auftreten mit einer anderen Bezeichnung (Legende).

- *Attribute* sind einer TeiIidentität zugeordnete und zurechenbare Eigenschaften.
- *Kontrolle* ist das bewusste Einwirken, Beaufsichtigen, Steuern und Gestalten.
- *Zurechenbarkeit* bezüglich eines Akteurs ist gegeben, wenn Vorgänge den Beteiligten Instanzen gegenüber dem Akteur zugeordnet werden können.[396]
- *Identifikator* ist ein Datensatz, mit dem eine eindeutige Identifizierung der natürlichen Person möglich ist.

B. Ex ante Rechtfertigung personaler Identitäten in der DSGVO

Der Zeitraum vor der Rechtfertigung einer Datenverarbeitung über die personale Identität unterliegt den Grundsätzen gemäß Art. 5 Abs. 1 DSGVO und verlangt entsprechende Maßnahmen durch den Verantwortlichen. Demnach soll für die Begründung des Identitätsverwaltungsmodells die Betrachtung chronologisch mit der Bestimmung der personenbezogenen Daten beginnen (I.) und mit den Anforderungen an die Transparenz fortgesetzt werden (II.). Anschließend sollen die Voraussetzungen, die der Verantwortliche gemäß Art. 5 Abs. 1 DSGVO zu erfüllen hat, konkretisiert werden (III.). Dafür sollen die Verpflichtungen hinsichtlich der Zweckbindung, der Datenminimierung, der Datensicherheit und der datenschutzkonformen Technikgestaltung ausgeführt werden. Daraus sollen die Anhaltspunkte für ein Identitätsverwaltungsmodell abgeleitet und zugleich die rechtlichen Anforderungen an die Identitätsverwaltung konkretisiert werden.

I. Bestimmung personenbezogener Daten

Die Identitätsverwaltung umfasst personenbezogene Daten als Bestandteile der personalen Identität und verlangt die Bestimmung dieser zur Eröffnung des datenschutzrechtlichen Anwendungsbereiches. Entscheidend für die Eingrenzung des Gegenstandes der Identitätsverwaltung ist daher die trennscharfe Differenzierung zwischen anonymen und personenbezogenen Daten. Indem anonyme Daten bei einer Kontextänderung zu personenbezogenen Daten werden können, stellt sich die Frage nach der Einbe-

396 *KASTEL-Kompetenzzentrum*, Begriffsdefinitionen in KASTEL S. 5.

ziehung dieser Sachlage in das Identitätsverwaltungsmodell. Aus der Perspektive der natürlichen Person, die ihre personalen Identitäten verwaltet, ist gemäß dem EWG 39 S. 5 eine Risikobetrachtung naheliegend, nach der die betroffene Person über die Risiken der Verarbeitung personenbezogener Daten informiert und aufgeklärt werden soll. Damit soll die betroffene Person von ihrem Entscheidungsspielraum über die Erteilung einer Einwilligung wirksam Gebrauch machen können. Weil bei anonymen Daten in einem Datenzyklus das Risiko der Identifizierbarkeit einer natürlichen Person (1.) besteht, wird gerade im *Big Data*-Zusammenhang der Bedarf nach einem Schutz vor der Identifizierung einer natürlichen Person deutlich. Weiter geht aus der DSGVO neben dem Schutz personenbezogener Daten der Schutz vor erlernbaren Erkenntnissen über personale Identitäten hervor, so dass die Informationen und das Wissen über eine personale Identität entsprechend zum Erkenntnismodell von der DSGVO geschützt werden. Folglich soll das Risiko der Erkenntnisse aus personenbezogenen Daten dargestellt werden (2.).

1. Risiko der Identifizierbarkeit

Das Risiko der Identifizierbarkeit einer natürlichen Person richtet sich nach den rechtlichen Bestimmungen, wann ein personenbezogenes Datum gegeben ist. Denn der datenschutzrechtliche Vorfeldschutz gebietet bei der Bewertung des Risikos der Identifizierbarkeit die Einbeziehung der kontextspezifischen Gefährdungslage,[397] was eine flexible Zuordnung zwischen anonymen und personenbezogenen Daten mit dem unbestimmten Rechtsbegriff der „Identifizierbarkeit" ermöglicht. Gemäß der Legaldefinition nach Art. 4 Nr. 1 DSGVO und dem EWG 26 S. 3–4 liegt die Identifizierbarkeit vor, wenn mit den Mitteln des Verantwortlichen die Person identifiziert werden kann, und wenn unter Einbeziehung von Informationen Dritter mit angemessenem Aufwand die Identifizierung ermöglicht wird.[398] Damit können anonymisierte Daten aus dem „digitalen Schattendasein" mit den Informationen des Verantwortlichen und des Dritten an das Licht der Identifizierbarkeit geführt werden, womit sie dem Anwendungsbereich der DSGVO unterliegen.

397 *Kühling/Klar*, NJW 2013, 3611 (3613).

398 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 Nr. 1 DSGVO Rn. 19.

In der Entscheidung *Breyer*[399] hat der EuGH dynamische IP-Adressen aufgrund ihrer dauerhaften Verfügbarkeit im Netz und die Möglichkeit der indirekten Identifizierbarkeit als personenbezogene Daten eingeordnet. Folglich wird aus der Entscheidung des EuGHs ein gemischt objektiv-relativer Ansatz angenommen,[400] wonach neben der subjektiven Perspektive des Verantwortlichen auch die objektive Perspektive für die Frage der Identifizierbarkeit maßgeblich ist. Dieser objektiv- relative Ansatz verlangt bei der Prüfung der Identifizierbarkeit die Einbeziehung der Abwägungskriterien, welche Kosten und welcher Zeitaufwand unter Einsatz der verfügbaren Technologie erforderlich sind. Dies entspricht den Wertungen aus dem EWG 26 S. 4, so dass sich die Entscheidung *Breyer* auf die DSGVO übertragen lässt, auch wenn die Entscheidung des EuGHs noch an die Rechtslage der Datenschutzrichtlinie 95/45/EG anknüpft. Für den Theorienstreit über die Identifizierbarkeit ist daher maßgeblich, wer über das Zusatzwissen zur Identifizierung verfügt, so dass es auf die Kenntnis des Verantwortlichen und eines *realistischen Dritten* ankommt. Nach dem relativen Ansatz[401] geht es um das Zusatzwissen des Verantwortlichen und nach dem objektiven Ansatz um das abstrakte Zusatzwissen eines Dritten.[402] Sobald sich mit einem Merkmal, einer Merkmalskombination oder dem Kontextwissen als Zusatzwissen auf eine natürliche Person rückschließen lässt, liegt ein identifizierendes Merkmal vor. Dieses Zusatzwissen kann aus Attributen oder Anmeldedaten bestehen und in seiner Verlässlichkeit über die Authentizität einem eigenen Risikogehalt unterliegen.

Weiter lässt sich dieses Zusatzwissen aufteilen in extrinsisch, außerhalb der natürlichen Person liegend, und intrinsisch, in der natürlichen Person liegend.[403] Darin lässt sich eine entscheidende Differenzierung erblicken, um das Zusatzwissen und das Verhalten des Betroffenen mit einem eigenen Anteil zu versehen, welches sich auf das Risiko der Identifizierbarkeit auswirkt. Damit hängt das Risiko der Identifizierbarkeit von dem Maß des potentiell einbeziehbaren Zusatzwissens ab, welches ein Verantwortlicher oder ein Dritter möglicherweise von dem Betroffenen erlangt. Folglich können viele verschiedene Attribute in sozialen Medien zu einem Namen

399 EuGH, Urt. v. 19.10.2016 – C-582/14, Breyer ./. BRD, Rn. 31, 36, 40.

400 *Karg*, DuD 2015, 520 (525), „objektiviert, relativer Ansatz"; *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 11, relativer Ansatz mit risikobasierten objektiven Elementen.

401 Vertreten von *Eckhardt*, CR 2016, 786 (790).

402 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 Nr. 1 DSGVO Rn. 23.

403 *Janeček*, CLSR 2018, 1039 (1044).

existieren, der als Pseudonym erscheint, aber durch die Anzahl der Attribute wird dennoch die Identifizierung der natürlichen Person möglich. Demnach erlaubt die Differenzierung zwischen extrinsischem und intrinsischem Zusatzwissen eine Aussage darüber, ob eine natürliche Person selbst zu einem gesteigerten Identifizierungsrisiko beigetragen hat.

Nach dem EuGH kann auch das Zusatzwissen eines Dritten einbezogen werden, wenn es dem Verantwortlichen zurechenbar ist und es sich um einen verhältnismäßigen Aufwand handelt, mit dem die natürliche Person identifiziert werden kann. Hinzu kommt die Frage, ob ein verhältnismäßiger und unverhältnismäßiger Aufwand anzunehmen ist, wenn ein rechtmäßiges Akteneinsichtsrecht besteht oder ob dieses ebenfalls einen unverhältnismäßigen Aufwand mit sich bringen würde.[404] Entscheidend bei der Bewertung ist, dass das einbezogene Zusatzwissen nach herrschender Meinung auf rechtmäßigem Weg[405] erlangt werden muss, da dies auch im Einklang mit dem Wortlaut des EWG 47 S. 1 „vernünftige Erwartung" steht. Dagegen lässt sich jedoch kritisch anführen, dass bei der Erlangung besonders sensibler Daten auf rechtswidrigem Weg die Schutzmechanismen der DSGVO ausgeschlossen wären und der Betroffene bei einem besonders weitreichenden Eingriff in die informationelle Selbstbestimmung schutzlos wäre. Dies wirkt sich in Anbetracht von *Big Data*-Phänomenen, die einen erleichterten Zugang zu Zusatzwissen auf rechtmäßigem und unrechtmäßigem Wege ermöglichen, als ein unbefriedigendes Ergebnis aus.[406] Daher muss im Ergebnis jede Identifizierung zu einem Schutz der personenbezogenen Daten und damit der personalen Identität führen, was mit der Identitätsverwaltung erleichtert erfolgen kann.

Aus den Verknüpfungsmöglichkeiten zwischen mehreren Daten- und Informationsbeständen geht das Risiko über die Beeinträchtigung des Schutzes der informationellen Selbstbestimmung hervor, welches für den Betroffenen und Verantwortlichen den Bedarf nach einer risikobasierten Prognoseentscheidung auslöst.[407] Demnach besteht das Risiko, dass anonymisierte Daten in einem Datenzyklus zu personenbezogenen Daten werden, wobei der Übergang von anonymen Daten zu personenbezogenen

404 Schlussanträge des Generalanwalts Manuel Campos Sanchez-Bordona, EuGH, C-582/14, 12. Mai 2016, Breyer ./. BRD, Rn. 61; *Kring/Marosi*, K&R 2016, 773 (774).

405 EuGH, Urt. v. 19.10.2016 – C-582/14, Breyer ./. BRD, Rn. 47.

406 *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 DSGVO Rn. 29; *Bergt*, ZD 2015, 365 (370).

407 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 12.

Daten in einer rechtlichen Grauzone[408] stattfinde, bei der für einen bestimmten Zeitabschnitt eine eindeutige Zuordnung erschwert ist. Um der Phänomenologie eines kontextspezifischen Wechsels von anonymen zu personenbezogenen Daten in einem Datenzyklus gerecht zu werden, könnte die zweischrittige Prüfung aus der Entscheidung des englischen „*Court of Appeal*" in *Vidal-Hall v Google*[409] einbezogen werden. Danach erfolgt erst eine kontextunabhängige Einordnung der Daten, und anschließend wird der Kontext in seinen Ausprägungen mit dem Risiko der Identifizierbarkeit einbezogen. Zwar begründet diese Prüfungsfolge eine gewisse Eindeutigkeit bei der Bestimmung der Daten und des Kontextes, jedoch bleibt die Ungewissheit über die Begrenzung des Kontextes und seiner Bedingungen, so dass mit der zweischrittigen Prüfung nicht zwingend eine gesteigerte Rechtssicherheit einhergeht.

Insgesamt wird aufgrund der exponentiell steigenden Datenverarbeitungen und der zügigen Identifizierungsmöglichkeit als *Big Data*-Phänomen angenommen, dass der Theorienstreit über die Identifizierbarkeit dahinstehen könne.[410] Gleichwohl erscheint für die Identitätsverwaltung ein objektiviert-relativer Ansatz naheliegend, wonach es für die Feststellung der Identifizierbarkeit auf das Zusatzwissen des Verantwortlichen und Dritten ankommt. Dabei sind das Risiko von Zusatzwissen eines Dritten und die Frage nach dem verhältnismäßigen Aufwand, dass dieses Zusatzwissen einbezogen wird, maßgeblich. Für die Identitätsverwaltung ist damit entscheidend, wann ein Datensatz in einem Datenzyklus als personenbezogen gilt und damit zum Gegenstand des Identitätsverwaltungsmodells werden muss. Ebenso lässt sich das Bewusstsein über das Bestehen von rechtlichen und technischen Grauzonen zwischen anonymen und personenbezogenen Daten als ein Risiko für den Schutz der Rechte und Freiheiten natürlicher Personen in das Identitätsverwaltungsmodell einbeziehen, indem darauf etwa ausdrücklich im Rahmen der Informationspflichten hingewiesen wird.

408 *Janeček*, CLSR 2018, 1039 (1043).
409 Vidal-Hall v Google [2015] EWCA 311, para. 111 ff.
410 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 73; *Reinhardt*, AöR 142 (2017), 528 (532).

2. Risiko der Erkenntnisse aus personenbezogenen Daten

Das Risiko der Erkenntnisse aus personenbezogenen Daten folgt aus der Verarbeitung personenbezogener Daten im Datenzyklus und der Einbeziehung von Zusatzwissen des Verantwortlichen und Dritten. Da personenbezogene Daten aus einer Kennung, Standortdaten oder einem Identifizierungsmerkmal und zudem aus Merkmalen als Ausdruck der personalen Identität gemäß Art. 4 Nr. 1 DSGVO bestehen können, schützt die DSGVO neben den personenbezogenen Daten auch die Informationen über natürliche Personen. Demnach ist der Informationsgehalt aus den Daten ausdrücklich als Schutzgegenstand benannt, wie es sich aus den Legaldefinitionen des Profiling (Art. 4 Nr. 4 DSGVO), der biometrischen Daten (Art. 4 Nr. 14 DSGVO) und der Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) ergibt. Dabei handelt es sich um Informationen aus den Daten und der Möglichkeit des Erlernens von Wissen über die personale Identität. Vom Schutz besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sind folglich auch solche Daten erfasst, aus denen mittelbare Rückschlüsse oder indirekte Hinweise auf sensible Daten möglich sind.[411] Denn aus den Nutzungsdaten bei dem Einsatz des Internets der Dinge etwa in einem „*Smart Home*" können Daten generiert werden, die zunächst Erkenntnisse über das Nutzungsverhalten geben, aber zugleich aus „unbewusst erzeugten Daten"[412] als Metadaten mittelbare Rückschlüsse über die personale Identität einer natürlichen Person erlauben.

Folglich besteht mit der Verarbeitung personenbezogener Daten das Risiko, dass aus einem anfänglich im Datenzyklus unbekannten Erkenntnisgehalt zu einem späteren Zeitpunkt im Datenzyklus ein besonders sensibler Erkenntnisgehalt erwächst, der dem Schutzniveau gemäß Art. 9 DSGVO unterliegt. Dieses gesteigerte Risiko einbeziehend, schlägt *Hoffmann-Riem* die Erweiterung des begrifflichen Schutzes auf Eigenschaften vor, die sich aus einem personenbezogenen Datensatz erlernen lassen.[413] Denn innerhalb eines Datenzyklus kann das „Nochnichtwissen, Nochnichtwissenkönnen, Nichtwissenkönnen"[414] in Erkenntnisse münden, die ursprünglich unvorhersehbar waren. Folglich bedarf es *Instruktio-*

411 *Weichert*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 9 DSGVO Rn. 37.
412 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 224; *Hildebrandt*, Smart technologies and the end(s) of law, 2015, S. 67–69.
413 *Hoffmann-Riem*, AöR 142 (2017), 1 (38 f.)
414 *Ders.*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (28).

nen über den Wissenserwerb und die Kanalisierung dessen, welches etwa über die Befristung und Sperrung von Datensätzen erfolgt. Für die Befristung der Speicherung spricht, dass das Risiko der Erkenntnismöglichkeit über einen Datenzyklus hinweg gemindert wird. Gleichwohl könnten auch kurzfristig generierte Erkenntnisse in die informationelle Selbstbestimmung eingreifen oder über eine redundante Speicherung perpetuiert werden, so dass die befristete Speicherung nicht zwingend zu einer Schutzsteigerung führt. Demnach erscheint für die wirksame Identitätsverwaltung der Bedarf nach Informationen über das Risiko der Erkenntnismöglichkeiten aus dem Datenverarbeitungsvorgang wünschenswert. Dazu gehört neben der Transparenz des Risikos die Einräumung der Kontrolle über die Chancen und Risiken von Erkenntnissen im Laufe des Datenzyklus.

3. Ergebnis

Die Bestimmung der personenbezogenen Daten ist für die Abgrenzung des Gegenstandes der Identitätsverwaltung und den Anwendungsbereich der DSGVO maßgeblich. Der Vorgang der Identifizierbarkeit ist allerdings mit rechtlichen und tatsächlichen Risiken verbunden, die sich auf das erlangte Zusatzwissen, die Qualität des Zusatzwissens und den möglichen Erkenntnisgehalt beziehen. Die Prüfung der Identifizierbarkeit ist ein wertender Vorgang, so dass für ein Identitätsverwaltungsmodell die natürliche Person über die rechtlichen und technischen Grauzonen zwischen anonymen und personenbezogenen Daten in Kenntnis gesetzt werden sollte. Weiter lassen sich bei der Verarbeitung personenbezogener Daten innerhalb eines Datenzyklus mittelbar Erkenntnisse ableiten, die zu einem Risiko für die informationelle Selbstbestimmung führen können.

Insgesamt wird in der DSGVO ein Paradigmenwechsel weg von dem Fokus auf die personenbezogenen Daten hin zu den Schutzzielen angenommen, was zu einer Verschiebung der Schutzmechanismen auf der Ebene der Grundsätze der Datenverarbeitung gemäß Art. 5 DSGVO und dem Risiko der Datenverarbeitung gemäß Art. 32 DSGVO führe.[415] Dies erscheint in Anbetracht der hohen Wahrscheinlichkeit einer Identifizierbarkeit im Laufe des Datenzyklus als *Big Data*-Phänomen naheliegend, zumal bei einem Fokus auf die Grundsätze der Datenverarbeitung für die kon-

415 *Veil*, ZD 2015, 347 (348 f.); *Quelle*, European Journal of Risk Regulation 2018, 502 (504).

textspezifische Risikolage geeignete Kompensationsmechanismen gemäß Art. 5 Abs. 1 DSGVO geschaffen werden können und sich so das Risiko von Erkenntnissen mindern lässt.

II. Transparenz zur Identitätsverwaltung, Art. 5 Abs. 1 a) DSGVO

Die Transparenz ist die tragende Voraussetzung für die Identitätsverwaltung. Denn die Transparenz ermöglicht eine bewusste Entscheidung des Betroffenen über die Einwilligung und eine Risikoabwägung, ob die mit einer Datenverarbeitung verbundenen Risiken von dem Betroffenen eingegangen werden sollen. Dies setzt voraus, dass die transparenten Angaben über das Risiko der Datenverarbeitung den Betroffenen zu einer risikobewussten Entscheidung befähigen. Folglich ist für die Transparenz zur Identitätsverwaltung maßgeblich, dass vorher eine Risikobewertung über die Datenverarbeitung durch den Verantwortlichen vorgenommen wurde und die Risikoinformationen anschließend dem Betroffenen in einer verständlichen Form mitgeteilt wurden. Erst mit diesen Informationen kann der Betroffene eine risikobewusste Entscheidung über die Einwilligungserteilung vornehmen.

Weiter muss der Betroffene über die konkreten Umstände der Verarbeitung personenbezogener Daten informiert werden, um auf die Teilidentitäten und Attribute der personalen Identität kontrollierend einwirken zu können. Darin spiegelt sich die informationelle Selbstbestimmung wider. Die Selbstbestimmung kann nur mit Kenntnis über die konkreten Datenverarbeitungen ausgeübt werden. Nur durch diese Kenntnis wird dem Betroffenen dazu verholfen, von seiner Selbstbestimmung risikobewusst Gebrauch zu machen.

Damit sind die Informationen über das Risiko der Datenverarbeitung im Datenzyklus zu Beginn der Identitätsverwaltung erforderlich und können sich auf die rechtfertigende Einwilligung und die Nutzung des Dienstes auswirken. Demnach sollen die Informationen über die Datenverarbeitung als Entscheidungsgrundlage des Betroffenen (1.) und die Informationen über das Risiko (2.) dargestellt werden. Anschließend soll der Frage nachgegangen werden, ob sich mit der Transparenz die Kontrolle über die Teilidentitäten ausüben lässt (3.), um dann eine Bewertung der Transparenz für die Identitätsverwaltung (4.) vornehmen zu können.

1. Informationen als Entscheidungsgrundlage

Die Transparenzpflichten nach Art. 5 Abs. 1 a), Art. 12–14 DSGVO sehen die Informationsgrundlage für die Entscheidungsprozesse durch den Betroffenen vor. Die Informationsgrundlage stellt sich aus der Perspektive des Betroffenen und somit zu Beginn des Datenzyklus dar. Danach sind solche Informationspflichten erfasst, mit denen der Betroffene Kenntnis über die Umstände und Risiken der Datenverarbeitung als Grundlage für eine rationale Entscheidung erlangen kann. Dazu gehören die Kontaktdaten der verantwortlichen Stelle, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke der Datenverarbeitung, ein möglicher Empfänger dieser Daten, die Dauer der Speicherung, die bestehenden Rechte des Betroffenen, die Grundlage der Datenverarbeitung, die technische Möglichkeit der Profilbildung und ihre potentiellen Auswirkungen sowie das Risiko der gesamten Datenverarbeitung, Art. 13 Abs. 1, 2 c) DSGVO, EWG 39 S. 5. Damit soll der Betroffene zur Antizipation der Risiken über die Datenverarbeitung und möglichen Profilerstellungen befähigt werden. Bei der Informationsmitteilung besteht jedoch ein Spannungsverhältnis zwischen einerseits detaillierten Informationen für den Betroffenen zur wirksamen Ausübung der Rechte und andererseits dem Bedarf, den Betroffenen vor einer Informationsflut zu bewahren. Maßgeblich ist jeweils, dass die Informationen gut lesbar sind und leicht verständlich etwa mit Piktogrammen versehen werden. Auch können die Informationspflichten in einem maschinenlesbaren Format zur Verfügung gestellt werden, Art. 12 Abs. 7 DSGVO. Dies ermöglicht ein ausgewogenes Verhältnis zwischen einerseits rechtskonformer Informationsmitteilung über die Datenverarbeitung und andererseits einer gut verständlichen Darstellung der Informationspflichten.

Gleichwohl richtet sich die Effektivität der Informationen in einer Datenschutzerklärung danach, ob die Datenschutzerklärung gelesen wird und zur Entscheidungsfindung beiträgt. Ebenso wird bei Betroffenen ein Transparenzirrtum dahingehend angenommen, dass bei komplexen Datenverarbeitungsvorgängen gerade keine umfangreiche Kenntnis über die tatsächliche Datenverarbeitung bestehen könne.[416] Dazu gehört besonders der gesonderte Informationsbedarf bei der kontextübergreifenden Datenverarbeitung im Rahmen eines Zweckes, Art. 5 Abs. 1 b) DSGVO. Entsprechend wird ein Recht auf Begründung zugunsten der betroffenen Person abgeleitet, welches dem Recht auf Informationen über die involvierte Lo-

416 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (23).

gik beim Einsatz algorithmusbasierter Einzelentscheidungen in einer Blackbox entspricht, Art. 13 Abs. 2 f) DSGVO.[417] Ein Recht auf Begründung der Einzelheiten über die Datenverarbeitung könnte dem Phänomen der betroffenen Person als „Sklaven des Algorithmus"[418] entgegenwirken und mögliche diskriminierende Wirkungen von Algorithmen aufdecken. Dieses Konzept greift zwar das Phänomen der fehlenden Kenntnis über die Folgen der Datenverarbeitung als Transparenzirrtum auf, führt jedoch nicht zu einem neuen Schutzmechanismus. Denn die Informationspflichten aus Art. 13 Abs. 2 DSGVO umfassen die Besonderheiten der jeweiligen Datenverarbeitung, so dass ein eigenes Recht auf Begründung nicht erforderlich ist. Gleichzeitig kommt in einem selbständigen Recht auf Begründung die Verantwortungsverteilung zum Ausdruck, die dem Verantwortlichen eine Begründungslast auferlegt.

Indem die Informationen für den Betroffenen als Grundlage der Entscheidungsfindung fungieren, wird die Verantwortung durch die Informationspflichten auf den Betroffenen übertragen, und mit einem Recht auf Begründung wird eine erweiterte Kenntnis über die Datenverarbeitung und damit eine weitere effektive Kontrollmöglichkeit eingeräumt.[419] Sobald die Datenschutzerklärung gelesen und auf ihrer Grundlage die Einwilligung erteilt wird, findet eine Verantwortungsverschiebung mit der Einräumung einer Kontrollmöglichkeit zum Betroffenen statt. Denn diese löst mit der Informationsgrundlage im Rahmen der informationellen Selbstbestimmung den nächsten Schritt im Datenzyklus aus, so dass die Transparenz in Gestalt eines *„notice and choice"*[420] auch als Grundlage der Kontrolle in einem Identitätsverwaltungsmodell fungieren kann.

2. Informationen über das Risiko

Der risikobasierte Ansatz gemäß Art. 32 DSGVO ist Bestandteil der Datenschutz-Folgenabschätzung, die allein bei einem hohen Risiko erforderlich ist. Gleichzeitig ist der risikobasierte Ansatz bereits in der Datenschutz-

417 Wahrnehmungsgegenstand bei der Blackbox können allein die Input- und Outputwerte sein, *Reisinger*, Rechtsinformatik, 2016, S. 64; *Hornung/Engemann* (Hrsg.), Der digitale Bürger und seine Identität, 2016, S. 18.

418 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18.

419 *Dies.*, Duke L. & Tech. Rev. 2017, 18 (41 f.); *Wischmeyer*, AöR 143 (2018), 1 (48–54).

420 *Solove*, Harv. L. R. 2013, 1880 (1883 f.).

richtlinie 45/95 verwurzelt[421] und kann als grundlegender Ansatz bei der Rechtfertigung eines Datenverarbeitungsvorgangs angesehen werden. Denn in jeder Datenverarbeitung innerhalb eines Datenzyklus der personalen Identität sei ein immanentes Grundrisiko gegenüber dem Schutzgut der Rechte und Freiheiten natürlicher Personen vorhanden (Art. 35 Abs. 1 S. 1 DSGVO), welches sich auf die Wahl des Rechtfertigungsgrundes auswirkt. Demnach verlangt die Entscheidung über den geeigneten Rechtfertigungsgrund durch den Verantwortlichen eine immanente Risikobewertung der bevorstehenden Datenverarbeitung. Diese Risikobewertung durch den Verantwortlichen wirkt sich zum einen auf der Rechtfertigungsebene und zum anderen auf der Ebene der Informationspflichten aus.

Zwar ist in Art. 12, 13 DSGVO nicht vorgesehen, das Risiko ausdrücklich zu benennen, aber in der Gesamtschau der Informationspflichten lässt sich der Informationsbedarf über die Risiken der Datenverarbeitung aus den ausdrücklich aufgezählten Informationspflichten entnehmen. Dazu gehört das Risikokriterium des Zwecks der Datenverarbeitung gemäß Art. 13 Abs. 1 c) und der entsprechend gewählte Begriff für die Zweckbestimmung, Art. 13 Abs. 3 DSGVO. Weiter enthalten Informationen über das Bestehen der Absicht, für einen weiteren Zweck eine Datenverarbeitung vornehmen zu wollen, ebenso eine Aussage über das bevorstehende Risiko. Denn aus dem Zweck werden der Kontext und der mögliche Umfang der Datenverarbeitung erkennbar, was die Bestimmung von Risikokriterien für die Rechte und Freiheiten natürlicher Personen ermöglicht. Weiter kann aus dem zur Verfügung stehenden Rechtfertigungsgrund etwa der Einwilligung gemäß Art. 6 Abs 1 a) DSGVO das Bestehen eines höheren Risikos der Datenverarbeitung entnommen werden, welches von dem legitimen Interesse gemäß Art. 6 Abs. 1 f) DSGVO nicht gedeckt wäre. Ebenso kann als Risikokriterium die Dauer der bevorstehenden Datenverarbeitung gemäß Art. 13 Abs. 2 b) DSGVO herangezogen werden. Denn je länger die Datenverarbeitung andauert, umso höher ist das Risiko für den Schutz der Rechte und Freiheiten natürlicher Personen. Demnach kann der Bedarf bei einer langfristigen Datenverarbeitung steigen, von den Betroffenenrechten Gebrauch zu machen. Schließlich sieht der EWG 39 S. 5 der DSGVO vor, dass der Betroffene über die Risiken im Zusammenhang mit der Verarbeitung der personenbezogenen Daten informiert werden soll, weshalb die ausdrücklichen Informationspflichten aus Art. 13, 14

421 Art. 7 f); 13 Abs. 2; 17; 20 Datenschutzrichtlinie 95/45; *Veil*, ZD 2015, 347 (351); *Kuner/Kate/Millard u.a.*, IDPL 2015, 95.

DSGVO um die Informationspflichten zum Risiko der Datenverarbeitung erweitert werden sollten.

Aus dieser Gesamtschau der Risikokriterien in den Informationspflichten wird immanent die Grundlage für eine Risikoentscheidung über die Einwilligung und die Nutzung des Dienstes durch den Betroffenen geschaffen und findet seine Bestärkung im EWG 39 S. 5 der DSGVO. Demnach besteht mit den Informationen über das Risiko der Datenverarbeitung der gleichzeitige Bedarf einer vorangegangenen Risikobewertung über die Datenverarbeitung durch den Verantwortlichen (a), was wiederum eine Risikobewertungsmethode voraussetzt. Die Anforderungen an eine Risikobewertungsmethode sollen daher im Folgenden umrissen werden. Infolge dieser Darstellung könnten die Risiken gegenüber den Rechten und Freiheiten der natürlichen Person zum Gegenstand der Informationspflichten für die Risikoentscheidung des Betroffenen gemacht werden (b).

a) Risikobewertung durch den Verantwortlichen

aa) Methode zur Risikobewertung

Die Bewertung des Risikos muss gemäß dem EWG 76 S. 2 DSGVO durch den Verantwortlichen objektiv erfolgen und setzt eine Prognose[422] über die „Informationsverwendungsfolgen“[423] mit der Datenverarbeitung als ein unsicheres Ereignis in der Zukunft voraus. Danach bedarf es der Bestimmung von Risikokriterien zur Unterscheidung der Anknüpfungspunkte möglicher Maßnahmen. Es bedarf demnach einer Kalibrierung[424] zwischen dem tatsächlichen Risiko der bevorstehenden Datenverarbeitung und den Datenschutzprinzipien, damit die Pflichten und Rechte des Ver-

422 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 181–189; *Kahneman/Tversky*, Econometrica 1979, 263 (273–277): Auf der Ebene der individuellen Prognoseentscheidung sind verhaltensökonomische Verzerrungen bei Wahrscheinlichkeitsbewertungen einzubeziehen, da scheinbar repräsentative Kriterien für die Entscheidungsfindung begründet werden und zu kognitiven Hürden führen können.

423 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 64.

424 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 57; *Quelle*, European Journal of Risk Regulation 2018, 502 (509); *Kuner/Kate/Millard u.a.*, IDPL 2015, 95.

antwortlichen konkretisiert werden können.[425] So wird die Risikobewertung mit einer Verhältnismäßigkeitsprüfung verglichen, wobei die Risikobewertung als ein Meta-regulatorisches Konzept näherliegend erscheint, da es um die übergeordnete Bewertung der Risiken einer Datenverarbeitung geht, die sich auf die Verhältnismäßigkeitsprüfung im Einzelnen auswirken könne.[426] Denn es geht um singuläre Risikobewertungen anknüpfend an die jeweiligen Risikokriterien, die in eine übergeordnete Gesamtbetrachtung über das Risiko der Datenverarbeitung münden. Damit wird eine konstatierte Skalierbarkeit der datenschutzrechtlichen Pflichten ermöglicht und die Risikobewertung in ein Konzept der „*Compliance 2.0*" überführt, welches über eine bloße binäre Struktur aus Zulässigkeit oder Unzulässigkeit einer Datenverarbeitungsmaßnahme hinaus eine wertende Betrachtung und Anpassung der Maßnahmen ermögliche, EWG 84 S. 2, 78 S 1.[427]

Als Methode zur Risikobewertung kommt eine semiquantitative Methode[428] in Betracht. In quantitativer Hinsicht wären die Zahlenwerte als Annäherungswerte einzubeziehen.[429] In qualitativer Hinsicht sind die Risikokriterien anhand der Rechtsbegriffe zu identifizieren. Gleichwohl fehle es bislang an einer Risikosystematik,[430] so dass die bestehenden Risikokriterien gemäß Art. 35 Abs. 3 a) – c) DSGVO für die Datenschutz-Folgenabschätzung und die Liste der Verarbeitungsvorgänge, die gemäß Art. 35

425 *Kuner/Kate/Millard u.a.*, IDPL 2015, 95 (97).

426 *Veil*, ZD 2015, 347 (351); *Quelle*, European Journal of Risk Regulation 2018, 502 (511).

427 *Ders.*, ZD 2015, 347 (351); *Quelle*, European Journal of Risk Regulation 2018, 502 (507); *Gellert*, CLSR 2018, 279 (284 f.)

428 *Raabe*, in: Beyerer/Winzer (Hrsg.), Beiträge zu einer Systemtheorie Sicherheit (acatech DISKUSSION), 2018, 97 (112); ebenso die quantitative und qualitative Methode befürwortend, vgl. *Quelle*, European Journal of Risk Regulation 2018, 502. Gegen einen rein quantitativen Ansatz spricht, dass die Quantifizierbarkeit der Menschenwürdegefährdung unmöglich erscheint und sich nicht mit der Verknüpfung zu Rechtsbegriffen vereinbaren ließe. Demgegenüber wäre der qualitative Ansatz geeignet, um die Auslegungsspielräume der Rechtsbegriffe angemessen zu berücksichtigen. Gleichzeitig birgt der qualitative Ansatz bei dem etwa Einstufungen in niedriges, mittleres und hohes Risiko vorgenommen werden, vgl. *Bieker/Bremert/Hansen*, DuD 2018, 492 (493), die Gefahr einer willkürlichen Entscheidung. Entsprechend wird ein semiquantitativer Ansatz befürwortet, für den aus der Empirie und Schadensersatzsummen die Zahlenwerte eingesetzt werden könnten.

429 *Ritter*, in: Schwartmann/Jaspers/Thüsing u.a. (Hrsg.), DS-GVO/BDSG, Kommentar, 2018, Art. 32 DSGVO Rn. 79 f.

430 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 8 f.

Abs. 4 DSGVO eine Datenschutz-Folgenabschätzung voraussetzen, einbezogen werden sollten. Diese Risikokriterien fungieren bei einer Risikobewertung als *„entry points"*[431] und dienen als Anknüpfungspunkte für einen prognostischen Blickwinkel der Kausalverläufe. Denn die Risikobewertung verlangt die Analyse von hypothetischen Kausalverläufen unter Einbeziehung der Datenverarbeitungskontexte und der Datenverarbeitungszwecke, die zu einer potentiellen Gefahr oder einem Schaden für die Rechte und Freiheiten natürlicher Personen führen können. Die entscheidende Aufgabe bei der Risikobewertung wird darin liegen, die mit den Risikokriterien verbundenen hypothetischen Kausalverläufe in ihren Wirkungen anhand spezifischer *Instruktionen* zu koppeln und entkoppeln[432], um die Risikokriterien für die konkrete Datenverarbeitung in quantitative Werte zu überführen. Damit soll der möglichen Willkür von Momentaufnahmen Rechnung getragen werden, so dass im Rahmen des Datenzyklus das Risiko in den jeweiligen Phasen der Datenverarbeitung der quantitativen Bewertung unterliegen sollte.

Insgesamt sind dafür die Risikokriterien aus Art. 5 Abs. 1 DSGVO und Art. 35 DSGVO abzuleiten, so dass für den Kontext der Datenverarbeitung die Risikokriterien des angewendeten Rechtfertigungsgrundes (Art. 5 Abs. 1 a) DSGVO), der Zweckbindung (Art. 5 Abs. 1 b) DSGVO),[433] des angewendeten Standes der Technik (Art. 5 Abs. 1 c) – f) DSGVO) und der Dauer mit dem Umfang der Datenverarbeitung einzubeziehen sind. Neben den Risikokriterien aus den Datenschutzprinzipien sind die Risikokriterien gemäß Art. 35 DSGVO zu konkretisieren. Jedes dieser Risikokriterien sollte mit quantitativen Werten versehen werden, die aus einer mathematischen Gesamtschau bereits bekannt gewordener Rechtsverstöße mit verhängten Bußgeldern oder aus fiktiven Zahlenwerten bestehen können.[434] Weiter sollten die Risikokriterien im Hinblick auf die hypothetischen Kausalverläufe möglicher Schadensfälle untersucht werden, was einer qualitativen Betrachtung unterliegen würde. Dafür wäre eine Eintei-

431 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 46 (48).
432 *Ders.*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 46 (58–60).
433 In der Risikobewertung ist zwischen allgemeinen Zwecken und privilegierten Zwecken etwa dem wissenschaftlichen, historischen und statistischen Zweck zu differenzieren, EWG 89 S. 3.
434 Die Quantifizierbarkeit von Risikokriterien in einer spezifischen Datenverarbeitung ist ein noch zu erforschender Gegenstand. Zunächst bestehen Unsicherheiten über die Verlässlichkeit der Informationen zu bekannt gewordenen Bußgeldern und weiter besteht Forschungsbedarf über die Bestimmung fiktiver Zahlenwerte.

lung in die Phasen der Datenverarbeitung erforderlich, die in hypothetische Schäden („potentiellen Einzelschaden“[435]) innerhalb einer Phase eingeteilt und mit einem spezifischen Zahlenwert für das Risikokriterium in der Datenverarbeitungsphase versehen werden könnten. Infolgedessen wäre eine Addition der Zahlenwerte aller Risikokriterien vorzunehmen, deren Ergebnis zwischen dem Minimal- und Maximalwert einzuordnen wäre und als semiquantitative Risikobewertung gelten könnte. Dabei geht es um eine deutlich differenziertere Darstellung des Risikos der Datenverarbeitung als es die Einordnung in eine Systematik zwischen hohem, mittlerem und niedrigem Risiko vorsehen würde, damit die Objektivität der Risikobewertungsmethode gewährleistet wird.

Insgesamt handelt es sich dabei um eine Prozeduralisierung der Datenschutzprinzipien, da diese über ein (Risikobewertungs-) Verfahren eine stufenweise Modifizierung erfahren und auf den Anwendungskontext in Gestalt der technischen und organisatorischen Maßnahmen gemäß Art. 25 Abs. 2 DSGVO übertragen werden. Denn die Prognose über die Risiken in einem Datenzyklus umfasst das Unwissen über die Wahrscheinlichkeit eines Schadenseintritts, welches prozedural „eingefangen“ werden könne.[436]

Im Hinblick auf ein Identitätsverwaltungsmodell stellt sich die Frage nach dem Umfang dieser Risikobewertung und den subjektiven Einflüssen bei der Entscheidung[437] des Betroffenen über die Verwaltung personaler Identitäten. Denn die Risikobewertung des Verantwortlichen muss zugleich die Perspektive des Betroffenen einbeziehen, welche Risiken dieser eingeht. Erst mit dieser Bewertung kann die Gesamtbetrachtung über das Risiko der Datenverarbeitung und eine Kalibrierung der geeigneten technischen und organisatorischen Maßnahmen zur Realisierung der Datenschutzprinzipien vorgenommen werden. Demnach bedarf es aus der Perspektive des Betroffenen der Transparenz über die Risiken der Datenverarbeitung, um auf dieser Grundlage eine Risikoentscheidung treffen zu können.

435 *Ritter*, in: Schwartmann/Jaspers/Thüsing u.a. (Hrsg.), DS-GVO/BDSG, Kommentar, 2018, Art. 32 DSGVO Rn. 81.
436 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (21).
437 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 178 f.

bb) Risikokriterien nach Art. 35 DSGVO als Bewertungsgrundlage

Die Risikokriterien sind zunächst aus den Datenschutzprinzipien gemäß Art. 5 Abs. 1 DSGVO abzuleiten und ermöglichen die Anpassung des Standes der Technik für die spezifische Datenverarbeitung. Daneben sind die Risikokriterien zur Bestimmung der Datenverarbeitung mit einem hohen Risiko gemäß Art. 35 DSGVO einzubeziehen. Dafür ist die Datenschutz-Folgenabschätzung vorzunehmen und die in Art. 35 Abs. 1 und in Absatz 3 DSGVO indizierend aufgezählten Risikokriterien heranzuziehen, um die semiquantitative Risikobewertungsmethode für Datenverarbeitungen mit einem hohen Risiko anwenden zu können. Gemäß Art. 35 Abs. 1 DSGVO wird ein Risikokriterium in der Verarbeitung mit neuen Technologien angenommen. Durch die neuen Technologien besteht etwa das Risiko der Informationspermanenz, wonach verarbeitete Informationen eigenständig im Raum stünden und systematisch zusammengetragen werden können.[438] Folglich ergibt sich mit den neuen Technologien eine Steigerung der Speicherungsmöglichkeiten, von denen ein eigenes Risiko für die informationelle Selbstbestimmung ausgehen kann. Daraus lässt sich das weitere Risikokriterium der systematischen Bewertung persönlicher Aspekte ableiten, wonach ein hohes Risiko bei der automatisierten Verarbeitung und dem Profiling angenommen werden kann, Art. 35 Abs. 3 a) DSGVO. Aufgrund von algorithmusbasierten automatisierten Zuordnungen können Profile erstellt werden, mit denen die Wahrscheinlichkeit über die Zugehörigkeit zu einer bestimmten Kohorte (Korrelation) bestimmt werden kann, wozu die Aussage über die Teilnahmewahrscheinlichkeit an einem Musikfestival oder die Bonität gehören kann.[439] Diese Auswirkungen lassen sich als Risiko eines Publizitätsschadens oder Reputationsverlusts[440] einordnen und können als eine Enttäuschung der berechtigten Vertraulichkeits- und Privatheitserwartung gesehen werden.

Weiter kommen die von *Drackert* beschriebenen Risiken der Informationspermanenz und Informationsemergenz zum Ausdruck, in denen jeweils die Häufigkeit der Datenspeicherung zu einer Perpetuierung des Risikos führt.[441] Die Informationspermanenz kann sich bei der Speicherung unbewusst verarbeiteter Verkehrsdaten ergeben, womit das Risiko eines

438 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 69.
439 4. Teil, A., I., 2.
440 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 69, 193.
441 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 193.

„gläsernen Bürgers“[442] bestünde und Überwachungsdruck ausgelöst werden könne.[443] Bei der Informationsemergenz werden die Daten fixiert und in unkontrollierbare, entkontextualisierte Informationen zusammengeführt, die zu Erkenntnissen und einer „verwaltungstechnischen Entpersönlichung“[444] führen können. Damit wird eine weitere Risikodimension begründet, die sich in dem gesteigerten Preisgabeverhalten des Einzelnen aufgrund eines „Kontrollgefühls“[445] niederschlagen kann. Die Risikokonzeption erfährt damit eine Subjektivierung, indem etwa psychischer Druck ausgelöst werden und dies freiheitshemmende Wirkung in Gestalt eines „Konformismusrisikos“ haben könne, was sich individuell und gesamtgesellschaftlich auswirke.[446]

Ein weiteres Risikokriterium liegt gemäß Art. 35 Abs. 3 b) in der Verarbeitung besonderer Kategorien personenbezogener Daten, wodurch aufgrund der Sensibilität von Daten das Risiko des umfassenden Erkenntnisgewinns bestehen kann. Das Risikokriterium über die systematische Überwachung öffentlich zugänglicher Bereiche gemäß Art. 35 Abs. 3 c) DSGVO erscheint dagegen als eines, welches neben dem individuellen Gefühl des Überwachtwerdens sich gesamtgesellschaftlich auswirken kann. Von diesem Risikokriterium sind besondere Kontexte im Verhältnis zwischen Staat und Bürger erfasst, so dass die „Instrumente staatlicher und privater Machtbildung“ gleichermaßen zum Risiko der Informationsmacht werden.[447] Dies gilt gerade bei dem Phänomen der im Auftrag des Staates agierenden privaten Sicherheitsunternehmen, so dass das Risiko für die Rechte und Freiheiten natürlicher Personen auch von den Akteuren und der Anzahl dieser abhängt.

Ebenso kommt bei der internationalisierten Datenverarbeitung eine weitere Dimension des Datenverarbeitungsrisikos hinzu, denn aufgrund des modifizierten Schutzregimes etwa mit dem „*EU-US-Privacy Shield*“[448]

---

442 Schlussanträge der Generalanwältin Kokott, EuGH, 18.07.2017, C-275–06, Promisucae, Rn. 97.

443 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 104 f.; EuGH, Urt. v. 08.04.2014 – C-293/12 und C-594/12, Digital Rights Ireland, Rn. 27.

444 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 183.

445 3. Teil, C., IV; *ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 291.

446 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 188–190.

447 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 280.

448 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016, Az. C (2016) 4176.

gemäß Art. 45 DSGVO wirkt bei diesen grenzüberschreitenden Datenverarbeitungen ein gegenüber der DSGVO parallel wirkendes Schutzregime. Weiter kann der effektive Rechtsschutz für den Betroffenen in Frage stehen, wenn die Rechtsstreitigkeiten gemäß 2.1. (20) *EU-US-Privacy Shield* über alternative Streitbeilegungsmethoden beigelegt werden sollen. Gleichwohl bleibt anzumerken, dass mit Art. 3 Abs. 2 DSGVO auch das Beobachten des Nutzungsverhaltens und das Anbieten von Diensten und Waren an Betroffene in der Europäischen Union vom Schutzregime der DSGVO erfasst ist (Marktortprinzip) und dieses damit eine weitreichende Wirkung über die Ländergrenzen hinweg entfaltet.

In der Gesamtbetrachtung bestehe das Risiko der Überwachungskumulation etwa durch das Zusammenführen vieler einzelner Datensätze mit Bewegungsdaten, so dass sich das Risiko des Überwachungsdruckes durch *De- und Rekontextualisierung* potenzieren könne.[449] Ebenso kommt das Risiko durch ein Kontextdefizit in Betracht, bei dem bestimmte Informationen nicht übernommen werden und nur Teilaspekte einer personalen Identität transparent werden, so dass die Erkenntnis verzerrt möglich ist.[450] Darin zeigen sich die Überschneidungen zu den bereits erwähnten Risiken der Informationspermanenz und Informationsemergenz, die sich ebenso aus den Überwachungsdaten ergeben. Somit kann Art. 35 Abs. 3 c) DSGVO als Konkretisierung zu den neuen Technologien gemäß Art. 35 Abs. 1 DSGVO angesehen werden. Als weiteres Risikokriterium kommt der materielle oder immaterielle Schaden gemäß Art. 82 Abs. 1 DSGVO hinzu, der aus der Verletzung des Schutzes personenbezogener Daten entstehen kann. Ein Schaden wird gemäß dem EWG 85 S. 1 DSGVO angenommen, wenn ein Verlust über die Kontrolle personenbezogener Daten, eine Diskriminierung bei der Verarbeitung, ein Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Verlust der Vertraulichkeit von dem Berufsgeheimnis, Rufschädigung vorliegen oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile, die dem Betroffenen drohen. Diese Schadensgruppen lassen sich übergeordnet in dem von *Drackert* beschriebenen Risiko informationeller Machtverschiebung und den Selektivitätsschäden einordnen.[451] Die

449 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 219 f.

450 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 302 f.; zum Konzept der „Kontrolle durch Intransparenz" nach *Luhmann*, vgl. 2. Teil, A., II., 1., c), bb).

451 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 280 f.; *Herfurth*, ZD 2018, 514 (518).

informationelle Machtverschiebung tritt bei dem Kontrollverlust etwa durch Identitätsdiebstahl oder Aufhebung der Pseudonymisierung auf. Demgegenüber sind Selektivitätsschäden bei Diskriminierungen aufgrund eines spezifischen Merkmals gegeben, die zu einer Stigmatisierung führen können.

Schließlich kann die Wahrscheinlichkeit des Schadenseintritts variieren, welches auch von dem angewendeten Stand der Technik und der technischen organisatorischen Maßnahmen abhängig ist. Denn gerade in der technischen Realisierung der Datenverarbeitung können der Kostendruck oder begrenzte Anreize zur Steigerung des Sicherheitsniveaus ebenfalls zu einer Steigerung des Risikos für die Rechte und Freiheiten natürlicher Personen führen und ein eigenes Risikokriterium begründen.

Insgesamt sind die Maßnahmen der Risikobewertung zu dokumentieren und können als Bestandteil der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO eingeordnet werden, welches die Berichtsphase vor der Datenverarbeitung und die Einzelheiten zu der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 7 DSGVO umfassen müsste.

b) Risikoinformationen an den Betroffenen

Nach der objektivierten Ermittlung des Risikos mit einer semiquantitativen Risikobewertungsmethode für die Rechte und Freiheiten natürlicher Personen bedarf es der Informationsmitteilung an den Betroffenen. Danach sind die Risiken der Datenverarbeitung gemäß Art. 12, 13 DSGVO, EWG 39 Gegenstand der Informationspflichten und sollten möglichst ausdrücklich benannt werden, damit die natürliche Person eine risikobewusste Entscheidung treffen kann. Die Entscheidung des Betroffenen soll die Möglichkeit einer Folgenabschätzung über die Eintrittswahrscheinlichkeit von materiellen und immateriellen Schäden umfassen können, für die der Verantwortliche mit den Informationspflichten unterstützend tätig wird. Damit sind die Informationen über die Risiken der Datenverarbeitung eine notwendige Voraussetzung für die effektive Identitätsverwaltung. Denn nur mit der Kenntnis über die mit der Einwilligung oder der Nutzung eines Dienstes verbundenen Risiken, kann die informationelle Selbstbestimmung wirksam wahrgenommen werden und Schutzmaßnahmen bei einem antizipierten Kontrollverlust über die Erkenntnisse zur personalen Identität eingeleitet werden.

Voraussetzung für die Realisierung der Informationspflichten ist die Einbeziehung der Risikobewertungsergebnisse in die Informationspflich-

ten, damit dem datenschutzrechtlichen Vorfeldschutz Rechnung getragen wird. Dazu kann die Benennung des Zahlenwertes nach der semiquantitativen Risikobewertungsmethode gehören und zusätzlich könnten die Risikokriterien mit einem hohen Risikowert in die Informationen aufgenommen werden, damit der Betroffene das kontextspezifische Risiko für die personale Identität in seine Entscheidungsfindung einbeziehen kann. Demnach besteht für die Identitätsverwaltung hinsichtlich der kontextspezifischen Datenverarbeitung ebenfalls ein Transparenzbedürfnis über das Risiko, um die Grundrisiken und hohen Risiken innerhalb eines Datenzyklus in unterschiedlichen Zeitabschnitten für den Betroffenen einschätzbar zu machen.

Ebenso können die kompensatorischen Schutzmaßnahmen zur Risikominderung gemäß Art. 32 Abs. 1 a) – c), 5 Abs. 1 d) – f) DSGVO durch den Verantwortlichen zum Gegenstand der Informationspflichten werden.[452] Damit und mit der Einbeziehung der Risikobewertungsergebnisse in den Informationspflichten erfolgt *quasi* eine Begründung über die Datenverarbeitung, die dem Ausgleich bestehender Asymmetrien zwischen Verantwortlichem und Betroffenen dient. Demnach werde der betroffenen Person zu einem frühen Zeitpunkt des Datenzyklus ermöglicht,[453] die informationelle Selbstbestimmung durch Kenntnis potentieller Schäden von Anfang an wahrzunehmen.

c) Bewertung

Die Risiken der Datenverarbeitung werden von *Drackert* in eine Mikro- und Makroebene eingeteilt, wonach diese sich auf die natürliche Person auswirken können oder in gesellschaftlich-politischen Zusammenhängen wirken.[454] Beide Risikoauswirkungen können ineinander übergehen, so dass die Ergebnisse einer semiquantitativen Risikobewertung in die Infor-

452 Gemäß Art. 32 DSGVO sind Maßnahmen angeführt, wozu die Pseudonymisierung, Verschlüsselung, Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme gehören und zum Gegenstand der Informationspflichten werden können. Sofern Zertifizierungen etwa über eine behördliche Prüfung des Verfahrens der Risikobewertung erfolgen würde, könnten diese ebenfalls in die Informationen einbezogen werden.

453 Über die frühzeitige Ausübung des „*Privacy Self Management*“, *Solove*, Harv. L. R. 2013, 1880 (1891).

454 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 278 ff.

mationspflichten aufgenommen werden sollten. Dabei könnten Risikokriterien mit hohen Zahlenwerten zum Gegenstand der Informationspflichten werden, was *de lege lata* nur aus einer Gesamtschau der Informationspflichten gemäß Art. 13 DSGVO abzuleiten ist, *de lege ferenda* wäre aber eine konkretisierte Informationpflicht über das spezifische Risiko wünschenswert.

Ebenso könnte die Einteilung gentechnischer Arbeiten in vier Sicherheitsstufen gemäß § 7 GentG für datenschutzrechtliche Risikokategorien herangezogen werden.[455] Dabei könnte für die Einteilung in die Sicherheitsstufen ein Rückgriff auf die Risikobewertung in ihrer Gesamtheit erfolgen. Die damit verbundenen Erkenntnisse könnten zum Gegenstand der Informationspflichten in den Sicherheitsstufen werden. Dies würde sich auf die Identitätsverwaltung positiv auswirken können, da das Bestehen von Sicherheits- und Risikostufen zu einer Übersichtlichkeit und gesteigerten Transparenz beitragen würde. Gleichwohl kann auch bei einer umfassenden Risikobewertung ein Risiko bestehen, welches unbekannt ist und damit in der Bewertung unberücksichtigt bliebe, sog. „*unknown unknown*“[456].

In einem Identitätsverwaltungsmodell sollte auch ein unbekanntes Risiko bei der umfangreichen Datenverarbeitung durch einen Intermediär als Plattformbetreiber über mehrere Kontexte hinweg einbezogen werden. Denn es können mehrere Identitäten in ihren *Ipse*- und *Idem*-Anteilen auf einer Plattform zu unterschiedlichen Zeitpunkten gespeichert werden und ein eigenes „*Ökosystem für personale Identitäten*“ bilden, welches erst im Laufe des Datenzyklus zu einem eigenen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dieses erweiterte Risiko über bislang unbekannte Risiken verlangt ein ausdifferenziertes Schutzregime, welches mit den Anonymisierungsmethoden umsetzbar ist. Dabei kann die Transparenz über den Schutz mit geeigneten Anonymisierungsmethoden zu einer so ausgeprägten Reputation des Plattformbetreibers führen, dass das Risiko eines Schadens für die Rechte und Freiheiten der natürlichen Person überschaubar bleibt. Weiter wäre die ausgeprägte Reputation über ein hohes Schutzniveau für personale Identitäten mit dem Geschäfsmodell unmittelbar verbunden, was zu umfassenden Schutzmaßnahmen durch den Verantwortlichen führen würde.

455 *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17 (30).
456 *Spina*, EJRR 2014, 248.

Insgesamt müsse dennoch einer überzogenen Risikobewertung („*Riskifikation*“[457]) begegnet werden und die Unbekanntheit mancher Risiken anerkannt werden. Entsprechend ist neben der ausdrücklichen Einbeziehung des Risikos in die Informationspflichten gemäß Art. 13 DSGVO das Vorliegen von zertifizierten Verfahren (Art. 42 DSGVO) zur Risikobewertung wünschenswert und könnte zu einer wirksamen Risikoallokation beitragen.

3. Kontrolle durch Transparenz

Mit den Informationspflichten wird zu Beginn des Datenzyklus dem Betroffenen eine Kontrollmöglichkeit eingeräumt, da die Informationen als Entscheidungsgrundlage des Betroffenen für die Einwilligung dienen. Diese Kontrolle lässt sich mit dem Zugang zu den Informationen in der Datenschutzerklärung und der Entscheidungsmöglichkeit begründen, so dass es sich um eine absolute Kontrolle über die Entscheidung auf Grundlage der Informationspflichten handelt. Eine Steigerung der Kontrollmöglichkeit beim Betroffenen kann durch gestufte Datenschutzerklärungen erfolgen, indem bei geringen Änderungen des Kontextes die Informationspflichten iterativ und gestuft als Kaskade wahrnehmbar werden, sog. „*layered approach*“.[458] Damit können umfangreiche Informationspflichten über ein gestuftes Modell differenziert werden, so dass auf der ersten Stufe die abstrakten Informationen über die Datenverarbeitung erfolgen, auf der zweiten Stufe die kontextbezogene Konkretisierung der Informationen und auf der dritten Stufe die Beschreibung der kontextspezifisch maßgeblichen Informationen für den besonders interessierten Betroffenen. Damit würde ein dialogischer Austausch über die Informationen als ein Wechselspiel zwischen dem Betroffenen und Verantwortlichen entstehen.

Ein derartiges Konzept steht im Gleichlauf zu der in Art. 12 Abs. 1 DSGVO und im EWG 58 S. 1 DSGVO geforderten „leicht zugänglichen Form“, wonach der iterative Zugang zu den Informationen eine effiziente-

457 *Quelle*, European Journal of Risk Regulation 2018, 502 (517 f.).

458 Dessen Rechtmäßigkeit anzweifelnd, vgl. *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 78; *Art. 29 Data Protection Working Party*, WP 260, Leitlinien für Transparenz gemäß der Verordnung 2016/679 (11. April 2018), S. 17; Vorschlag einer Teil-Einwilligung von *Kremer*, CR 2012, 438 (446); www.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 aufgerufen 20.06.2020).

re Nachvollziehbarkeit und kontextspezifische Antizipation der Risikolage ermöglicht. Entsprechend gehöre es zu den Transparenzanforderungen, dass beim Besuch von *Facebook*-„*Fanpages*" auf den Zweck und die Art der verarbeiteten Daten hingewiesen wird, welches in der Verantwortlichkeit der Betreiber von „*Fanpages*" liege.[459] Damit räumt der EuGH eine gesteigerte Kontrollmöglichkeit durch die Erweiterung der Transparenzpflichten ein, die für die Betroffenen absolut wirkt und das Spektrum der Kontrolle über die personalen Identitäten erweitert.

Insgesamt wird sogar die Einbeziehung von ausdrücklichen Warnungen über den Schutz der Privatheit, vergleichbar mit den Warnungen über die Gefahren des Rauchens, vorgeschlagen, die in den kontextspezifischen iterativen Einwilligungsprozess einbezogen werden und als Bildgebote ihre Wirkung entfalten könnten.[460] Damit würde die Kontrolle für den Betroffenen durch eindeutige Informationen erleichtert werden. Ebenso könnten sog. „*sticky policies*" eingesetzt werden, die den verarbeiteten Datensätzen über den Datenzyklus hinweg anhaften und die Kontrolle über die zweckgebundene Datenverarbeitung mit maschinenlesbaren Verarbeitungsbedingungen ermöglichen.[461] Damit könne die garantierte Umsetzung der Datenverarbeitungsbedingungen aus den Datenschutzerklärungen umgesetzt werden.

Mit diesen technischen Unterstützungen können die Kontrollmöglichkeiten sichergestellt werden, ohne dass eine regelmäßige und bewusste Entscheidung des Betroffenen herbeigeführt werden muss. Folglich sind die Informationspflichten für den Betroffenen dazu geeignet, zu Beginn des Datenzyklus über die Risiken der Datenverarbeitung und der mit ihr verbundenen personalen Identitäten Kontrolle auszuüben.

4. Bewertung

Die Transparenz als Grundlage der Informationspflichten dient im Sinne einer „juristischen Glaskultur"[462] der Schaffung von Sichtbarkeit über Vorgänge, die nicht im Verantwortungsbereich des Betroffenen liegen. Viel-

459 EuGH, Urt. v. 05.06.2018 – Az.: C-210/16, Rn. 40, 44.
460 *Solove*, Harv. L. R. 2013, 1880 (1885); zu Bildgeboten und zum zwangsweise vor Augen führen von Risiken am Beispiel der Zigarettenschachteln, vgl. *Dreier*, Bild und Recht, 2019, S. 246.
461 *Pearson/Casassa-Mont*, Computer 2011, 60.
462 *Damler*, Rechtsästhetik, 2016, S. 303–305.

mehr sind zwischen Verantwortlichem und Betroffenen asymmetrische Informationslagen festzustellen, so dass die Informationspflichten zur Kompensation dieser beitragen können. Dazu gehört die Einbeziehung der Informationen aus der Risikobewertung in die Datenschutzerklärung. Denn in Kenntnis der konkreten mit der Datenverarbeitung verbundenen Risiken ist die umfassende Einschätzung möglich und kann die Grundlage für eine wirksame Identitätsverwaltung bilden.

Folglich kann sich der Bedarf nach einer fortgesetzten Informationspflicht im Rahmen von gestuften Datenschutzerklärungen als *„layered approach"* auch nach der Rechtmäßigkeit ergeben und würde in einem Identitätsverwaltungsmodell der Kontrollausübung dienen. Weiter wird aus dem Treu und Glauben-Grundsatz über die Datenverarbeitung gemäß Art. 5 Abs. 1 a) DSGVO eine Hinwendung zum Abbau bestehender Informationsasymmetrien durch Transparenz über die Datenverarbeitung und ihre Risiken angenommen.[463] Demnach wären gestufte Datenschutzerklärungen für ein Identitätsverwaltungsmodell nicht nur eine Anforderung aus den Informationspflichten gemäß Art. 12 ff. DSGVO, sondern auch aus dem Gebot der Verarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 a) DSGVO abzuleiten und würden dem Ausgleich bestehender Informationsasymmetrien dienen.

Da Intransparenz zu Unsicherheit und Vermeidungsverhalten führen kann, wird eine eigene Informationspflicht über das Bestehen der Informationsasymmetrie und den mit ihr verbundenen Risiken befürwortet.[464] Danach sind die maßvollen Informationspflichten über die Datenverarbeitung und die Rechtsbeziehung zum Verantwortlichen eine Voraussetzung für das Identitätsverwaltungsmodell, wenn der Betroffene zu Beginn des Datenzyklus eine wirksame Kontrollmöglichkeit erhalten soll. Diese Kontrollmöglichkeit sollte jedoch beschränkt sein, um die Wirkungen des Kontroll-Paradoxons,[465] dass mit einer ausgeprägten Kontrollmöglichkeit eine höhere Offenlegungsbereitschaft besteht, einzudämmen. Entsprechend sollte der Umfang der Informationen maßvoll gestaltet werden und in inhaltlicher Hinsicht sollten aufklärende und zugleich warnende Informationen gewählt werden. Damit können die Informationen über den Datenzyklus und seine Risiken für die personale Identität langfristig zu einem gesteigerten Schutz der informationellen Selbstbestimmung beitragen.

---

463 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 173.
464 *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 52.
465 3. Teil, C., IV.

III. Konkretisierte Datenschutzgrundsätze für die Identitätsverwaltung, Art. 5 Abs. 1 b) – f) DSGVO

Der Verantwortliche muss für die Erstellung der Datenschutzerklärung zunächst die Grundsätze der bevorstehenden Datenverarbeitung festgelegt haben. Insoweit ist eine umfassende Kenntnis über die inhaltliche und organisatorische Ausgestaltung der Datenverarbeitung mit der technischen Umsetzung vor der Erstellung einer Datenschutzerklärung notwendig, was die Risikobewertung einschließt. Dafür müssen die Grundsätze der Datenverarbeitung gemäß Art. 5 Abs. 1 b) – f) DSGVO mit den Anforderungen an die Identitätsverwaltung zusammengeführt und konkretisiert werden, um die Schutzmöglichkeiten für die personalen Identitäten aufzeigen zu können. Demnach wirken sich diese Anforderungen *ex ante* zur Rechtfertigung dahingehend aus, inwieweit aus der Perspektive des Betroffenen die Kontrolle über die personalen Identitäten im Rahmen der Zweckbindung gemäß Art. 5 Abs. 1 b) DSGVO ausgeübt werden kann (1.). Weiter muss bei der Datenverarbeitung der Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 c) DSGVO umgesetzt werden, so dass die Datenverarbeitungen und Erkenntnismöglichkeiten über personale Identitäten auf ein minimales Niveau zu beschränken oder sogar zu vermeiden sind (2.). Davon ist die Gewährleistung der Richtigkeit, Integrität und Vertraulichkeit der personenbezogenen Daten durch den Verantwortlichen erfasst, was eine wesentliche Anforderung zum Schutz der personalen Identitäten im Identitätsverwaltungsmodell darstellt und über die Datensicherheitsanforderung gemäß Art. 5 Abs. 1 d), f) DSGVO nachvollzogen werden soll (3.). Schließlich könnte mit einem „*identity management by design*"-Konzept als Ausprägung des Standes der Technik gemäß Art. 25 DSGVO (4.) die Identitätsverwaltung als ein eigenständiges „*privacy by design*"-Konzept ausgestaltet werden. Dieses würde als wirksamer Schutzmechanismus für die Identitätsverwaltung dienen und zum Gegenstand einer abschließenden Bewertung werden (5.).

1. Zweckgebundene Identitätsverwaltung, Art. 5 Abs. 1 b) DSGVO

Die Informationspflichten umfassen den Zweck der Datenverarbeitung, Art. 13 Abs. 1 c), Art. 5 Abs. 1 b), Art. 6 Abs. 4 DSGVO, EWG 50. Danach kann die Entscheidung des Betroffenen zur Einwilligungserteilung von den Informationen über den Zweck der Datenverarbeitung abhängig sein. Mit der Zweckbestimmung des Verantwortlichen lässt sich zudem die

Grundlage für eine „freiwillige Kooperation“[466] mit der natürlichen Person schaffen, indem der transparente Zweck die Aufmerksamkeit auf die Datenverarbeitung richtet und das Interesse an dem Dienst steigern kann. Gleichzeitig ist mit der Zweckfestlegung des Verantwortlichen das inhaltliche und zeitliche Spektrum der rechtmäßigen Datenverarbeitung festgelegt, so dass überflüssige Datenverarbeitungen identifiziert und ausgenommen werden müssen.[467] Dabei hat der Verantwortliche einen Einschätzungsspielraum über die Zweckfestlegung, der seine Grenze in der Rechtmäßigkeit des Zweckes finden würde, womit die Zweckfestlegung eine Selbstbindung des Verantwortlichen zur Einhaltung des Zwecks im Laufe des Datenzyklus auslöst. Dazu gehört das Gebot, dass die Datenverarbeitung befristet wird und nach der Zweckerreichung die Sperrung oder Löschung der Daten, wenn kein normativer Aufbewahrungsgrund besteht, vorgenommen wird, Art. 5 Abs. 1 e) DSGVO, EWG 39.[468] Damit findet das Verhältnismäßigkeitsprinzip eine einfachrechtliche Realisierung zum Schutz der informationellen Selbstbestimmung vor unvorhersehbaren Datenerhebungen und Datensammlungen in dem Zweckbindungsgrundsatz.[469]

Ebenso kommt innerhalb eines Datenzyklus des Betroffenen nach der DSGVO eine Änderung des Zweckes ohne erneute Rechtfertigung gemäß Art. 6 Abs. 1 DSGVO durch die verantwortliche Stelle in Betracht, wenn der neue Zweck mit dem ursprünglichen Zweck „vereinbar“ ist, Art. 6 Abs. 4 DSGVO, EWG 50 S. 6.[470] Die Bestimmung, wann der Zweck mit dem ursprünglichen Zweck vereinbar ist, unterliegt der rechtlichen Unsicherheit, wann zwischen beiden Zwecken ein „Zusammenhang“ angenommen werden kann und der neue Zweck von den „vernünftigen Erwartungen“ der betroffenen Person gedeckt wäre, Art. 6 Abs. 4 a)–e) DSGVO, EWG 50 S. 6. Somit besteht eine rechtliche Unsicherheit, mit welchen Datenverarbeitungen der Betroffene über die ursprüngliche Datenverarbeitung hinaus zu rechnen hat. Folglich ergibt sich aus der Zweckänderung ein konkretes Risiko für den Schutz der informationellen Selbstbestimmung, denn der ursprüngliche Umfang der Datenverarbeitung dient als Grundlage für die Erkenntniserlangung und kann unvorhersehbar zu Las-

466 *Grimm*, JZ 2013, 585 (588).
467 *Kühling/Klar/Sackmann*, Datenschutzrecht, 2018, Rn. 286, 338 f.
468 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 142–145; *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 64–68.
469 BVerfGE 65, 1 (46, 63).
470 EWG 50 S. 1 und 2.

ten des Betroffenen erweitert werden. Dies läuft dem Gebot zuwider, dass mit der Zweckbindung als Minimalprinzip[471] die Datenverarbeitung eingegrenzt werden soll und als *Instruktion* für das mögliche Erkenntnisspektrum über eine personale Identität dient. Daher geht mit der Zweckfestlegung und der Zweckänderung das Risiko einher, dass der erweiterte Datensatz zu einer Erkenntniserweiterung über die personale Identität in unvorhersehbarem Maß für den Betroffenen führt.[472] Demnach wird in praktischer Hinsicht die regelmäßige Bereinigung des Datenzyklus auch für die Datenrichtigkeit als notwendiger Bestandteil der Zweckbindung angesehen.[473]

Die Zweckgebundenheit verlangt für die Identitätsverwaltung, dass eine verfahrensrechtliche Sicherung durch kanalisierte Datenverarbeitung zur Beschränkung der Erkenntnismöglichkeiten führt und damit die Risiken gegenüber den Rechten und Freiheiten natürlicher Personen minimiert werden. Mit der Zweckfestlegung durch den Verantwortlichen und der Information über den Zweck an den Betroffenen wird eine Kontrollmöglichkeit eingeräumt, die es dem Betroffenen ermöglicht, die Datenverarbeitung über die personale Identität einschätzen zu können. Gleichwohl erfährt die Einschätzungsmöglichkeit mit der Änderung des Zweckes gemäß Art. 6 Abs. 4 DSGVO eine Einschränkung, da es aus der Perspektive des Betroffenen keine erneute Kontrollmöglichkeit gibt, mit der die ursprüngliche Einschätzung korrigiert werden kann. In Anbetracht der fehlenden Möglichkeit für den Betroffenen bei der Zweckänderung durch eine erneute Einwilligung mitentscheiden zu können, kann eine Einbuße der Kontrolle des Betroffenen und damit des *Selbstdatenschutzes* angenommen werden. Daher bleibt für die Identitätsverwaltung die Transparenz des Zweckes über die Datenverarbeitung der maßgebliche Anknüpfungspunkt für die Kontrolle der personalen Identitäten und der Erkenntnismöglichkeiten über diese.

2. Datenminimierte Identitätsverwaltung, Art. 5 Abs. 1 c) DSGVO

Die Datenminimierung als Prämisse für die Identitätsverwaltung erwächst aus dem Vorsorgeprinzip und wird aus dem Verhältnismäßigkeitsgrundsatz abgeleitet. Danach wird bei der Datenverarbeitung das Gebot verfolgt,

471 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 254.
472 *Grafenstein*, DSRI 2016, 233 (240 f.).
473 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 125.

die Datenerhebung und Datenverarbeitung auf einem minimalen Niveau zu halten, wonach die Datenverarbeitung grundsätzlich vermieden und bei Erforderlichkeit eine schonende Form der Datenverarbeitung in Gestalt von frühzeitiger Löschung, Sperrung oder Pseudonymisierung gewählt werden soll.[474] Damit liegt ein Schutzregime gegenüber den möglichen Erkenntnissen über eine personale Identität vor, indem die Datenverarbeitung von Anfang an auf die wesentlichen personenbezogenen Daten beschränkt und die Vielfalt an Lernmöglichkeiten aus den Informationen eingedämmt wird. Der Grundsatz zur Datenminimierung stellt somit Anforderungen an die technischen und organisatorischen Maßnahmen für die Datenverarbeitung und ist nach neuer Rechtslage gemäß Art. 83 Abs. 5 a) DSGVO bußgeldbewährt, so dass ein wirksamer Anreizmechanismus zur Umsetzung für den Verantwortlichen geschaffen wurde, Art. 25 Abs. 1, 32 DSGVO, EWG 156.

Zu der Datenminimierung gehört die Pseudonymisierung der Daten, womit über die Kennung ein gesteigertes Schutzniveau eingeführt wird und die Zuordnungsregel allein bei der verantwortlichen Stelle liegt, Art. 4 Nr. 5 DSGVO.[475] Die Kennung ermöglicht den Zugang zu einer Teilidentität, so dass diese Ausprägung für die Identitätsverwaltung und die Steigerung des Schutzniveaus von Teilidentitäten eingesetzt werden kann. Demnach setzt die Datenminimierung voraus, dass die Datensätze pseudonymisiert, verschlüsselt oder anonymisiert werden sollten, um die Personenbeziehbarkeit zu mindern. Von der Datenminimierung erfasst ist die Anonymisierung der Datensätze, auch wenn anonyme Informationen aus dem sachlichen Anwendungsbereich der DSGVO ausgeschlossen sind, EWG 26 S. 5. Dies erklärt sich damit, dass der ausgeprägteste Schutz für die informationelle Selbstbestimmung mit der Anonymisierung erfolgt und die eindeutige Zuordnung zwischen anonymen und personenbezogenen Daten fließend erfolgt und einem Graubereich unterliegt. Damit ist die technisch-methodische Abgrenzung zwischen anonymen und personenbezogenen Daten als graduell einzuordnen.

Anonyme Daten sind gegeben, wenn die Verknüpfung zu einer natürlichen Person direkt oder in einer Kohorte faktisch aufgrund des hohen Aufwandes an Zeit, Kosten und Arbeitskraft ausgeschlossen ist, was in Übereinstimmung mit der vom Bundesverfassungsgericht geforderten ab-

474 *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 57 f.

475 4. Teil, A., I., 3.

soluten und mathematischen Anonymität steht.[476] Indem mehrere Datenverarbeitungen zusammengefasst werden und als Daten einer Kohorte erscheinen, kann dies zu einer faktischen Anonymisierung führen, so dass Methoden mit der Zuordnung von Daten in Kohorten naheliegend für die Anonymisierung erscheinen. Dies kann mit den Anonymisierungsmethoden „*differential privacy*" und „*pufferfish framework*" erfolgen, die eine methodische Annäherung an die dauerhafte Unlesbarkeit und Unverfälschbarkeit von Daten ermöglichen. Nach dem Konzept der „*differential privacy*" werden die personenbezogenen Daten in einer Datenbank modifiziert und strukturiert, so dass die Authentizität gewährleistet wird, aber keine Rückschlüsse auf die natürliche Person möglich sind.[477] Diese Datenbanken sind mehrrelational und verfügen über Zufallsverteilungen der Datensätze, so dass für einen neugierigen Angreifer keine personenbezogenen Daten festzustellen sind.[478] Die Angriffsperspektive richtet sich dabei auf die verwendbaren Daten zur Erkenntniserlangung und die Möglichkeit der Re-Identifikation einer natürlichen Person. Dabei können etwa mit der Einordnung von Kohorten zu Gehältern die Durchschnittsgehälter gebildet werden, Erkenntnisse über die Gehaltsverteilung erlangt und Tendenzaussagen getroffen werden, ohne dass dabei die natürlichen Personen identifizierbar sind.[479] Gegenüber der Methode „*differential privacy*" geht „*pufferfish framework*" einen Schritt weiter, weil über einen Datensatz hinaus beliebige Paare von Datensätzen gebildet werden, so dass aufgrund dieser Datenpaare keine eindeutigen Erkenntnisse möglich sind und eine Intransparenz hergestellt wird.[480] Bei diesen Methoden geht es um das Risiko der Identifizierbarkeit und Erkenntniserlangung, welches mit den Me-

476 BVerfGE 65, 1 (16 f.); BVerfGE 27, 1; *Kühling/Klar/Sackmann*, Datenschutzrecht, 2018, Rn. 262 f.; *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 37; *Pfitzmann*, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management-A Consolidated Proposal for Terminology, 2006, S. 24.

477 *Spiecker gen. Döhmann/Tambou/Bernal u.a.*, EDPL 2016, 535 (539).

478 *Buchmann*, DuD 2015, 510 (514).

479 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 103; *Klar/Kühling*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 4 DSGVO Rn. 15 f.; *Gola*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 4 DSGVO Rn. 9. Etwa die Informationen über die Kohorte der Einwohner eines Stadtteils und das dort erreichte Wahlergebnis bestimmter Parteien. Die Rückschlüsse und inhaltlichen Aussagen über das Wahlverhalten hängen dann von dem Zusatzwissen und den Interpretationsregeln (*Instruktionen*) ab.

480 *Buchmann*, DuD 2015, 510 (513).

thoden „*differential privacy*“ und „*pufferfish framework*“ *quasi* ausgeschlossen wird. Damit ist die Anonymisierung von personenbezogenen Daten und personalen Identitäten in Kohorten in technischer Hinsicht möglich.[481]

Dem Grundsatz der Datenminimierung folgend, geht es nicht allein um die Verringerung des Umfangs der Datenverarbeitung, sondern auch um die Minimierung der Erkenntnismöglichkeiten, so dass die Anonymisierungsmethoden entscheidend für die Gewährleistung der Datenminimierung und des Identitätsschutzes sind. Mit der Datenminimierung werden Beschränkungen der Erkenntnisse ermöglicht und zugleich wird das Risiko für die Rechte und Freiheiten natürlicher Personen verringert. Dabei kann mit den Anonymisierungsmethoden der Eindruck erweckt werden, dass diese eine Garantie über den Schutz vor Erkenntnismöglichkeiten darstellen, wobei in Anbetracht ubiquitärer Datenverarbeitungen als *Big Data*-Phänomen lediglich eine Garantie über den Schutz vor Erkenntnismöglichkeiten für einen bestimmten Kontext ausgesprochen werden kann. Im Sinne eines umfassenden Schutzes vor Erkenntnissen im online-Kontext fungiert die Anonymisierung als Prämisse, kann aber zugleich nicht als Garant für den kontextübergreifenden Schutz vor Datenmacht und Informationsasymmetrien verstanden werden.[482] Insofern können Plattformen mit einem ausdifferenzierten Schutzmechanismus von Anonymisierungsmethoden ein *Ökosystem für personale Identitäten* bilden, in dem die *Ipse*- und *Idem*-Anteile aus verschiedenen Kontexten gespeichert und interoperabel ausgestaltet werden. Der Grundsatz der Datenminimierung kann darin den notwendigen Schutz vor Erkenntnismöglichkeiten bieten, die innerhalb des Ökosystems entstehen können und dem *Konzept des Selbstdatenschutzes* dienen würden.

Mit der Pseudonymisierung kann ein Schutz annähernd zu der Anonymisierung erreicht werden, wenn eine Kombination von mehreren Pseudonymen zu einer Erschwerung der Zuordnung zur natürlichen Person führt und die Erkenntnismöglichkeiten über personale Identitäten einschränkt. Indem es bei dem Identitätsverwaltungsmodell um den Schutz vor der Erkenntniserlangung in den Kontexten und bei Kontextüberschneidungen geht, liegt in den Methoden der Datenminimierung (Verschlüsselung, Pseudonymisierung, Anonymisierung) ein entsprechender

481 Die Möglichkeit der Anonymität innerhalb einer Gruppe wird bei drei oder fünf Personen angenommen, vgl. *Weichert*, DuD 2007, 17 (19).

482 *Becker*, JZ 2017, 170 (172); *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 1 Rn. 20–22.

Schutzmechanismus. Folglich muss das Identitätsverwaltungsmodell an die Methoden der Datenminimierung und die *Instruktionen* anknüpfen, um das Risiko für die informationelle Selbstbestimmung antizipierbar zu machen und den Informations- und Wissensgehalt über eine personale Identität einzuschränken. Dabei könnte Bestandteil der Datenminimierung in einem Identitätsverwaltungsmodell sein, dass ein spezifischer Datensatz mehrfach in verschiedenen Kontexten verwendbar wird. Dies würde in einem Datenzyklus den kontextübergreifenden Einsatz von bestimmten *Idem*-Anteilen einer personalen Identität ermöglichen. Darin kommt das Spannungsverhältnis der Datenminimierung zum Ausdruck, wonach die Authentizität und Verfügbarkeit der Daten etwa über mehrfache Speicherung sichergestellt werden muss, was zum Bedarf an redundanten Datenverarbeitungsprozessen führt, zugleich aber im Wertungswiderspruch mit der Datenminimierung steht.

Demnach könnte die Speicherung mehrfach einsetzbarer Datensätze über die *Idem*-Anteile einer personalen Identität zu einer Umsetzung der Datenminimierung in ein Identitätsverwaltungsmodell führen, so dass die Verwaltung der personalen Teilidentitäten eine übergeordnete Maßnahme im Einklang mit der Datenminimierung sein kann. Insofern würde die Identitätsverwaltung dem kontextspezifischen Einsatz von Pseudonymisierungs- und Anonymisierungsmethoden übergeordnet sein und als Maßnahme der „Meta-Datenminimierung" fungieren können. Damit würde die Identitätsverwaltung eine Kontrollmöglichkeit mit Hilfe der Methoden zur Datenminimierung schaffen und die Beschränkung der Erkenntnismöglichkeiten fördern. Daher lassen sich der Grundsatz der Transparenz und die Datenminimierung als Mittel der Kontrolle in der Identitätsverwaltung einsetzen, so dass eine kontextspezifische Realisierung der Datenminimierung von der natürlichen Person kontrolliert werden kann. Darin liegt ein wesentlicher Bestandteil des *Selbstdatenschutzes*, da die Vorzüge des Grundsatzes der Datenminmierung gerade in der Pseudonymisierung bei der kontextübergreifenden Identitätsverwaltung zum Ausdruck kämen.[483]

483 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 56.

3. Datensicherheit in der Identitätsverwaltung, Art. 5 Abs. 1 d), f), Art. 32 DSGVO

Die Voraussetzung für die Identitätsverwaltung ist ein Modell, in dem die Verwaltung der personalen Teilidentitäten unter den Vorgaben der Datensicherheit erfolgt, wobei die Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit der Daten und der personalen Identität gewährleistet werden müssen. Bei einem Verstoß besteht nach Art. 33 DSGVO die Meldepflicht der verantwortlichen Stelle innerhalb von 72 Stunden, so dass auch mit der Bußgeldbewährtheit gemäß Art. 83 Abs. 5 a) DSGVO ein effektiver Schutzmechanismus besteht. Zudem unterliegt die Realisierung der Datensicherheit dem risikobasierten Ansatz nach Art. 32 Abs. 1 DSGVO, wonach sich die angemessene Maßnahme zur Datensicherung nach der Eintrittswahrscheinlichkeit eines Schadens und dem Maßnahmenkatalog aus Art. 32 Abs. 1 a) – d) DSGVO richtet. Demnach bedarf es einer Kalibrierung der Datensicherheitsmaßnahme spiegelbildlich zur Risikobewertung, die sich in dem Stand der Technik und den technischen und organisatorischen Maßnahmen abbildet.

Zu den funktionalen Anforderungen an ein Identitätsverwaltungsmodell gehören die Richtigkeit, die Speicherbegrenzung, die Integrität und die Vertraulichkeit der Daten sowie die Belastbarkeit des technischen Systems, womit die Widerstandsfähigkeit und Ausgleichsfähigkeit eines Systems gegenüber Störungen umfasst ist, sog. Resilienz gemäß Art. 32 Abs. 1 b) DSGVO.[484] Weiter ist die Gewährleistung der Richtigkeit der personenbezogenen Daten gemäß Art. 5 Abs. 1 d) DSGVO maßgeblich für die Datensicherheit der personalen Identitäten. Die Richtigket der Daten sieht die sachliche Richtigkeit als objektives Kriterium vor, so dass eine enge Verbindung von der inhaltlichen Richtigkeit der Daten zu dem Zweck der Datenverarbeitung besteht.[485] Denn würde der Zweck der Datenverarbeitung in der Identifizierung der natürlichen Person liegen, wäre die Speicherung eines fiktiven Namens als Pseudonym unrichtig.

Weiter erfordert die sachliche Richtigkeit der Daten auch die Gewährleistung der Nicht-Verkettbarkeit von Datensätzen, damit die objektive Richtigkeit separater Datensätze nicht durch die kontextübergreifende Verbindung gefährdet wird. Dabei ist zwischen absoluter und relativer

484 *Gonscherowski/Hansen/Rost*, DuD 2018, 442 (446); *Jandt*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 32 DSGVO Rn. 26, Fn. 55, 56.

485 *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 60–62.

Nicht-Verkettbarkeit zu unterscheiden. Die absolute Nicht-Verkettbarkeit gewährleistet, dass keinerlei Verbindung zwischen den jeweiligen Datensätzen hergestellt werden darf und die relative Nicht-Verkettbarkeit verlangt, dass sich der Informationsgehalt durch die Verbindung der Datensätze nicht verändert.[486] Diese Differenzierung ist für ein Identitätsverwaltungsmodell entscheidend, da mit der Datensicherheit die Anforderung erfasst ist, dass neben der kontextübergreifenden Verbindung von Datensätzen keine kontextübergreifenden Erkenntnisse generierbar sein dürfen. Damit stellt der Grundsatz der Datensicherheit die kontextspezifische Trennung der Datensätze zu den personalen Teilidentitäten sicher und gewährleistet, dass keine kontextübergreifende Erkenntniserlangung erfolgt.

Weiter umfasst die Datensicherheit den Schutz vor unbefugtem Zugang und den Schutz der Daten vor Zerstörung und Verlust, was den technischen und organisatorischen Maßnahmen aus der Anlage des § 9 BDSG a. F. entspricht.[487] Danach verlangt die Datensicherheit die dynamische Sicherstellung von Zutritts-, Zugangs- und Zugriffskontrolle und etwa der Weitergabekontrolle durch den Verantwortlichen. Aus der Zugangskontrolle lässt sich die Identitätsverwaltung unmittelbar ableiten, so dass verhältnismäßige technische und organisatorische Maßnahmen hierzu getroffen werden sollten. Sobald eine physische Zugangskontrolle etwa über das Wissen eines Passwortes oder den Besitz eines Schlüssels implementiert wurde, muss sichergestellt werden, dass diese Einrichtung über den Datenzyklus hinweg die Datensicherheit gewährleistet. Hier kommen Software-Lösungen in Betracht, die aus regelmäßigen Aktualisierungen und Fehlerbehebungen bestehen.[488] Für die Gewährleistung der Datensicherheit eines Datenzyklus bei der Identitätsverwaltung bedarf es demnach der regelmäßigen Sicherstellung, dass mit dem Stand der Technik und den technischen und organisatorischen Maßnahmen die aktuellen Risiken der Datenverarbeitung einbezogen werden.

---

486 *Unabhängiges Landeszentrum für Datenschutz* (ULD), Identity Management Systems (IMS), 2004, S. 8.

487 *Herbst*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 5 DSGVO Rn. 74–76.

488 *Faber/Sedlacek*, DuD 2017, 440 (443). Indem sich das Problem bei Softwareschwachstellen manifestieren und perpetuieren kann, soll vergleichbar mit einem Sicherheitssystem in Zügen (Lockführer betätigt Knopf alle dreißig Sekunden, damit er wach bleibt) auch bei Software in bestimmten Sicherheitsstufen integriert werden, sogenanntes „Life – Sign – Controll" mit dem nur regelmäßig gepflegte Geräte am Netz bleiben sollen, „Mindesthaltbarkeit".

Für die Gewährleistung der kontextspezifischen Datensicherheit von Teilidentitäten kommen solche technischen Lösungen in Betracht, mit denen die personalen Teilidentitäten aktiviert und deaktiviert werden oder personale Teilidentitäten in Übereinstimmung mit der Zweckerreichung einer Mindesthaltbarkeit[489] unterliegen können. Darin liegen geeignete Maßnahmen für die Datensicherheit in einem Identitätsverwaltungsmodell, die von dem Verantwortlichen zunächst vor der Datenverarbeitung und nach Beginn der Datenverarbeitung im Rahmen der Sicherstellungspflichten umgesetzt werden müssten.

4. Identitätsverwaltung durch Technikgestaltung, Art. 25 DSGVO

Die Identitätsverwaltung kann Gegenstand der Technikgestaltung sein und über die Berücksichtigung des Standes der Technik gemäß Art. 25 DSGVO bestimmt werden. Es kommt neben der datenschutzkonformen Technikgestaltung der Identitätsverwaltung als „*privacy by design*" und „*privacy by default*", EWG 78 S. 2, die Konkretisierung als „*identity management by design*" in Betracht, so dass der Feststellungsvorgang über den geeigneten Stand der Technik untersucht werden soll. Gemäß Art. 25 Abs. 1 DSGVO soll durch den Verantwortlichen der Stand der Technik „berücksichtigt" werden. Der Stand der Technik wird nach der Drei Stufen-Theorie oberhalb der ersten Stufe über die allgemein anerkannten Regeln der Technik und unterhalb der dritten Stufe, dem Stand von Wissenschaft und Technik, eingeordnet.[490] Der Stand der Technik gilt in diesem Gefüge als ein unbestimmter Rechtsbegriff mit Verweisungsgehalt, wodurch der Einbeziehungsbedarf des aktuellen technischen Entwicklungsstands mit dem im Markt verfügbaren Fortschritt sichergestellt wird.[491] Damit soll über diesen unbestimmten Rechtsbegriff die Front der technischen Entwicklungen durch den Verantwortlichen angewendet und eine justiziable Lösung aus dem Spannungsverhältnis zwischen Recht und Technik ermöglicht werden.[492] Die Bestimmung der konkreten technischen Maßnahme richtet sich nach dem Öffnungsprädikat der „Berücksichtigung" des Standes der

489 *Dies.*, DuD 2017, 440 (444 f.).
490 BVerfG, NJW 1979, 359 – Kalkar-Entscheidung.
491 *Breuer*, AöR 101 (1976), 46 (50); *Seibel*, NJW 2013, 3000; *Bartels/Backer*, DuD 2018, 214 f.
492 BVerfG, NJW 1979, 359 (362) – Kalkar-Entscheidung; *Breuer*, AöR 101 (1976), 46 (68).

Technik und erlaubt die Einbeziehung subjektiver Fähigkeiten der verantwortlichen Stelle, etwa das technisch Mögliche und wirtschaftlich Zumutbare.[493]

Für die Bestimmung der potentiellen technischen Maßnahmen zur Realisierung der Identitätsverwaltung ist die Bildung eines Maßnahmenbündels für die abschließende Identifizierung der Bestleistung notwendig.[494] Der Festlegungsvorgang aus dem Maßnahmenbündel unterliegt einer iterativen individuellen Machbarkeits- und Verhältnismäßigkeitsprüfung und entspricht einer eigenständigen Risikobewertung, da es bei dem jeweiligen Stand der Technik um die Bewertung der Eintrittswahrscheinlichkeit eines potentiellen Schadens nach dem EWG 85 S. 1 geht.[495] Hierbei werden prognostische Elemente einbezogen, wenn die Datenschutzrisiken aus der technischen Gestaltung der Datenverarbeitung, der Zweck der Datenverarbeitung und die Kategorien personenbezogener Daten miteinander in Einklang zu bringen sind, EWG 83 S. 3.

Aus dem Öffnungsprädikat der Berücksichtigung kommt der prozedurale Charakter zum Ausdruck, wonach es sich um einen dynamischen Prozess zur Bestimmung des geeigneten Standes der Technik handelt.[496] Aufgrund der Bestimmung des Standes der Technik durch den Verantwortlichen aus seiner subjektiven Perspektive kann dies zu Divergenzen des Schutzniveaus innerhalb einer Produktgruppe führen, da jeder Verantwortliche über andere subjektive Kriterien verfügt, mit denen eine Maßnahme aus dem Maßnahmenbündel bestimmbar wird.[497] Zwar kann sich dies aus Gründen des Wettbewerbs positiv auf das Marktverhalten der Ver-

493 *Baumgartner*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2018, Art. 25 DSGVO Rn. 15; *Seibel*, NJW 2013, 3000 (3003); zum Öffnungsprädikat *Raabe/Schallbruch/Steinbrück*, CR 2018, 706 (708): Im Gegensatz zu dem Öffnungsprädikat der „Berücksichtigung" müssen gemäß §§ 30a Abs. 2, 36 Abs. 5 Nr. 2 StVG Maßnahmen nach dem Stand der Technik „getroffen" werden, in §§ 71 Abs. 1 S. 2, 64 Abs. 1 S. 1, 22 Abs. 2 S. 2 BDSG soll die „Berücksichtigung gewährleistet" werden, in § 18 Abs. 2 De-Mail-G soll der Stand der Technik „erfüllt" werden und in § 8a Abs. 1 S. 2 BSIG soll der Stand der Technik „eingehalten" werden. In diesen mit dem Stand der Technik verbundenen Prädikaten kann ein „mehr" oder „weniger" an Prüfungsintensität enthalten sein.

494 *Knopp*, DuD 2017, 663 (664); *Teletrust*, Handreichung zum „Stand der Technik", 2018, S. 8.

495 *Martini*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 24 DSGVO Rn. 41 f.; *Bartels/Backer*, DuD 2018, 214 (216).

496 *Martini*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 24 DSGVO Rn. 41–43; *Jandt*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 32 DSGVO Rn. 9.

497 *Schallbruch*, CR 2016, 663 (668 f.).

antwortlichen auswirken, jedoch liegt darin das Risiko eines eingesetzten Standes der Technik, der sich für das Schutzniveau des Betroffenen als Verbraucher nachteilig auswirkt. Ferner kann die Reputation des Verantwortlichen mit dem eingesetzten Stand der Technik erweitert werden, um im Wettbewerb über ein hohes Privatheitsniveau chancenreich zu sein. Folglich kommt dem Stand der Technik in Verbindung mit dem Öffnungsprädikat eine prinzipielle Funktion zu, indem bereichsübergreifend ein prozedurales Schema zur justiziablen Technikbestimmung angewendet wird.[498]

Sobald die geeignete technische Maßnahme zur Realisierung eines „*identity management by design*" identifiziert werden konnte, kann dies zu einer Schutzsteigerung der informationellen Selbstbestimmung führen. Wobei als Voraussetzung dafür gewährleistet sein müsste, dass den kontextabhängigen technischen Präferenzen der natürlichen Person Rechnung getragen und eine Kontrollmöglichkeit über den „*digitalen Hausrat*"[499] eingeräumt wird. Dies müsste mit entsprechenden Investitionen in die technische Gestaltung erfolgen, denn ohne ein differenziertes „*privacy by design*" wird in der Technik eine neue Risikoquelle gesetzt. Dabei sind neben den Verantwortlichen faktisch eher die Hersteller gefragt, die gemäß EWG 78 S. 4 zur Berücksichtigung des Standes der Technik bei der Produktentwicklung „ermutigt" werden sollen. Nicht selten werden Hersteller und Verantwortlicher in Personalunion auftreten, so dass *de lege ferenda* die Haftung des Herstellers wegen eines fehlerhaften Produktes nach § 3 ProdHG bei Nichteinhaltung der „*privacy enhancing technology*"-Vorgabe denkbar wäre. Dies würde ein übergeordnetes Prinzip „*privacy by design*" voraussetzen, welches die Schutzgegenstände des ProdHG mit dem Schutz der persönlichen Informationen in § 1 ProdHG erweitern könnte. Damit könnte auch ein Anreiz zur Herstellung datenerhebungsfreier Produkte, die etwa mit einem Heimlichkeitsmodus „*Stealth Modus*" versehen werden könnten, geschaffen werden.[500]

5. Zusammenfassung

Insgesamt richtet sich die inhaltliche und organisatorische Ausgestaltung der Identitätsverwaltung nach den Datenschutzgrundsätzen aus Art. 5 Abs. 1 b) – f) DSGVO. Demnach wurden die Grundsätze der Datenverar-

498 *Raabe/Schallbruch/Steinbrück*, CR 2018, 706 (714).
499 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 25 ff.
500 *Becker*, JZ 2017, 170 (178); *Schallbruch*, CR 2016, 663 (669).

beitung für die Identitätsverwaltung konkretisiert. Dafür wurden die Zweckfestlegung, Datenminimierung, Datensicherheit und entsprechende Technikgestaltung hinsichtlich der Identitätsverwaltung untersucht. Dabei stellt die Zweckfestlegung einen zentralen Grundsatz dar, weil mit ihm die Dauer und der Umfang der Datenverarbeitung und die Erkenntnismöglichkeiten über die personalen Identitäten beschränkt werden. Demgegenüber sieht Art. 6 Abs. 4 DSGVO die Möglichkeit vor, im Laufe des Datenzyklus den Zweck zu ändern, was eine besondere Aufgabe an ein Identitätsverwaltungsmodell darstellt. Denn mit der Zweckänderung wird ein weiteres Risiko über die Erkenntnismöglichkeiten geschaffen, welches nicht mit der vorangegangenen Kontrollmöglichkeit des Betroffenen über den ersten Zweck der Datenverarbeitung übereinstimmt.

Weiter kann der Verantwortliche über den Grundsatz der Datenminimierung die Identitätsverwaltung gestalten, indem umfassende Pseudonymisierungsmethoden eingesetzt werden und gegebenenfalls über die Anonymisierungsmethoden Datensätze zu personalen Teilidentitäten aus dem Anwendungsbereich der DSGVO ausgenommen werden können. Dazu gehört, dass ein Identitätsverwaltungsmodell die Nicht-Verkettbarkeit der Datensätze gewährleisten muss, wonach der Informationsgehalt durch Verknüpfung von Daten unverändert bleiben soll. Demnach kommt eine Infrastruktur in Betracht, nach der die kontextübergreifende Verbindung von Datensätzen und personalen Identitäten in Gestalt einer Mehrfachverwendung ermöglicht wird. Entsprechend kann ein Plattformbetreiber für die Identitätsverwaltung ein Ökosystem (sog. „*Identity Ecosystem*“) begründen, welches die rechtlichen Anforderungen gerade in technischer Hinsicht umfassend umsetzt und eine Reputation über den Schutz personaler Identitäten im Markt erlangt. Folglich ist die Technikgestaltung durch den Verantwortlichen für die Realisierung der Identitätsverwaltung eine entscheidende Grundlage, zumal auf diesem Weg die Datensicherheit gewährleistet wird.

Für diese bedarf es der Sicherstellung kontextbeschränkter Datenverarbeitungsvorgänge und der Sicherheit über die Datensätze selbst. Demnach kann mit dem Stand der Technik ein Konzept begründet werden, welches einer eigenständigen technischen Gestaltung als „*identity management by design*“ unterliegen könnte. Damit würden neben dem Schutz der informationellen Selbstbestimmung die technische Anforderung des Standes der Technik gewährleistet werden. Der Betroffene wird demnach dazu befähigt, die personalen Identitäten mit einer angepassten Technologie kontrollieren zu können. Ein solches Konzept des „*identity management by design*“ müsste primär durch den Verantwortlichen umgesetzt werden,

gleichwohl erscheint die Realisierung durch den Hersteller ebenso naheliegend und wünschenswert. Dahingehend könnte *de lege ferenda* das Regelungsregime im Produkthaftungsrecht um den Schutz der informationellen Selbstbestimmung bei der Produktherstellung erweitert werden.

IV. Ergebnis

Die Identitätsverwaltung setzt bei den personenbezogenen Daten an und verlangt eine informierte Entscheidung über die Verwaltung personaler Identitäten. Demnach ist *ex ante* zur Rechtfertigung der Datenverarbeitung zu bestimmen, wann personenbezogene Daten vorliegen und wann der sachliche Anwendungsbereich der DSGVO eröffnet ist. Dabei befindet sich die Differenzierung in einer rechtlichen und tatsächlichen Grauzone, so dass in Anbetracht ubiquitärer Datenverarbeitungen innerhalb eines Datenzyklus die Identifizierungswahrscheinlichkeit hoch ist und der Theorienstreit über die Identifizierbarkeit an Bedeutung verliert.

Weiter kann mit den verarbeiteten personenbezogenen Daten das Risiko von Erkenntnissen einhergehen, so dass es gegenüber der natürlichen Person um die Transparenz über die mit der Verarbeitung verbundenen Erkenntnisrisiken geht. Diese transparent mitgeteilten Risiken sind das Ergebnis einer Risikobewertung durch den Verantwortlichen, wobei die Frage nach der geeigneten Methodik zur Risikobewertung noch offen ist, aber nach den bisherigen Untersuchungen in einer semiquantitativen Methodik liegen sollte. Folglich bedarf es über die Informationspflichten nach Art. 12, 13 DSGVO hinaus der Benennung von Risiken, damit die natürliche Person risikobewusste Entscheidungen bei der Verwaltung der personalen Identitäten treffen kann. Davon umfasst sind das Risiko der Identifizierung und das Risiko von Erkenntnissen über die natürliche Person. Bereits auf der zeitlichen Ebene vor Beginn des Datenzyklus und der Rechtfertigung erlangt die natürliche Person somit eine Kontrollmöglichkeit mit den Informationen über die Datenverarbeitung. Diese Kontrolle kann sogar als absolute Kontrolle eingeordnet werden, da diese sich in dem Lesen der Datenschutzerklärung und dem damit verbundenen Prozess der Entscheidungsfindung abbildet. Somit schließt die Identitätsverwaltung an die Transparenz der Verarbeitung personenbezogener Daten an.

Für die inhaltliche und organisatorische Ausgestaltung der Identitätsverwaltung muss der Verantwortliche die Grundsätze der Datenverarbeitung gemäß Art. 5 b) – f) DSGVO und den Stand der Technik gemäß Art. 25 DSGVO einbeziehen. Dabei dient die Zweckbindung der Beschränkung

der Datenverarbeitung und der damit verbundenen Erkenntnismöglichkeiten im Rahmen der *Instruktionen* durch den vorher festgelegten Zweck. Damit besteht eine Kontrollmöglichkeit über die Kenntnis des Zwecks, die aber mit einer späteren Zweckänderung aufgelöst werden kann. Weiter besteht nach dem Grundsatz der Datenminimierung mit den Pseudonymisierungs- und Anonymisierungsmethoden ein Schutzmechanismus gegenüber Erkenntnismöglichkeiten über personale Identitäten. Dieser Schutzmechanismus kann in einem Identitätsverwaltungsmodell dahingehend erweitert werden, dass Datensätze über personale Identitäten in einer interoperablen Struktur mehrfach verwendbar werden, sog. „*Identity Ecosystem*". Dies könnte mit einer spezifischen Konkretisierung des Standes der Technik über die Anforderung eines „*identity management by design*" umgesetzt werden.

C. Rechtfertigung der personalen Identität, Art. 6 DSGVO

Die Identitätsverwaltung bedarf der Kontrolle von personalen Teilidentitäten durch die natürliche Person, was die Rechtmäßigkeit der Datenverarbeitung zu den personalen Teilidentitäten voraussetzt. Das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt steht dem zunächst entgegen, so dass die Identitätsverwaltung das Vorliegen eines Erlaubnistatbestandes gemäß Art. 6, 5 Abs. 1 a) DSGVO voraussetzt. Basierend auf dem Phänomen ubiquitärer Datenverarbeitungen und den sich daraus ergebenden personalen Teilidentitäten, soll die Identitätsverwaltung unter dem Erlaubnisvorbehalt (I.) untersucht werden. Dabei wird die schwerpunktmäßige Kontrollmöglichkeit über die Identitätsverwaltung bei der Einwilligung (II.) liegen, so dass diese differenziert betrachtet werden soll. Denn der Einwilligung kommt eine weichenstellende Funktion zu, da mit ihr der Datenzyklus beginnt. Von der Einwilligung geht eine Serie von Erkenntnismöglichkeiten über eine personale Identität aus, die zum Gegenstand der Risikoentscheidung des Betroffenen gehören sollten.

Weiter soll die Rechtfertigung allein durch den Verantwortlichen ohne das Zutun des Betroffenen gemäß Art. 6 Abs. 1 b) – f) DSGVO der rechtfertigenden Einwilligung gegenübergestellt werden (III.) und mit einem zusammenfassenden Ausblick (IV.) auf die Identitätsverwaltung *ex post* zur Rechtfertigung abgeschlossen werden.

I. Identitätsverwaltung unter Erlaubnisvorbehalt

Die Identitätsverwaltung wurde in dem bisherigen Gang der Untersuchung als grundsätzlich umsetzbar angenommen und dem Regelungsgefüge des IKT-Rechts zugeordnet. Gleichwohl gilt im Datenschutzrecht das Verbotsprinzip mit Erlaubnisvorbehalt, welches gegen die grundsätzliche Umsetzbarkeit der Identitätsverwaltung sprechen könnte. Das Verbotsprinzip wird als „Fundamentalprinzip“[501] des Datenschutzrechts angesehen und aus dem grundrechtlichen Schutz personenbezogener Daten abgeleitet, Art. 8 Abs. 2 S. 1 GRC. Danach wird zunächst keine Differenzierung vorgenommen, ob die Datenverarbeitung im öffentlich-rechtlichen oder privatrechtlichen Kontext erfolgt. In der Anwendung der Rechtfertigungsgründe wird im öffentlich-rechtlichen Kontext das öffentliche Interesse (Art. 6 Abs. 1 e) DSGVO) maßgeblich sein. Demgegenüber werden im privatrechtlichen Kontext die Einwilligung (Art. 6 Abs. 1 a) DSGVO), das berechtigte Interesse (Art. 6 Abs. 1 f) DSGVO) und die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 c) DSGVO) durch den Verantwortlichen als Rechtfertigungsgrundlage herangezogen, wobei die Rechtfertigung aufgrund einer rechtlichen Verpflichtung ebenso im öffentlich-rechtlichen Kontext in Betracht kommt.

Im privatrechtlichen Kontext kann jedoch durch das Verbotsprinzip ein „überschießender Schutz“[502] entstehen, da jede Datenverarbeitung mit einer Einwilligung oder dem berechtigten Interesse gerechtfertigt werden müsse und dies nach der tatsächlichen Risikolage unverhältnismäßig sei. Demnach ist die Identitätsverwaltung allein in denjenigen Kontexten realisierbar, in denen eine aktive Handlung zur Rechtfertigung und *ex post* zur Rechtfertigung vorgenommen werden kann. Gleichzeitig umfasst die Identitätsverwaltung die Bewertung des mit der Datenverarbeitung verbundenen Risikos der Identifizierbarkeit und der Erkenntnismöglichkeiten, so dass sich auch auf der Ebene der Rechtfertigung die Frage nach dem Wirkungsgrad des risikobasierten Ansatzes stellt. Indem die Entscheidung über die Begründung der Rechtfertigungsgrundlage durch den Verantwortlichen erfolgt, muss dieser auch die kontextspezifische Risikobewertung über die Datenverarbeitung vornehmen, so dass der risikobasierte Ansatz auch auf der Rechtfertigungsebene seine Wirkung entfaltet.

---

501 *Spiecker gen. Döhmann*, in: Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, 263 (271).

502 *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 84.

Im Rahmen der Bestimmung des Rechtfertigungsgrundes für den Datenverarbeitungsprozess werden der verfolgte Zweck und die Risiken der Datenverarbeitung gegenübergestellt. Dabei geht es im privatrechtlichen Kontext um den Rechtfertigungsgrund der Einwilligung und dem berechtigten Interesse. In diesem Vorgang kann ein Paradigmenwechsel gesehen werden, der sich von einem „rigiden Verbotsprinzip“[503] abwendet und dem risikobasierten Ansatz zuwendet, damit sich die prohibitive Wirkung des Verbotsvorbehalts in der Bestimmung des Rechtfertigungsgrundes verwirkliche. Darin kann eine Prozeduralisierung des Verbotsprinzips in Gestalt einer risikobasierten Bewertung gesehen werden, worin die datenschutzrechtlichen Regelungen ihre Vereinigung im Vorgang der Maßnahmen- und Rechtfertigungsbestimmung fänden.[504] Dieser prozedurale Anteil des Verbotsprinzips soll als ein wesentlicher Bestandteil für das Identitätsverwaltungsmodell herangezogen werden, um den Schwerpunkt auf die prozedurale Dimension der Identitätsverwaltung zu setzen und den dynamischen *Ipse*-Anteil personaler Identitäten zu gewährleisten.

Mit der Geltung des Verbotsprinzips für den privatrechtlichen Kontext werde zudem das strukturelle Ungleichgewicht zwischen dem Betroffenen und dem Verantwortlichen nicht ausgeglichen, sondern vielmehr werde die bestehende Marktmacht des Verantwortlichen zementiert.[505] Entsprechend schlägt *Masing* für die Datenverarbeitung im privatrechtlichen Kontext die Umkehr des Verbotsvorbehalts in die Begründung von Ausgestaltungsspielräumen vor.[506] Folglich erscheint der Gleichlauf des grundrechtlichen Schutzumfangs mit dem Verbotsvorbehalt für den privatrechtlichen und öffentlich-rechtlichen Kontext in Anbetracht des geringeren Schutzumfanges über die mittelbare Drittwirkung der Grundrechte als fragwürdig. Demnach ist die risikobasierte Rechtfertigung im privatrechtlichen Kontext als konsequente Anpassung an die grundrechtliche Differenzierung zwischen der Abwehrdimension gegenüber dem Staat und der mittelbaren Drittwirkung anzusehen. Mit einer Abkehr vom rigiden Verbots-

503 *Quelle*, European Journal of Risk Regulation 2018, 502 (517); *Veil*, ZD 2015, 347.

504 *Dies.*, European Journal of Risk Regulation 2018, 502 (521 f.).

505 *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 85; *Roßnagel*, NJW 2019, 1 (5); *DeHert/Gutwirth*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 61 (77 f.)

506 *Masing*, NJW 2012, 2305 (2307 f.); *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 6 DSGVO Rn. 14; zur kritischen Betrachtung der Legitimationswirkung, *Kühling/Klar/Sackmann*, Datenschutzrecht, 2018, Rn. 495.

prinzip kann auch dem Eindruck begegnet werden, dass mit der rechtfertigenden Einwilligung im privatrechtlichen Kontext eine Kontrollmöglichkeit über die *Ipse-* und *Idem-*Anteile einer personalen Identität besteht. Damit ist eine risikobasierte Öffnung für Gestaltungsspielräume zur Identitätsverwaltung denkbar, in der der Schutz vor Erkenntnismöglichkeiten einbezogen wird. Demnach ist im privatrechtlichen Kontext eine Abkehr von einem rigiden Verbotsprinzip und eine Hinwendung zu einer differenzierten Ausgestaltung der Kontrollmöglichkeiten des Betroffenen im Datenzyklus wünschenswert und kann mit der Identitätsverwaltung erfolgen.

Für die Identitätsverwaltung unter dem Erlaubnisvorbehalt erstreckt sich das Schutzkonzept auf die Verwaltung der Risiken aus den Datenverarbeitungen. Dabei ist für den privatrechtlichen Kontext der Rechtfertigungsgrund der Einwilligung hervorzuheben. Mit ihm gehen das Konzept der Kontrolle über die (risiko-) bewusste Entscheidung zur Einwilligung in die Datenverarbeitung und das Risiko von Erkenntnissen über personale Identitäten einher. Weiter kann in der Einwilligung der Schlüssel zur Identitätsverwaltung gesehen werden, mit dem die personalen Identitäten zu Beginn des Datenzyklus begründet werden und sich im Verlauf des Datenzyklus vielfältige Erkenntnismöglichkeiten ergeben. Gleichwohl wird im privatrechtlichen Kontext die Rechtfertigung mit dem berechtigten Interesse erfolgen können, so dass auch ohne aktive Handlung der Datenzyklus von personalen Identitäten ausgelöst werden kann und eine Kontrollmöglichkeit erst *ex post* zur Rechtfertigung besteht.

II. Identitätsverwaltung durch Einwilligung, Art. 6 Abs. 1 a), 7 DSGVO

Die Entscheidung zur Einwilligungserteilung mit der Folge, dass personale Teilidentitäten in ihren *Idem-* und *Ipse-*Anteilen begründet und verwendet werden, stellt einen zentralen Bestandteil der Identitätsverwaltung und des Selbstdatenschutzes dar. Die Einwilligung unterliegt primärrechtlichem Schutz gemäß Art. 8 Abs. 2 S. 1 GRC und ist zentral in der Grundrechtsausübung, so dass deren Vorliegen an strenge Voraussetzungen gebunden ist. Danach bedarf es einer informierten freiwilligen Entscheidung durch den Betroffenen, in der die individuellen Präferenzen etwa über die Risikobereitschaft zu der Verarbeitung personenbezogener Daten einfließen können. Die Rechtsnatur der Einwilligung gleicht einer rechtsgeschäftlichen Erklärung und unterliegt Bestimmtheitsanforderungen, die sich auf

die Informationen und den Zweck der Datenverarbeitung beziehen.[507] Somit liegt in der Einwilligung zu einem frühen Zeitpunkt des Datenzyklus eine weichenstellende Funktion vor, da sich in ihr vielfältige Erkenntnismöglichkeiten über die personale Identität innerhalb eines Datenzyklus bündeln können und diese Gegenstand der Risikoabwägungen des Betroffenen werden sollten.

Sobald die Einwilligung erfolgt ist, wird die Datenverarbeitung durch den Verantwortlichen gerechtfertigt, so dass in der Einwilligung zunächst die absolute Kontrolle zum Ausdruck kommt und diese in eine relative Kontrolle gegenüber dem Verantwortlichen durch das begründete Kommunikationsverhältnis übergeht. Dies umfasst die Entscheidung des Betroffenen über die Verarbeitung der personenbezogenen Daten und die bevorstehenden Erkenntnismöglichkeiten des Verantwortlichen über die personale Identität infolge der Datenverarbeitung. Weiter geht mit der Einwilligung eine relative Kontrolle einher, in der auch ein „Verzicht über die Herrschaft und Kontrolle der Daten“[508] gesehen wird und diese mit der Einwilligung legitimiert werde. Dabei ist der „Herrschaftsverzicht“ mit der Einwilligung in rechtsdogmatischer Hinsicht jedoch dahingehend umstritten, ob es sich bei der Einwilligung um eine Rechtfertigung des Eingriffs handelt oder ob schon gar kein Eingriff vorliege.[509] Gleichwohl bleibt aus der weitreichenden Wirkung der Einwilligung das Fortbestehen eines Schutzbedarfs nach Einwilligungserteilung festzustellen.

Gerade im privatrechtlichen Kontext fungiert die Einwilligung als Primat[510] für umfangreiche Datenverarbeitungsprozesse, indem sie einen ausgeprägten Wirkmechanismus für den Datenzyklus der personalen Identität entfaltet. Folglich sollen für das Identitätsverwaltungsmodell die informierte freiwillige Einwilligung (1.), sowie das Verhältnis des AGB-Rechts zur Einwilligung (2.) analysiert werden und eine prozedural geprägte Betrachtung der Einwilligung (3.) vorgenommen werden. Anschließend soll

507 Der Streit über die Rechtsnatur der Einwilligung als rechtsgeschäftliche Willenserklärung oder als geschäftsähnliche Handlung ist für die Identitätsverwaltung nicht maßgebend, sondern allein die Feststellung, dass der Datenzyklus zu einer personalen Identität mit der Einwilligung beginnt. Demnach erscheint das Konzept der antizipierten Erlaubnis als rechtserhebliche Handlung *sui generis* für das Identitätsverwaltungsmodell naheliegend zu sein *Buchner/Kühling*, in: dies. (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 7 DSGVO Rn. 1a, 61.

508 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 77.

509 *Knecht*, in: Schwarze/Becker/Hatje u.a. (Hrsg.), EU-Kommentar, 2019, Art. 8 GRC Rn. 3.

510 *Veil*, NVwZ 2018, 686 (688).

der Frage nach dem Bedarf einer paternalistischen Intervention (4.) nachgegangen werden.

1. Informierte freiwillige Einwilligung, Art. 7 DSGVO

Die informierte freiwillige Einwilligung lässt sich nunmehr unter erleichterten Bedingungen erteilen. Gemäß Art. 4 Nr. 11 DSGVO setzt die Einwilligung eine in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung voraus, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Im Gegensatz zur alten Rechtslage gemäß § 4a BDSG a.F. BDSG, die ein Schriftformgebot[511] voraussetzte, sind nunmehr die mündliche Einwilligung und die Einwilligung durch schlüssiges Verhalten für die Rechtfertigung der Datenverarbeitung ausreichend, Art. 6 Abs. 1 a), 7 DSGVO, EWG 43, 42 S. 5. Dies hatte zur Folge, dass mit dem Schriftformgebot der Bedarf nach einer schriftlichen Einwilligung in manueller oder technischer Gestalt einherging und dies zu einem Medienbruch führen konnte. Nach der DSGVO lässt sich jedoch die Einbeziehung einer ausdrücklichen Einwilligungsabfrage aufgrund der niedrigeren Einwilligungsanforderungen vermeiden. Gleichwohl bedarf es einer „unmissverständlich abgegebene(n) Willensbekundung" gemäß Art. 4 Nr. 11 DSGVO in einer Erklärung, die von dem Verantwortlichen gemäß Art. 5 Abs. 2 DSGVO dokumentiert wird.[512]

Demgegenüber wird bei der Verarbeitung besonderer Kategorien personenbezogener Daten aufgrund des gesteigerten Risikos für die Rechte und Freiheiten natürlicher Personen eine explizite Einwilligung gemäß Art. 9 Abs. 1 DSGVO verlangt, da aufgrund der „informationellen Diskriminie-

511 Das Schriftformgebot ist nunmehr in § 26 Abs. 2 S. 3 BDSG für eine spezifische Anhebung des Schutzniveaus im Beschäftigendatenschutzrecht geregelt. Jedoch wird darin ein Widerspruch zu Art. 7, 4 Nr. 11 DSGVO gesehen. Denn der Zweck der DSGVO, das Schutzniveau in den Mitgliedstaaten zu harmonisieren, könne nur entsprochen werden, wenn die nationale Regelung in § 26 Abs. 2 S. 2 BDSG teleologisch reduziert werde, vgl. *Maschmann*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, § 26 BDSG Rn. 64.

512 *DSK*, Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DS-GVO, 22.02.2019, S. 2.

rungsverbote“[513] ein gesteigertes Risiko für den Schutz der personalen Identitäten besteht. Mit dem Erfordernis einer expliziten Einwilligung wird ein gesteigertes Bewusstsein für die Einwilligung vorausgesetzt, damit der Betroffene über die potentiell diskriminierenden Auswirkungen und die Erkenntnismöglichkeiten entscheiden kann. Entsprechend könnten die Anforderungen an die Einwilligung erweitert werden mit einer vorherigen fachkundigen Beratung, einer bestimmten Bedenkzeit oder den Formerfordernissen,[514] die sich in einem Identitätsverwaltungsmodell verwirklichen können. Insbesondere kommt für die Identitätsverwaltung die Einrichtung eines elektronischen Substituts der Einwilligung in Betracht, welches über eine elektronische Signatur oder PIN-Eingabe für die Einwilligungserklärung erfolgen könnte.[515] Diese elektronische Einwilligung hätte den Vorteil, dass die Dokumentations- und Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO automatisiert gewährleistet werden könnten, indem mit einem Zeitstempel die Erteilung der Einwilligung und der Zeitpunkt eindeutig feststellbar wären und zu einer erleichterten Beweisführung beitragen könnten.

Die Einwilligung stellt eine omnipräsente Rechtfertigungsmöglichkeit dar und zugleich ist eine hohe Bereitschaft bei den Betroffenen erkennbar, die Einwilligung schnell zu erteilen, so dass „die Bürger, matt vom Nicken, zu allem Ja sagen(d)“[516] die Einwilligung erteilen.[517] Somit liegt in dem Phänomen der faktisch bereitwilligen Einwilligungserteilung des Betroffenen eine Freigabe der personalen Identitäten in ihren *Idem*- und *Ipse*-Anteilen an den Verantwortlichen, dem ein effektives und wirksames Sanktionssystem gegenüberstehen müsste. Denn die Einwilligung als zentrales Instrument der informationellen Selbstbestimmung muss den rechtlichen Anforderungen gerecht werden, was mit dem Sanktionssystem gemäß Art. 83 DSGVO möglich ist.

Neben dem Sanktionssystem zur Gewährleistung der informierten freiwilligen Einwilligung könnte die interdisziplinäre Analyse der Einwilligung erhellend sein, um weitere Anhaltspunkte für einen effektiven Me-

513 *Weichert*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 9 DSGVO Rn. 1, 13.

514 *Ders.*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 9 DSGVO Rn. 47 f.

515 *Raabe/Lorenz*, DuD 2011, 279 (283).

516 *Wieduwilt*, FAZ vom 20.10.2018, 17.

517 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, F 99; *Hoffmann-Riem*, AöR 142 (2017), 1 (22); *Radlanski*, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016, S. 79.

chanismus in einem Identitätsverwaltungsmodell erlangen zu können. Denn mit der bereitwilligen Erteilung einer rechtfertigenden Einwilligung könnte ein legitimatorisches Defizit einhergehen, welches in einem unzureichenden Bewusstsein zum Zeitpunkt der Einwilligungserteilung über die personalen Identitäten und die Erkenntnismöglichkeiten im Rahmen des Datenzyklus liegt. Für eine nähere Analyse dieser Sachlage soll die *verhaltensökonomische Perspektive* herangezogen werden, um die Annahme einer rationalen Kosten-Nutzen-Analyse bei der Einwilligungserteilung näher untersuchen zu können. Denn es kann die Ansicht vertreten werden, dass neben der Kosten-Nutzen-Analyse aufgrund der Informationspflichten gemäß Art. 12–14 DSGVO die Entscheidung des Betroffenen von weiteren inneren und äußeren Entscheidungsfaktoren geprägt ist und Verzerrungen unterliegt. Diese möglichen Verzerrungen in der Entscheidungsfindung sollen für den Schutz der informationellen Selbstbestimmung in das Identitätsverwaltungsmodell einbezogen werden. Dafür soll zunächst die verhaltensökonomische Betrachtung motiviert (a), sowie die Einwilligung in ihren endogenen (b) und exogenen (c) Faktoren der Entscheidungsfindung in Frage gestellt werden, um anschließend die Ergebnisse auf das „*Privacy Paradox*" (d) und die Identitätsverwaltung (e) zu übertragen.

a) Motivation

Die Phänomenologie der Einwilligung als tatsächliche Verhaltensweise soll in der weiteren Untersuchung vertieft analysiert werden. Denn es könnte der rechtlichen Intention einer informierten freiwilligen Einwilligung, den Maßgaben gemäß Art. 6, 7 DSGVO folgend, eine Realität gegenüberstehen, die gerade keine bewusste informierte Entscheidung darstellt. Die beschriebenen Phänomene einer hohen Einwilligungsbereitschaft können als Indiz gewertet werden, dass eine umfassende oder nur minimale Kosten-Nutzen-Analyse durch den Betroffenen nicht immer erfolgt. Damit erscheint die tatbestandlich vorausgesetzte bewusste und rationale Einwilligung zumindest fragwürdig. Denn aufgrund von direkten Netzwerkeffekten und der Omnipräsenz von Einwilligungsabfragen kann die bewusste und freiwillige Entscheidungsfindung in hohem Maß von äußeren Faktoren beeinflusst werden. Hinzu kommt, dass die Verhandlungsmacht zwischen dem Verantwortlichen und der betroffenen Person ungleich verteilt ist, so dass die Einwilligung im B2C-Kontext besondere Aufmerksamkeit für die Identitätsverwaltung verlangt.

In dem Identitätsverwaltungsmodell bedarf es der Gewährleistung einer freiwilligen Kontrolle personaler Identitäten gerade bei bestehenden Verhandlungsungleichgewichten, EWG 43 S. 1. Denn die Identitätsverwaltung verwirklicht den Schutz der personalen Identität in ihren *Idem-* und *Ipse*-Anteilen, wenn die Entscheidungsfindung von den Anforderungen an die Freiwilligkeit gedeckt ist und die Einwilligung effektiv realisiert werden kann, da nur mit einer tatsächlich freiwilligen Entscheidung der *Selbstdatenschutz* verwirklicht wird. Für die Analyse der Voraussetzungen eines wirksamen *Selbstdatenschutzes* mit der Einwilligung bedarf es daher der Einbeziehung verhaltensökonomischer Betrachtungen, um einen umfassenden Schutzmechanismus ableiten zu können.

b) Endogene Faktoren der Entscheidungsfindung

Die Einwilligung wird durch Faktoren beeinflusst, die im Inneren des Betroffenen liegen und auf individuellen Präferenzen und Überlegungen beruhen. Zu diesen endogenen Entscheidungsfaktoren gehört der „*Rational Choice*"-Ansatz (aa), der als theoretische Grundlage für die Willensbildung fungiert und anschließend mit der Darstellung der neuen Erwartungstheorie („*Prospect-Theory*") ergänzt werden soll (bb). Mit der „*Prospect-Theory*" erfährt der „*Rational Choice*"-Ansatz eine Erweiterung, so dass abschließend beide Theorien für das Identitätsverwaltungsmodell ausgewertet werden sollen (cc).

aa) „Rational Choice"-Ansatz

Die Entscheidungsfindung bei der Einwilligung stellt eine freiwillige und bewusste dem „*Rational Choice*"-Ansatz („*Utility Theory*"[518]) unterliegende Handlung dar. Dabei verfolge die Entscheidungsfindung ein bestimmtes Ziel, welches dem Kosten-Nutzen-Kalkül eines wirtschaftlich handelnden „*homo oeconomicus*" entspricht.[519] Demnach müsste sich der Betroffene mit dem Nutzen und damit einem Zustand der Vorteile und Nachteile seiner Entscheidung auseinandersetzen. Weiter müsste der Betroffene über die

518 *Kahneman/Tversky*, Econometrica 1979, 263.

519 *Eidenmüller*, JZ 2011, 814 (816 f.); von einer „approximativen Rationalität" ausgehend, vgl. *Glöckner*, in: Funke/Schmolke (Hrsg.), Menschenbilder im Recht, 2019, 79 (81).

Risiken seiner Entscheidung eine bewusste Kosten-Nutzen-Abwägung vornehmen, die zur Grundlage der bewussten freiwilligen Einwilligung wird. Von dieser Entscheidungsfindung müssten die Erkenntnismöglichkeiten über eine personale Identität erfasst sein, die der Verantwortliche infolge der Datenverarbeitung erlangen kann. Auch könnten individuelle Präferenzen des Betroffenen zum Schutz der informationellen Selbstbestimmung in die Kosten-Nutzen-Analyse einfließen, was sie zu einer zeit- und kontextbezogenen Entscheidung und Prognose über die Folgen der Einwilligung macht. Denn die individuellen Präferenzen über den Schutz der personenbezogenen Daten sind situativ und neigen dazu, unvollständig zu sein, so dass eine abschließende Abwägung über die Risiken gegenüber der informationellen Selbstbestimmung ausgeschlossen werden könne und ein rationales Kosten-Nutzen-Kalkül in Frage gestellt werden müsse.[520]

Für eine abschließende Abwägung des Betroffenen kommt hinzu, dass der Entscheidungsgegenstand der informationellen Selbstbestimmung einer hohen Komplexität unterliegt und daher eine umfassende Kosten-Nutzen-Analyse und rationale Entscheidung kaum erwartet werden könne.[521] Vielmehr können endogene Faktoren zu *kognitiven Verzerrungen* der individuellen Präferenzen führen und die Entscheidung über die Einwilligung beeinflussen. Dazu gehöre, dass der Betroffene risikoaffin oder risikoavers sein könne, welches sich über den „*Rational Choice*"-Ansatz durch die fehlende Auswirkung auf das Abwägungsergebnis nicht abbilden ließe.[522] Damit kann in dem „*Rational Choice*"-Ansatz eine Vermutung über das Entscheidungsverhalten gesehen werden, so dass sich die Frage nach der Einbeziehung der durchgeführten psychologischen und empirischen Untersuchungen in der Verhaltensökonomie stellt.[523]

Es lässt sich aufgrund des *Big Data*-Phänomens mit der bereitwilligen Erteilung von Einwilligungen und den damit einhergehenden Risiken über die vielfachen Erkenntnismöglichkeiten die Frage nach den Ursachen dafür stellen. Folglich seien die Untersuchungen von *Acquisti* angeführt, nach denen sich die „*Rational Choice*"-Entscheidungen im Zusammenhang mit der informationellen Selbstbestimmung anzweifeln und mit Modellen zu den psychologischen Verzerrungen präziser beschreiben lassen.[524] Dem-

520 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 130 f.
521 *Solove*, Harv. L. R. 2013, 1880 (1897).
522 *Kahneman/Tversky*, Econometrica 1979, 263 (285).
523 *Van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (189 f).
524 *Acquisti*, ACM 2004, 21.

nach konnte nachgewiesen werden, dass die rationale Entscheidung von einer kontextbezogenen sog. „*Privatheitskurzsichtigkeit*" geprägt sei und den umfassenden Schutz der Privatheit nicht gewährleisten könne.[525] Somit bedarf es für das Identitätsverwaltungsmodell der Einbeziehung kontextspezifischer Entscheidungsfaktoren, um einen umfassenden Schutz der personalen Identität und der damit verbundenen Erkenntnismöglichkeiten im Datenzyklus gewährleisten zu können. Dabei geht es um die Bestimmung derjenigen Faktoren, die die Entscheidungsfindung endogen beeinflussen können und zu einer möglichst umfassenden Entscheidung über die Einwilligungserteilung führen. Dafür können die maßgeblichen Faktoren nach der neuen Erwartungstheorie aufschlussreich sein.

bb) „Prospect Theory"- Neue Erwartungstheorie[526]

In der Verhaltensökonomie wird der „*Rational Choice*"-Ansatz mit der „*Prospect Theory*" als neue Erwartungstheorie erweitert und damit ein der Realität näherkommendes Modell über die individuelle Entscheidungsfindung dargelegt. Dieses unterscheidet zwischen der rationalen Motivation und dem tatsächlichen Verhalten des Betroffenen.[527] Demnach geht es nicht mehr um den Nutzen, sondern um die Erwartungen des Betroffenen.[528] Die maßgebliche Frage liege vielmehr darin, was sich mit der Entscheidung verändern würde und weniger in dem statischen Nutzen.[529]

Dabei wird von *Kahnemann* zwischen System 1 und System 2 differenziert: Das System 1, welches mühelos und ohne willentliche Steuerung als erinnerndes Selbst im Unterbewusstsein arbeitet und unwillkürlich über die vermeintlich rationalen Entscheidungen von System 2 herrscht. Demgegenüber geht das System 2 davon aus, dass es eine „*Rational Choice*"- Entscheidung treffe, ohne die tatsächlichen Wirkungen von System 1 wahrzunehmen.[530] Dies könne dazu führen, dass der Betroffene gegenüber dem Offensichtlichen blind sei und kein Bewusstsein über die Blindheit bestünde, auch wenn eine hohe Aufmerksamkeit aufgebracht werde.[531] Demnach

525 *Ders.*, ACM 2004, 21 (22).
526 *Kahneman/Tversky*, Econometrica 1979, 263.
527 *Van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (191).
528 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 348.
529 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 344.
530 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 33.
531 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 37.

könne in der rationalen Entscheidungsfindung bei hoher Auslastung des bewusstseinsgesteuerten Systems 2, die Entscheidung faktisch durch unwillkürliche Faktoren von System 1 getroffen werden, so dass „*to pay attention*" sprichwörtlich verstanden werden müsse.[532] Damit wird die Aufmerksamkeit aus System 2 von unwillkürlichen Faktoren des Systems 1 verdrängt. Daraus schließt *Kahnemann* sogar eine „Tyrannei des erinnernden Selbst" von System 1 und beschreibt das erinnernde Selbst als „Fremden".[533] Folglich ergibt sich der Differenzierungsbedarf des Entscheidungsprozesses, der auf den Erinnerungen und vergangenheitsgeprägten Erfahrungen basiert und zum Gegenstand der Aufmerksamkeit wird.

Für die Einwilligung stellt sich demnach die Frage, ob sich die Aufmerksamkeit bei der Einwilligungserteilung tatsächlich auf die Abwägung der Kosten und Nutzen für die informationelle Selbstbestimmung richtet oder die Aufmerksamkeit von der Darstellung und den mit einer bevorstehenden Datenverarbeitung verbundenen Gratifikationen absorbiert wird. Denn die ursprüngliche Anforderung des Schriftformgebots an die Einwilligung gemäß § 4a Abs. 1 S. 3 BDSG a. F. hatte für den Betroffenen die Warn-, Beweis- und Kontrollfunktion, so dass der Betroffene auf mehreren Ebenen eine Abwägung und damit eine von System 2 getragene Entscheidung treffen konnte. Nunmehr sieht Art. 6 Abs. 1 a), Art. 4 Nr. 11 DSGVO vor, dass die Einwilligung ohne Formerfordernis als „unmissverständlich abgegebene Willensbekundung" erkennbar sein muss und somit konkludent erteilt werden kann. Diese Abschwächung der Einwilligungsanforderungen wirkt sich auf die Ausübung der Einwilligung dahingehend aus, dass bereits mit der Nutzung eines Dienstes die Einwilligung konkludent erteilt und diese Entscheidung möglicherweise weniger von System 2 als von System 1 getragen wird. Der Anreiz, den Dienst unmittelbar nutzen zu können, wird von System 1 ausgelöst und weniger von einer Kosten-Nutzen-Analyse des Systems 2 getragen. Demnach erleichtern die Einwilliguganforderungen nach der DSGVO eine von System 1 getragene Entscheidung. Gleichwohl ist nicht auszuschließen, dass Rahmenbedingungen und die Darstellung der Informationspflichten derart ausgestaltet werden, dass ein Anreiz für eine von System 2 getragene Entscheidung über die Datenverarbeitung geschaffen wird.

Im Einzelnen können insbesondere „*Priming*"-Effekte, „*Framing*"- und *Ankereffekte* die Entscheidungsfindung beeinflussen und zum Gegenstand der Rahmenbedingungen und der Darstellung von Informationspflichten

532 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 58.
533 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 470–480.

für die Einwilligungserteilung werden. Durch „*Priming*"-Effekte erfolgt etwa mit dem ersten Wort, dem ersten Verhalten oder der technischen Einstellung die Bahnung der Aufmerksamkeit in die Richtung einer bestimmten Assoziationskette, was über System 1 erfolge.[534] Durch „*Priming*"-Effekte wird eine Überbewertung des ersten Informationsgegenstandes gegenüber den darauf folgenden Informationen ausgelöst, so dass Chancen und Risiken fehlinterpretiert werden können.[535] Ebenso kann die Entscheidungsfindung durch *Ankereffekte* beeinflusst werden, die dem „*Priming*"-*Effekt* sehr nahe sind. Danach lösen die Ankereffekte bei System 1 und System 2 einen Anknüpfungspunkt aus, an den sich alle folgenden Einschätzungen richten. Folglich wird bei der Verhandlung eines Preises das erste Angebot die weiteren Preisvorschläge maßgeblich beeinflussen. Daraus ergibt sich, dass die Unabhängigkeit der Folgeverhandlung von dem ersten Gebot überschätzt und die intuitive Wirkung des ersten Angebotes auf die Folgeverhandlung unterschätzt werde.[536] Mit „*Framing*"-*Effekten* wird entsprechend der Begrifflichkeit ein Rahmen für die folgenden Assoziationen und Vorstellungen erweckt.[537] Demnach beeinflusst die Begriffswahl den Rahmen der Assoziationen bei der Entscheidungsfindung, so dass der Gestaltung der Informationspflichten und der damit auslösbaren Assoziationsketten bei dem Betroffenen eine entscheidende Bedeutung in der Einwilligungserteilung zukommt.

Für die Identitätsverwaltung können sich diese Befunde auf die Gestaltung der Informationspflichten durch den Verantwortlichen auswirken. Danach können Ankereffekte über die wahrnehmbaren Informationen in dem Sinne wirken, dass „*What you see is all there is*" – „WYSIATI" – Entscheidungen zu voreiligen Schlussfolgerungen und Urteilssprüngen verleiten können.[538] Denn die „WYSIATI"-Regel führe zu der Gewichtung von Faktoren, die Wahrnehmungsgegenstand sind und blenden weniger offensichtliche Faktoren aus, so dass eine kontextabhängige Fokussierungsillusion entstehen könne.[539] Demnach kann bei der Entscheidungsfindung im Rahmen der informationellen Selbstbestimmung das Risiko eines Schadenseintritts oder ein Risikokriterium außerhalb der Wahrnehmung des Betroffenen liegen, obwohl diese Faktoren in der Entscheidungsfindung

534 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 72 f.
535 *Kahneman/Tversky*, Econometrica 1979, 263.
536 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 152–163.
537 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 447–450.
538 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 112 f.
539 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 497.

relevant sein müssten. Ebenso können Faktoren bei der Entscheidungsfindung einbezogen werden, die irrelevant sind und sich auf die Risikobewertung nicht auswirken können. Damit beruhen Entscheidungen nach der „*Prospect Theory*" auf der Illusion der umfassenden Gültigkeit einer Entscheidung, obwohl sie faktisch allein kontextbezogene Gültigkeit haben und auf irrelevanten Faktoren oder Bewertungen beruhen können.[540] Diese Problematik könne aufgelöst werden, wenn subjektive Risikobewertungen mit einem Verfahren derart modifiziert würden, dass diese nicht den „*Priming*"-, Anker-[541] und den „*Framing*"-Effekten unterliegen. Ein solches Verfahren könnte als ein gestuftes Verfahren ausgestaltet werden, in dem einzelne Merkmale separat bewertet werden und anschließend in eine Gesamtbewertung überführt werden können.[542]

Indem die erste datenschutzrechtliche Phase zwischen dem Betroffenen und Verantwortlichen über die Informationspflichten in der Datenschutzerklärung für die Entscheidungsfindung maßgeblich ist, müsste diese in dem Identitätsverwaltungsmodell differenziert einbezogen werden. Denn die Einwilligungsentscheidung ist von der Mühelosigkeit des Systems 1 geprägt, so dass die Generierung von personalen Identitäten nur einer eingeschränkten Rationalität unterliegt. Dieses Phänomen könnte zu der Annahme eines legitimatorischen Defizits bei der Einwilligung führen und eines eigenen Verfahrens zur Kompensation der eingeschränkt rationalen Entscheidung bedürfen. Weiter kann sich das Entscheidungsergebnis auf den gesamten Datenzyklus der personalen Identität auswirken, so dass der Einwilligungsvorgang im Identitätsverwaltungsmodell in einem separaten Verfahren aufgegliedert werden sollte. Mit einer Prozeduralisierung der Einwilligung in ein gestuftes Verfahren würde ein weitergehender Schutz für die personale Identität gewährleistet werden können.

cc) Bewertung

Die endogenen Faktoren wirken sich auf die Entscheidungsfindung und damit die Einwilligung aus, so dass die Annahme der rein rationalen Entscheidung für ein Identitätsverwaltungsmodell modifiziert werden muss. Dazu könnte die Differenzierung der Phase *ax ante* zur Rechtfertigung und der rechtfertigenden Einwilligung in weitere Iterationen gehören, mit

---

540 *Ders.*, Schnelles Denken, langsames Denken, 2012, S. 262.
541 *Tversky/Kahneman*, Science 1974, 1124 (1129).
542 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 287.

der die Datenschutzerklärung in den Fokus rückt. Es kommt das Konzept einer iterativen und geschichteten Einwilligung, sog. „*layered approach*" in Betracht, bei der eine konkretisierte Einwilligung etwa auf kontextspezifische Risikofaktoren abgegeben werden könnte. Dem steht gegenüber, dass das empirisch nachgewiesene Interesse an unmittelbaren Gratifikationen zu einem „Abnicken" der einzelnen Einwilligungsabfragen führen könnte. Gleichwohl könnten die „*Priming*"-, Anker- und „*Framing*"-Effekte dazu eingesetzt werden, eine kontextspezifische bewusste Entscheidung über die Risiken für die personale Identität zu fördern. Demnach ist eine informierte freiwillige Einwilligung als „*layered approach*" unter Einbeziehung der verhaltensökonomischen Erkenntnisse dazu geeignet, das Legitimationsdefizit der Einwilligung zu kompensieren und in einem Identitätsverwaltungsmodell eingesetzt zu werden.

Insgesamt kommt der Datenschutzerklärung in ihrer inhaltlichen Ausrichtung und Darstellung besonderes Gewicht zu, denn mit ihr könnte der inhaltliche Hinweis auf die verhaltensökonomischen Verzerrungsfaktoren vorgenommen werden. Zwar ist dies an sich Gegenstand der Warn-, Beweis- und Kontrollfunktion des Schriftformgebotes, wie es gemäß § 4a Abs. 1 S. 3 BDSG a. F. vorausgesetzt wurde, aber nunmehr unterliegt die Einwilligungserteilung gemäß Art. 6 Abs. 1 a), 4 Nr. 11 DSGVO erleichterten Bedingungen, was eine Verschiebung zu einer Entscheidungsdominanz durch System 1 zur Folge haben kann. Folglich sollten die verhaltensökonomischen Verzerrungsfaktoren in die Informationspflichten und in die Rahmenbedingung der Entscheidungsfindung aufgenommen werden. Diese Konzeption hätte den Vorteil, dass die endogenen Entscheidungsfaktoren in die bewusste Entscheidungsfindung einbezogen und die Wahrnehmungsverzerrungen minimiert werden könnten. Eine derartige Wirkung ist in manchen Kontexten denkbar, gleichzeitig wurde festgestellt, dass Datenschutzerklärungen nicht immer zur Kenntnis genommen werden, so dass eine paternalistische Intervention in Betracht kommt. Hierbei erscheint im Rahmen der Gestaltung des Identitätsverwaltungsmodells ein weiches paternalistisches Konzept[543] auf der technischen Gestaltungsebene für die Förderung der Entscheidungsfindung naheliegend. Damit könnte eine kontextspezifische Bewusstseinsförderung über die Risiken für die personalen Identitäten und die Erkenntnismöglichkeiten über diese gestaltet werden. Zudem würde dem legitimatorischen Defizit infolge einer fehlenden, überwiegend rationalen Entscheidung in einem Identi-

543 *Brandimarte/Acquisti*, in: Peitz/Waldfogel (Hrsg.), The Oxford Handbook of the Digital Economy, 2012, S. 564.

tätsverwaltungsmodell mit einer gestuften Prozeduralisierung der Einwilligung Rechnung getragen werden können.

c) Exogene Faktoren der Entscheidungsfindung

Ebenso kann die Einwilligung durch äußere Faktoren beeinflusst werden, die in dem Verantwortungsbereich des Verantwortlichen oder in dem Verhalten mehrerer Nutzer liegen. Zunächst kommt als exogener Faktor der Entscheidungsbeeinflussung die Verbindung der datenschutzrechtlichen Einwilligung mit einer vertraglichen Angebotsannahme über das Koppelungsverbot (aa) in Frage und anschließend die Beeinflussung des Betroffenen durch Algorithmen und Netzwerkeffekte (bb).

aa) Koppelungstatbestand, Art. 7 Abs. 4 DSGVO

Die freiwillige Erteilung der Einwilligung kann in direkter Verbindung zu einem verfolgten Vertragszweck stehen, so dass dieser als exogener Faktor die Erteilung der Einwilligung beeinflusst. Durch den Koppelungstatbestand gemäß Art. 7 Abs. 4 DSGVO[544] soll bei der Beurteilung der Freiwilligkeit dem Umstand der Abhängigkeit von einem Vertragsschluss Rechnung getragen werden. Indem die Einwilligung bei einem gleichzeitigen Vertragsabschluss zu einem bloßen Formalismus verkommen und die Grundrechtsausübung mit der Einwilligung faktisch unterlaufen werden kann, kommt dem Koppelungstatbestand eine besondere Bedeutung zu.

Gemäß Art. 7 Abs. 4 DSGVO würde es an einer freiwilligen Einwilligung fehlen, wenn die Monopolstellung ausgenutzt und die Einwilligung allein aufgrund der ausgeprägten Abhängigkeit erteilt werde.[545] Dabei kann die Rechtsbeziehung derart ausgestaltet sein, dass die Einwilligung faktisch als Bedingung des Vertragsschlusses fungiert, so dass eine echte Wahlmöglichkeit ausgeschlossen ist und die Verweigerung der Einwilligung mit dem Nachteil verbunden wäre, keinen Vertrag abschliessen zu

544 Entsprechend im Telekommunikationsrecht ist der Koppelungstatbestand in § 95 Abs. 5 TKG geregelt.

545 *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 2 Rn. 19 f.; *Kühling/Schall/Biendl*, Telekommunikationsrecht, 2014, Rn. 637; *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 12 TMG Rn. 28–31.

können, EWG 42 S. 5 DSGVO.[546] Schließlich wird ein Verstoß gegen den Koppelungstatbestand angenommen, wenn die Einwilligung eine „sachfremde Begleiterscheinung zum Vertrag" darstellt, wobei die Feststellung im Einzelnen eine wertende Betrachtung verlange.[547]

Für die Identitätsverwaltung wirkt sich dies auf den Schutz des Entschließungsspielraums über die Einwilligung und die Begründung des Datenzyklus zur personalen Identität aus, indem durch den Verantwortlichen eine echte noch so granulare Wahlmöglichkeit im Rahmen der Freiwilligkeit[548] gewährleistet werden muss. Dem ist besondere Aufmerksamkeit beizumessen, wenn die Verhandlungsposition der Parteien ungleich ist, da das Verhandlungsungleichgewicht zwischen Intermediären und Betroffenen erheblich sein kann, was in die Freiwilligkeitsbewertung einzubeziehen ist. Diese ökonomische Dimension der freiwilligen Einwilligung in Gestalt von „Machtproblemen" wird im traditionellen Datenschutzrecht als noch unzureichend eingebettet angesehen.[549] Mit dem Machtungleichgewicht gelange der Betroffene in die Situation, die einer „*take it or leave it*"-Situation gleiche, bei der gerade keine Verhandlungsmöglichkeit bestünde und schnell ein „Häkchen" als mechanischer Prozeduralismus gesetzt werde.[550] Dem steht das beschriebene Erfordernis einer bewussten Entscheidung mit einer echten Wahlmöglichkeit ohne drohende Nachteile gegenüber, Art. 7 Abs. 4 i.V.m. 43 DSGVO. Dies erscheint bei einem Verhandlungsungleichgewicht nur eingeschränkt möglich, so dass die Freiwilligkeit kaum realisiert werden kann. Dies hat zur Folge, dass die Risikobewertung des Betroffenen als echte Wahlmöglichkeit im Hinblick auf die personale Identität unzureichend erfolgt oder gänzlich ausfällt. Demnach kann die enge Verbindung der Einwilligung zu einem Vertrag oder eine ungünstige Verhandlungsposition eine exogene Einschränkung der Freiwilligkeit mit sich bringen, die sich auf den tatsächlichen Rechtfertigungsgrad der kontextspezifischen personalen Identität auswirkt.

546 *Maschmann*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, § 26 BDSG, Rn. 62.

547 *Schulz*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 7 DSGVO Rn. 28.

548 *DSK*, Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DS-GVO, 22.02.2019, S. 1.

549 *Hoffmann-Riem*, AöR 142 (2017), 1 (7) Fn. 20.

550 *Veil*, NVwZ 2018, 686 (688); *Hoffmann-Riem*, AöR 142 (2017), 1 (22 f.); *Becker*, JZ 2017, 170 (174).

bb) Netzwerkeffekte und Algorithmen

Die Entscheidungsbeeinflussung des Betroffenen kann durch exogene, außerrechtliche Faktoren erfolgen und im unmittelbaren Zusammenhang mit dem Kontext der Einwilligung stehen. Die exogenen Faktoren der Verhaltensbeeinflussung können unbewusst erfolgen und in den Algorithmen und dem Verhalten anderer Nutzer liegen. Dieses Phänomen der Verhaltensbeeinflussung geschieht dahingehend beiläufig, dass das Verhalten im online-Kontext unmittelbar algorithmisch verarbeitet wird, ohne mehrdeutige Interpretationen des Verhaltens zuzulassen. Sobald dies in einem großen Umfang geschieht, erlangt das unbewusste Verhalten in der algorithmischen Verarbeitung das gleiche Gewicht wie bewusste Verhaltensweisen.

Die Netzwerkeffekte können sich bei einer großen Nutzerzahl auf die Entscheidungsfindung des Einzelnen auswirken, indem die sozialen „Kosten", sich nicht dem Netzwerk anzuschließen, zu hoch erscheinen und der Nutzer zur Vermeidung des sozialen Ausschlusses die Einwilligung erteilt. Damit fungiert die Einwilligung nicht mehr als solipsistische Entscheidung, sondern unterliegt dem Eindruck des Verhaltens weiterer Nutzer, was wiederum Einwilligungsdruck auslösen und zu nachteiligen Netzwerkeffekten für den Verbraucher führen kann.[551] Dabei können die individuellen Präferenzen über den Schutz personaler Identitäten zurücktreten und die exogenen Faktoren die Entscheidungsfindung maßgeblich beeinflussen, so dass die Entscheidungsfindung als formbar angesehen wird.[552] Damit zeichnet sich die Grenze vom „*Nudging*", Gängeln hin zu einer manipulativen Herbeiführung der konsumorientierten Einwilligung ab, die durch das deutliche Ansprechen bestimmter Motivationsfaktoren in einer kaum durchschaubaren Form gekennzeichnet sei.[553] Dabei wird bereits die Motivation des Betroffenen zu einer bestimmten Handlung und das Ablenken der Aufmerksamkeit, ohne dass dies durchschaubar ist, als eine manipulative Beeinflussung eingeordnet,[554] was zu einer suggerierten freiwilligen Einwilligung führen kann. Dies kann mit einem Korridor von „zugelassenen" Verhaltensweisen erfolgen und zu einer Verhaltenssteuerung führen, mit der ein Vorhersageimperativ durch den verantwortlichen

551 *Bundeskartellamt*, Fallbericht vom 15.02.2019, Az.: B6-22/16, S. 7 f.; *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 19 f.
552 *Acquisti*, IEEE Security & Privacy Magazine 2009, 72 (73 f.).
553 *Zuboff*, FAZ vom 24.09.2018, 12.
554 *Glasl*, Konfliktmanagement, 2020, S. 331.

Intermediär über das künftige Verhalten geschaffen wird.[555] Damit findet eine Paternalisierung durch den verantwortlichen Intermediär statt, die sich weniger auf den Schutz der informationellen Selbstbestimmung und der personalen Identitäten richtet, sondern vielmehr auf die bereitwillige Erteilung der Einwilligung in die Datenverarbeitung.

Gegenüber diesen Phänomenen kann das Recht in seiner verhaltenssteuernden Funktion wirken, indem eine freiwillige Einwilligung gemäß Art. 6 Abs. 1 a), 7 DSGVO stipuliert und gewährleistet wird. Demnach kann die Verhaltenssteuerung durch das Recht mit der Verhaltenssteuerung durch die Technik ergänzt werden. Denn das Wirken der technischen Gestaltung im „Schatten der Einwilligung" führt zu einer Beeinflussung der Entscheidungsfindung des Betroffenen, so dass der Technologie *quasi* eine normative Dimension zukomme[556]. Somit können die algorithmusbasierten Wirkmechanismen eine Quelle der sozialen Ordnung sein,[557] wenn sie für den Betroffenen dahingehend dienlich sein können, dass sie den rechtlichen Schutz der informationellen Selbstbestimmung mit einer algorithmusbasierten Unterstützung ausweiten.

Erschwerend kommt hinzu, dass die Verhaltensbeeinflussungen auf Korrelationen beruhen[558] und die Eigenschaften eines Betroffenen in ihrer Korrelation zu künftigem Verhalten führen können, so dass der Verhaltenskorridor davon geprägt sein kann, was bei Kohorten als Korrelationsmaßstab bestimmt wurde. Dabei kann die Bildung des Verhaltenskorridors blind gegenüber Kausalitätsketten sein, die für ein bestimmtes Verhalten ursächlich sind und den Verhaltenskorridor erweitern würden. Somit könnte etwa eine häufig auftretende Suchanfrage des Betroffenen über bestimmte Buchtitel bei einem online-Händler zu einem algorithmisch festgelegten Buchgeschmack führen, ohne dabei die situative Ursächlichkeit einzubeziehen, die der tatsächlich suchenden personalen Identität in ihrem *Ipse*-Anteil am ehesten entspräche. Die Buchempfehlungen aufgrund des festgestellten Buchgeschmacks verstärken somit den vorangegangenen Verhaltenskorridor und lassen den *Ipse*-Anteil einer personalen Identität als vorübergehendes Verhalten außen vor. In diesen Verhaltenskorridoren liegt für ein Identitätsverwaltungsmodell eine Beschränkung

555 *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 13; *Hoffmann-Riem*, AöR 142 (2017), 1 (8); *Graf von Westphalen*, IWRZ 2018, 9 (10 f.).
556 *Hoffmann-Riem*, AöR 142 (2017), 1 (35); *Steinmüller*, Information, Modell, Informationssystem, S. 47.
557 *Ders.*, AöR 142 (2017), 1 (5 f.).
558 4. Teil, A., I., 2.

der potentiellen Verhaltensmöglichkeiten des Betroffenen, so dass eine Erweiterung und Verhandlungsfähigkeit des Verhaltenskorridors dem Schutz der informationellen Selbstbestimmung dienen könnte. Damit würde der dynamischen Ausprägung einer personalen Identität in ihrem *Ipse*-Anteil Rechnung getragen werden.

Gleichwohl bieten Algorithmen die Chance, dass eine Vorauswahl und Steuerung in die rechtlich und individuell gewünschte Richtung ermöglicht wird, so dass die rechtlichen Maßgaben etwa des Diskriminierungsschutzes effektiver verwirklicht werden und zu einer Entlastung in Überforderungssituationen führen können.[559] Damit kann für die Identitätsverwaltung ein wesentlicher Schutz durch Algorithmen erfolgen, indem die Risiken für die personale Identität hinsichtlich eines bevorstehenden Kontrollverlustes oder eines erhöhten Diskriminierungsrisikos antizipiert werden und Gegenstand von Warnungen werden könnten. In Anknüpfung an das von *Hildebrandt* beschriebene Phänomen des „*digital unconscious*" erscheint im online-Kontext das Spektrum an intransparenten Beeinflussungsmöglichkeiten deutlich weitgehender als im offline-Kontext, so dass ein eigenständiges Risiko von der subtilen technischen Beeinflussungsmöglichkeit ausgeht, welches für eine effektive Identitätsverwaltung in die Modellbildung einbezogen werden sollte. Folglich sollten die Netzwerkeffekte und Algorithmen als exogene Faktoren der Entscheidungsbeeinflussung spiegelbildlich zum Schutz der informationellen Selbstbestimmung in die Identitätsverwaltung einbezogen werden.

cc) Zwischenergebnis

Der Entscheidungsprozess über die Einwilligung hängt von exogenen Faktoren ab, die aus der Einwilligung im Zusammenhang mit dem Vertragsschluss, den Netzwerkeffekten und Algorithmen bestehen. Im online-Kontext können diese exogenen Faktoren bei der Entscheidungsfindung unbewusst wirken, so dass von dem Verantwortlichen ein gewisser Paternalismus gegenüber dem Betroffenen ausgeübt wird. Dies kann zu einer Kanalisierung der Entscheidungsfindung beim Betroffenen führen, die eine Einwilligungserteilung nahelegt. Dabei wird die echte Wahlmöglichkeit durch einen parallelen Vertragsschluss oder algorithmusbasierten Verhaltenskorridor eingeschränkt.

---

559 *Hoffmann-Riem*, AöR 142 (2017), 1 (36).

Wegen der ungünstigen Verhandlungsposition des Betroffenen gegenüber marktbeherrschenden Verantwortlichen führt eine Kanalisierung zur Einwilligungserteilung etwa durch „*Nudging*" zu einer Verstärkung der Verhandlungsungleichheit. Somit kann festgestellt werden, dass der verantwortliche Intermediär ein Interesse an der Einwilligung hat und eine dahingehende Strategie zur Herbeiführung der Einwilligung verfolgt, was zu einer *Erosion der freiwilligen Entscheidung* im Rahmen der informationellen Selbstbestimmung und einem legitimatorischen Defizit der rechtfertigenden Einwilligung führen kann. Folglich könnten die exogenen Faktoren der Entscheidungsbeeinflussung für ein Identitätsverwaltungsmodell spiegelbildlich eingesetzt werden, indem die Förderung der informationellen Selbstbestimmung mit technischer Unterstützung erfolgt. Dies könnte durch die Einbeziehung der verhaltensökonomischen Erkenntnisse des „*Framings*" und „*Primings*" erfolgen. Ebenso kommt der Einsatz von Algorithmen in Betracht, mit denen automatisiert das Bewusstsein für eine risikobewusste Identitätsverwaltung gesteigert wird. Dies könnte mit einem iterativen Verfahren erfolgen, und damit der personalen Identität in ihrem dynamischen *Ipse*-Anteil entsprochen werden.

d) „Privacy Paradox"?

Den endogenen und exogenen Faktoren der Entscheidungsfindung ist gemein, dass diese den Entscheidungsprozess zur Einwilligungserteilung beeinflussen und zu einem legitimatorischen Defizit führen können. Zu dem *Big Data*-Phänomen lässt sich die Bereitwilligkeit der Verbraucher zählen, die Einwilligung in die Datenverarbeitung vorzunehmen, ohne das Risiko der Erkenntnismöglichkeiten über den Datenzyklus einer personalen Identität umfassend antizipieren zu können. Mit diesem als „Exzess der Privatheit" bezeichneten Phänomen[560] geht der Kontrollverlust des Betroffenen über die Datenverarbeitung und mit ihr verbundenen Erkenntnisse über die personalen Identitäten einher. Gleichzeitig kann ein ausgeprägtes Interesse am Privatheitsschutz bestehen, welches im Widerspruch zur hohen Einwilligungs- und Nutzungsbereitschaft steht.

Demnach wird von einem „*Privacy Paradox*" ausgegangen, wonach die Bereitschaft zur Informationspreisgabe hoch ist, obwohl ein ausgeprägtes

560 *Froomkin*, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, S. 41–47

Schutzinteresse an der Privatheit beim Betroffenen besteht.[561] Aufgrund des Komforts oder der unmittelbaren Gratifikation, die mit der Nutzungsmöglichkeit eines Dienstes einhergingen, würden die Privatheitsinteressen kontextbedingt zurücktreten, so dass im „*Privacy Paradox*" die Einstellung des Betroffenen und das tatsächliche Verhalten auseinanderfallen.[562] Dabei konnte nachgewiesen werden, dass selbst bei geringwertigen Gratifikationen, aus Komfortgründen die Bereitschaft zur Informationspreisgabe ausgeprägt sei, da ein scheinbares Wohlwollen des Verantwortlichen durch die Bereitstellung von Gratifikationen angenommen werde und dies Vertrauen beim Betroffenen auslöse.[563] Denn der Betroffene würde sofortige Gratifikation gegenüber langen Phasen ohne Gratifikationen vorziehen,[564] was die Bereitwilligkeit der Einwilligungserteilung fördere. Weiter wurde eine Verlustaversion festgestellt, aus der ein erhöhtes Interesse an Gratifikationen hervorgehe und die Bereitschaft zurücktrete, für die Privatheit schützende Dienste zu bezahlen.[565]

Somit wird die Entscheidung über die Einwilligung von endogenen Faktoren der „*Priming*"-, Anker- und „*Framing*"-Effekte[566] sowie von exogenen Faktoren und damit bestehenden Anpassungsdruck geleitet. Wenn die Entscheidungsgrundlage auf endogene und exogene Faktoren, aber nicht auf das Schutzinteresse der Privatheit zurückzuführen ist, erscheint die bereitwillige Erteilung von Einwilligungen als logische Konsequenz und nicht als Widerspruch, so dass das „*Privacy Paradox*" in Frage gestellt werden könne.[567]

Die Einbeziehung der Phänomene des „*Privacy Paradox*" in das Identitätsverwaltungsmodell könnte durch eine weiche paternalistische Regelung erfolgen. Als ein paternalistisches Konzept kommt auf der inhaltlichen Ebene die Datenschutzerklärung mit einem Hinweis auf die möglichen Wahrnehmungsverzerrungen durch Gratifikationen in Betracht, wobei die ausbleibende Kenntnisnahme der Datenschutzerklärung der Wirksamkeit dieser Maßnahme entgegenstehen könnte. Auf der Einwilligungs-

561 *Engels/Grundwald*, Das Privacy Paradox: Digitalisierung versus Privatsphäre, No. 57.2017, S. 1; *Solove*, Harv. L. R. 2013, 1880 (1886).
562 *Dies.*, Das Privacy Paradox: Digitalisierung versus Privatsphäre, No. 57.2017, S. 2; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 231–233.
563 *Brandimarte/Acquisti*, in: Peitz/Waldfogel (Hrsg.), The Oxford Handbook of the Digital Economy, 2012, S. 561–263.
564 *Acquisti*, ACM 2004, 21 (25) Fn. 27.
565 *Hermstrüwer*, JIPITEC 2017, 9 (19) Rn. 40.
566 4. Teil, C., II., b), bb).
567 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 24.

ebene kommt ein paternalistischer Ansatz mit einem kontextspezifischen „*layered approach*" für die Datenschutzerklärungen in Betracht, der für kontextspezifische Entscheidungen mit einer beschränkten Informationslage geeignet ist und damit eine freiwillige und bewusste Entscheidungsfindung begünstigt.

e) Übertragung auf die Identitätsverwaltung

Die informierte freiwillige Einwilligung lässt sich nicht als solipsistische Entscheidung abbilden, sondern unterliegt exogenen Faktoren der Entscheidungsbeeinflussung durch das Verhalten anderer im Entscheidungskontext. Auch auf der Ebene der endogenen Entscheidungsfaktoren wird die Annahme einer rationalen Entscheidung über die Einwilligung als Kern der informationellen Selbstbestimmung als „Mythologie"[568] oder als unrealistisch eingeordnet[569]. Damit ist der Grat einer rationalen freiwilligen Einwilligung schmal und könnte für das Identitätsverwaltungsmodell einem Modifizierungsbedarf unterliegen. Wenn weder durch exogene noch durch endogene Faktoren eine rein rationale Entscheidung gewährleistet werden kann und der Markt alleine den Schutz der informationellen Selbstbestimmung nicht regelt, bedarf es der Schutzmaßnahme über die Identitätsverwaltung.

Es könnte der Annahme nachgegangen werden, dass die rechtfertigende Einwilligung einem Legitimationsdefizit unterliege, wobei die Einwilligung im Außenverhältnis ihre vollständige Rechtfertigungswirkung beibehält. Und dies obwohl die Einwilligung das Ergebnis von Netzwerkeffekten sein kann und eine echte Auseinandersetzung mit den Verantwortlichen in Gestalt einer echten Wahlmöglichkeit ausgeblieben ist. Denn die Einwilligung sei geprägt von dem Interesse an der Nutzung und knüpft weniger an die bestehende Datenschutzqualität an, wodurch eine von dem Nutzungsvertrag unabhängige Einwilligung zur Datenverarbeitung ausbleibe.[570] Demnach wirkt sich die Einwilligung mit einem Legitimationsdefizit auf das Schutzniveau der generierten personalen Teilidentität in ihrem *Ipse*-Anteil aus. Denn nur mit einer vollständig bewussten Entscheidung über die Generierung neuer personaler Teilidentitäten, aus denen

568 *Veil*, NVwZ 2018, 686 (688).
569 *Cohen*, JTHTL 2012, 242 (249); *Solove*, Harv. L. R. 2013, 1880 (1888); *Graf von Westphalen*, IWRZ 2018, 9 (11).
570 *Becker*, JZ 2017, 170 (174 f.).

möglicherweise kontextübergreifend Erkenntnisse im Rahmen des Datenzyklus erlangt werden können, ist von ihrer Rechtfertigung und damit von ihrer Legitimität auszugehen.

Die Einwilligung mit einem Legitimationsdefizit könnte daher mit der Rechtsfigur der mutmaßlichen Einwilligung verglichen werden, die aber in der DSGVO nicht vorgesehen ist. Zugleich sieht Art. 4 Nr. 11 DSGVO die konkludente Einwilligung vor, deren Vorliegen sich auch nach der allgemeinen Verkehrsanschauung richtet. Gleichzeitig wurde von der Rechtsprechung die Konstruktion einer mutmaßlichen Einwilligung bei einem Suchmaschinenzugriff auf gespeicherte Fotos bei einer Plattform angenommen,[571] was jedoch als „dogmatische Krücke"[572] eingeordnet wird. Ob damit eine Kompensation des dogmatischen Defizits erfolgen kann, ist zweifelhaft, zumal die endogenen und exogenen Entscheidungsfaktoren nicht in die Einwilligungsdogmatik einbezogen werden. Demnach kann nach der bisherigen Rechtslage in der DSGVO zur Einwilligung das Legitimationsdefizit nicht kompensiert werden und es besteht weiterhin ein rechtlicher und tatsächlicher Ausgleichsbedarf.

Das Legitimationsdefizit könnte mit einem Konzept der Einwilligung ausgeglichen werden, welches eine Erweiterung in wenigstens granulare Wahlmöglichkeiten vorsieht. So könnte die Einwilligung in ein kompensatorisches Modell einer iterativen Identitätsverwaltung überführt werden. Mit diesem wäre die Einbuße des Schutzes über die personalen Identitäten in einem Datenzyklus auszugleichen, wenn dem Betroffenen über die datenschutzrechtliche Einwilligung hinaus ein Schutzmechanismus zur Verfügung gestellt wird. Dieser Schutzmechanismus würde in der iterativen Identitätsverwaltung liegen und weitere Einfluss- und Kontrollmöglichkeiten des Betroffenen vorsehen. Damit könnte das festgestellte Legitimationsdefizit über die Einwilligung auf der technischen Ebene mit einem *„layered approach"* kompensiert werden, was eine innovative und effektive technische Gestaltungsmöglichkeit darstellen würde.

In struktureller Hinsicht geht es bei der Identitätsverwaltung um die Einbeziehung der endogenen und exogenen Entscheidungsfaktoren bei der Einwilligungserteilung, da ein erweiterter Schutzbedarf besteht. Dieser Schutzbedarf kann aber nicht mit der Annäherung an ein eigentumsähnliches Verständnis über Daten und Informationen gelöst werden, wie bereits

571 OLG Köln, MMR 2011, 323.
572 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 67.

nachgewiesen wurde.[573] Folglich erscheint die Identitätsverwaltung mit einer kontinuierlichen und dynamischen Kontrollmöglichkeit als eine geeignete Lösung. Dabei wären die endogenen und exogenen Entscheidungsfaktoren einzubeziehen, so dass die „*Priming*"-*Effekte* und die WYSIATI-Regel derart eingesetzt werden könnten, dass ein direkter Einblick in die generierten personalen *Ipse*- und *Idem*-Identitäten ermöglicht und die Risikobewertung für den Betroffenen damit erleichtert wird. Weiter könnten Markt- und Netzwerkeffekte zum Gegenstand von Informationspflichten werden oder in regelmäßigen Zeitabschnitten eine reaktivierende Warnung[574] über die Übermittlung von Daten, die Generierung neuer personaler Identitäten und Erkenntnisse erfolgen. Demnach könnte mit den iterativ erneuerbaren Einwilligungen[575] über den Datenzyklus einer personalen Identität das Legitimationsdefizit sukzessive kompensiert werden, was mit der Identitätsverwaltung erfolgen könnte.

In der Identitätsverwaltung kommt damit eine Steigerung der Kontrollmöglichkeit durch den Betroffenen zum Ausdruck. Gleichzeitig kann mit einer iterativ ausgestalteten Einwilligung in regelmäßigen Zeitabschnitten das Kontroll-Paradoxon wirken und langfristig zu einer Einbuße der informationellen Selbstbestimmung führen. Folglich könnte sich das iterative Identitätsverwaltungsmodell auf die Einwilligung und die personalen Identitäten direkt beziehen, die irreversibel aber im Datenzyklus erweiter- und veränderbar sind, da ein hohes Maß an Wahlmöglichkeiten[576] über die Einwilligung eingeräumt werden würde. Somit stellt die Einwilligung in normativer Hinsicht eine Öffnung für den Verhaltensspielraum durch

---

573 3. Teil, C, II., 1. Die ökonomische Perspektive spiegelt sich auch im angloamerikanischen System des „*contracting over privacy*" wider, in dem die Einwilligung einer Willenserklärung entspräche und eine Vereinbarung über die Datenverarbeitung geschlossen werde. In diesem Ansatz kommt das Verständnis von Daten als Tauschgegenstand zum Ausdruck, der negative Externalitäten gegenüber dem Schutz des öffentlichen Gutes der persönlichen Informationen zur Folge haben könnte, *Ben-Shahar/Strahilevitz*, The Journal of Legal Studies 2016, S1–S11.

574 *Faber/Sedlacek*, DuD 2017, 440 (443). Im Zusammenhang mit Standortdaten *Art. 29 Data Protection Working Party*, WP 185, Stellungnahme zu Geolokalisierungsdiensten von intelligenten mobilen Endgeräten (16. Mai 2011), S. 15.

575 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 105–109; *Brandimarte/Acquisti/Loewenstein*, Social Psychological and Personality Science 4 (2013), 340; Zum Vorschlag eines *Double Opt-in*, *Hermstrüwer*, JIPITEC 2017, 9 (23) Rn. 55.

576 *Jay*, Data protection law and practice, 2012, Rn. 4–41, beschreibt das Phänomen als „*Degree of Choice*".

den Betroffenen dar. Gleichzeitig ist die Einwilligung begrenzt auf das kontextbezogene Wissen und Nichtwissen über die personalen Identitäten. Demnach führt eine uninformierte Entscheidung ebenso zu einer wirksamen Einwilligung über die Generierung personaler Identitäten.

Die Entscheidung über die Erteilung der Einwilligung ist folglich davon geprägt, dass der Betroffene die Informationen über die Datenverarbeitung einbezieht und dabei zugleich *kognitiven Verzerrungen* unterliegt, so dass die Legitimation der rechtfertigenden Einwilligung in der Vorstellung des Betroffenen, rational zu handeln, zu liegen scheint. Die Einwilligung kehrt sich von einer ursprünglich intendierten Bestätigung der informationellen Selbstbestimmung in eine „riskante Aktivität“[577] um.

f) Zwischenergebnis

Die rechtfertigende Einwilligung unterliegt der bereitwilligen Einwilligungserteilung aufgrund endogener und exogener Entscheidungsfindungsfaktoren. Daher lässt sich hinsichtlich der freiwilligen Entscheidungsfindung bei der Einwilligungserteilung ein Legitimationsdefizit feststellen. Gleichwohl entfaltet die Einwilligung im Außenverhältnis ihre vollständige Rechtfertigungswirkung. Folglich sind die verhaltensökonomischen Verzerrungsfaktoren bei der Entscheidungsfindung einzubeziehen und das Wirken der „*Priming*“-Effekte, „*Framing*“- und *Ankereffekte* sollte für die Identitätsverwaltung nutzbar gemacht werden.

Aufgrund der verbreiteten Einwilligungsbereitschaft und dem Schutzinteresse an der informationellen Selbstbestimmung lässt sich bei genauer Betrachtung nachweisen, dass sich die Einwilligung primär an Gratifikationen orientiert und nicht an dem Schutzinteresse der Privatheit, so dass das „*Privacy Paradox*“ in Frage steht. Folglich dient die Einwilligung im Außenverhältnis der informationellen Selbstbestimmung und im Innenverhältnis wirken kurzfristige Gratifikationsinteressen („Myopia“). Demnach könnte es eines differenzierten Schutzregimes bedürfen, um das Legitimationsdefizit der freiwilligen Einwilligung zu kompensieren. Dabei lässt sich an das Recht der allgemeinen Geschäftsbedingungen (AGB) denken. Denn im Recht der AGB trifft der Verbraucher mit dem Akzeptieren der AGBs eine riskante Entscheidung, die aber durch die Schutzvorschriften der §§ 305 ff. BGB kompensiert wird. Folglich könnte das AGB-Recht

577 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 2.

für die Einwilligung in einem Identitätsverwaltungsmodell ebenfalls aufschlussreich sein.

2. AGB-Recht und Einwilligung

Das AGB-Recht kann durch das Nebeneinanderstehen von Nutzungsbedingungen eines Dienstes und datenschutzrechtlicher Einwilligung im engen Zusammenhang mit dem Datenschutzrecht stehen.[578] Der Vergleich zwischen der Einwilligung in die Datenschutzerklärung und der Zustimmung in die allgemeinen Geschäftsbestimmungen wird in der Literatur vielfach aufgegriffen.[579] In Anbetracht des Phänomens ungleicher Verhandlungspositionen im datenschutzrechtlichen Kontext, lässt sich das gleiche Phänomen als Regelungsgegenstand der §§ 305 ff. BGB feststellen. In beiden Kontexten stehen sich Verbraucher und Unternehmer mit einer ungleich verteilten Informationslage gegenüber, die über Transparenzregeln zu Beginn der Rechtsbeziehung kompensiert werden soll, indem der Verbraucher umfassend informiert wird, Art. 12, 13 DSGVO, § 305 Abs. 2 BGB.

Unter der Annahme, dass der Verbraucher die AGBs liest, müsste dieser nach der Interpretation und dem Verstehen des Inhaltes die Konsequenzen der AGB und seine fehlende Verhandlungsmacht feststellen können.[580] Gleichzeitig erscheint die Annahme einer rationalen Entscheidung, die AGB nicht zu lesen, ebenso naheliegend. Für das AGB-Recht wurde „der

578 LG Nürnberg-Fürth, Urt. v. 17.04.2018 – Az.: 7 O 6829/17: Nach diesem Urteil wurde die Datenschutzerklärung beanstandet, da aufgrund der akzeptierten AGB, die Nutzungsdaten an Dritte freigegeben wurden. In den AGB hieß es standardmäßig: „Ich möchte gefunden werden (...) von Personen, die nicht bei StayFriends sind bei Portalen mit Ehemaligenverzeichnissen bei öffentlichen Suchmaschinen (…) Wir zeigen Ihr Profilbild außerhalb von StayFriends und Sie können mit diesem Profilbild bei Suchmaschinen, wie z.B. Google, gefunden werden." Die allgemeine Einwilligung in die Datenschutzerklärung könne nicht zugleich die Zustimmung zur Veröffentlichung personenbezoger Daten sein.

579 *Becker*, JZ 2017, 170; *Hoffmann-Riem*, AöR 142 (2017), 1 (21 f.); *Hermstrüwer*, JIPITEC 2017, 9. Eine missbräuchliche Leistungsbeschreibung bei Unvereinbarkeit mit *privacy by design*-Grundsätzen wird als Verstoß gegen AGB-Recht anerkannt, vgl. *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749).

580 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (67); *Solove*, Harv. L. R. 2013, 1880 (1886).

Mythos von der Möglichkeit zu lesen“[581] begründet, der sich auf die Datenschutzerklärungen übertragen lässt.[582] Damit wurde nachgewiesen, dass nur „exotische Individuen“[583] die AGB lesen würden und es insgesamt rationaler sei, die AGB nicht zu lesen. Dieses Phänomen wird vorliegend auch bei den Datenschutzerklärungen angenommen, denn das Lesen der Datenschutzerklärung würde keine signifikante Änderung mit sich bringen.[584] Lediglich würde der Betroffene nach dem Lesen feststellen können, dass es Änderungsbedarf oder Unklarheiten bei den Informationen in der Datenschutzerklärung gibt, um dann aber das Fehlen einer Verhandlungsposition festzustellen. Folglich könne die Lücke zwischen dem „Ideal der autonomen informierten Entscheidungswahl“ und der „Realität von Uninformiertheit“ durch Mechanismen des „*Ratings*“ und „*Labelns*“ von AGB eingesetzt werden,[585] die sich auch auf Datenschutzerklärungen übertragen ließen.

Im Recht der allgemeinen Geschäftsbedingungen wird über die *contra proferentem*-Regel nach § 305c Abs. 2 BGB die inhaltliche Kontrolle der AGB eröffnet, die zu einer teilweisen Unwirksamkeit gemäß § 306 BGB führen kann. Die datenschutzrechtlichen Informationspflichten sehen eine derartige Kontrolle nicht vor, obwohl die Verhandlungsmacht und die Informationen über die Datenverarbeitung ungleich verteilt sind, wie es bei dem Recht der AGB der Fall ist. Demnach hält *Hermstrüwer* eine *contra proferentem*-Regel im Datenschutzrecht für wünschenswert.[586] Ebenso könnten nach *Hoffmann-Riem* die im Recht der allgemeinen Geschäftsbeziehungen vorgesehenen Rechtsfolgen im Datenschutzrecht einbezogen werden, wonach rechtlich indizierte inhaltliche Restriktionen für Datenschutzerklärungen in Frage kämen.[587] Dabei könnten Datenschutzerklärungen in einem für den Betroffenen unvorteilhaften Kontext einer besonders kritischen Prüfung im Hinblick auf ihre Bestimmtheit unterliegen,[588] die ein mit §§ 307–309 BGB vergleichbares Regelungsregime umfassen würden. Eine weitergehende Differenzierung könnte den Regeln II 9:402–9:405 DCFR (*Draft Common Frame of Reference*) entnommen werden, in denen

581 *Ben-Shahar*, ERCL 2009, 1. Das fehlende Erklärungsbewusstsein bei der Einwilligung anerkennend, *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3746 f.).
582 4. Teil, C., II., 1.
583 *Ben-Shahar*, ERCL 2009, 1.
584 *Veil*, ZD 2018, 9; *Veil*, NVwZ 2018, 686 (688).
585 *Ben-Shahar*, ERCL 2009, 1 (9).
586 *Hermstrüwer*, JIPITEC 2017, 9 (23) Rn. 53.
587 *Hoffmann-Riem*, AöR 142 (2017), 1 (21 f.).
588 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 29 f.

der Rechtsbegriff „unfair" differenzierend zwischen B2C-, C2C- und B2B-Vertragsbeziehungen definiert wird. Eine entsprechende Differenzierung könnte im Datenschutzrecht für die kontextspezifische Wirksamkeit der Einwilligung herangezogen werden. Sofern das Recht der allgemeinen Geschäftsbedingungen als staatlicher Paternalismus eingeordnet wird, könnte nach einer Übertragung entsprechender Schutzmechanismen auf das Datenschutzrecht gefragt werden. Zudem wird festgestellt, dass das private Wirtschafts- und Verbraucherrecht von einer Diskussion über staatlichen Paternalismus geprägt und dies entsprechend im Datenschutzrecht kaum erkennbar sei.[589]

Neben einer dem AGB-Recht vergleichbaren rechtlichen Konkretisierung der Art. 12, 13 DSGVO kommen technische Gestaltungsmechanismen in Betracht. Diese können als „*reading agents*"[590] eingesetzt werden, mit denen die Entscheidungsfindung des Betroffenen durch einen Assistenten erleichtert wird. Ebenso kommen „*rating*"-Systeme in Betracht, bei denen die Datenschutzerklärungen vergleichbar zu Produktbewertungsportalen überprüft und bewertet werden können.[591]

3. Prozeduralisierte Einwilligung

Die Einwilligung stellt eine Prozeduralisierung der Rechtfertigung dar, denn mit ihr wird eine informierte Entscheidung vorgenommen und gleichzeitig wird mit der Einwilligung die informationelle Selbstbestimmung für die kontextbezogene Datenverarbeitung beschränkt.[592] Denn mit der Einwilligung wird die informationelle Selbstbestimmung ausgeübt, gleichzeitig wirkt diese für den Zeitpunkt der Einwilligung und für die personalen Identitäten mit den Erkenntnismöglichkeiten im Datenzyklus, ohne jedoch eine weitere Kontrollmöglichkeit vorzusehen. Daraus wurde ein legitimatorisches Defizit für die informationelle Selbstbestimmung begründet, welches mit einer erweiterten Prozeduralisierung durch die Identitätsverwaltung kompensiert und die Kontrolle über die personalen Identitäten wiederhergestellt werden könnte. Diese Prozeduralisierung

589 *Spiecker gen. Döhmann*, in: Vesting (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, 263 (278) mwN.
590 *Ben-Shahar*, ERCL 2009, 1 (19).
591 *Ders.*, ERCL 2009, 1 (22 f.).
592 2. Teil, A., I., 2., b).

könne in einer *iterativen Verhandlung*[593] bestehen, indem mit der Einwilligung des Betroffenen die Rechtsbeziehung zum Verantwortlichen nachverhandelt[594] wird. Dahingehend könnte einerseits die Verhandlung der Datenschutzerklärungen und andererseits die Einwilligungen über den *Ipse*-Anteil der personalen Identität umfasst sein.

Auf der Ebene der Datenschutzerklärung wird ein Austausch der Vorgaben einer Datenschutzerklärung auf syntaktischer Ebene zwischen dem Verantwortlichen und Betroffenen vorgeschlagen. Dabei erfolgt eine Prüfung, anschließend wird in einer weiteren Iteration eine Modifizierung ermöglicht, die in einer abschließenden Autorisierung der Datenschutzerklärung über statische Protokolle mündet.[595] Auf der Ebene der Einwilligung kommt für einen bestimmten Zeitraum der personalen Identität eine kontextspezifisch wirkende Einwilligung in Betracht, die mit dem „*layered approach*" erteilt werden könnte. Für den Betroffenen könnte die Nutzung über ein „*Dashboard*" erfolgen, in dem die Informationen über die personalen Identitäten und die dazugehörigen kontextspezifischen Transaktionen enthalten sind und zu denen dem Betroffenen der Zugang eingeräumt werden müsste. Das Konzept eines *Dashboard-Systems* wurde von *Raschke/Küpper/Drozd/Kirrane*[596] vorgeschlagen. Es soll die Betroffenenrechte zur Verfügung stellen, die Verwaltung der Rechte ermöglichen und unter der Prämisse der „*Usability*" gestaltet werden. Entsprechend würde die Einbeziehung von Transparenzmethoden für die Informationspflichten und die anschließenden Betroffenenrechte, insbesondere das Auskunftsrecht, dazu gehören. Nach dem vorgeschlagenen Konzept bedarf es eines Zugangs für alle Betroffenen und der Visualisierung von Datenflüssen mit ihren jeweiligen Datenverarbeitungszwecken, damit die Betroffenenrechte ausgeübt werden können. In diesem Konzept werden die Datenschutzprinzipien mit den Rechten des Betroffenen vereint, so dass das Schutzregime über ein technisches Verfahren erfolgen würde.[597]

Für die Identitätsverwaltung erscheint ein *Dashboard-System* als ein geeignetes technisches Verfahrenssystem, da gerade auf der Visualisierungsebene neben den Datenflüssen die personalen Identitäten transparent ge-

---

593 2. Teil, A., II., 1., d).

594 *Jay*, Data protection law and practice, 2012, Rn. 6–39, „renegotiate the terms of that relationship".

595 *Birnstill/Beyerer*, in: ACM-PETRA 2018, 292.

596 *Raschke/Küpper/Drozd u.a.*, in: Hansen/Kosta/Nai-Fovino u.a. (Hrsg.), Privacy and Identity Management, 2017, 221.

597 *Dies.*, in: Hansen/Kosta/Nai-Fovino u.a. (Hrsg.), Privacy and Identity Management, 2017, 221 (226).

macht werden können und damit der absoluten Kontrolle für die weitere Datenverarbeitung unterliegen würden. Dieses *Dashboard-System* würde zunächst an den Zeitpunkt *ex ante* zur Rechtfertigung anknüpfen und zugleich die Möglichkeit der kontextbezogenen rechtfertigenden Einwilligung umfassen. Insgesamt könnte der Betroffene im Sinne einer „*guided tour*"[598] mit einem *Dashboard-System* durch seine personalen Identitäten und Rechte nach der DSGVO geführt werden, womit ein Verfahren zur iterativen Realisierung der rechtfertigenden Einwilligung vorliegen würde.

4. Paternalistische Intervention?

Es kommt für die Kompensation des Legitimationsdefizits personaler Identitäten die paternalistische Intervention als „*opacity tool*" zum Schutz des Betroffenen in Betracht. Unter der Annahme, dass die rationale Zielverfolgung der natürlichen Person mit der neuen Erwartungstheorie unhaltbar scheint, ließe sich eine paternalistische Regelung vergleichbar mit der Verpflichtung, sich anzuschnallen gemäß § 21a StVO,[599] zum Schutz des Betroffenen vor irrationalen Entscheidungen bei der Entschließung für die Einwilligung in Erwägung ziehen. Es kommt eine Regelung in Betracht, die vor den Verzerrungsfaktoren bei der Entscheidungsfindung mit den spezifischen Risikolagen aufgrund der fehlenden Haptik von Datenverarbeitungsprozessen schützt und die Verhandlungsmacht des Verantwortlichen durch normative Intervention beschränkt.

Eine solche Regelung würde den Betroffenen vor sich selbst schützen können, zugleich aber eine tiefgreifende und mit den Annahmen einer freiheitlichen Entscheidungsfindung kaum zu vereinbarende Intervention darstellen.[600] Damit kommt ein Kompensationsmechanismus auf der Gestaltungsebene in Betracht, wonach mit Hilfe von „*Interface Design*" die bewußte Entscheidung im Rahmen der informationellen Selbstbestimmung gefördert wird. Hierbei wäre eine Kanalisierung und Beschränkung der Wahlmöglichkeiten denkbar, so dass damit der anvisierte Effekt herbeigeführt wird, einen besseren Schutz für die informationelle Selbstbestimmung zu generieren.[601] Infolgedessen könnte durch das Richten der Aufmerksamkeit auf die Veröffentlichungsrisiken eine Steigerung des Schut-

598 *Spindler*, in: Verhandlungen des 69. Deutschen Juristentages, 2012, S. F 108.
599 *Eidenmüller*, JZ 2011, 814 (815).
600 *Ders.*, JZ 2011, 814 (815) Fn. 13.
601 *Schneider/Weinmann/Vom Brocke*, Communications of the ACM 2018, 67 (71).

zes bewirkt und damit die Einwilligungsbereitschaft minimiert werden.[602] Der Betroffene könnte auch zu entsprechenden Vorsichtsmaßnahmen nach der Einwilligung animiert werden.

Für das Identitätsverwaltungsmodell erscheint die Abstufung der Einwilligungen über die personalen Identitäten in dem jeweiligen Kontext vorzugswürdig. Dabei könnte durch „*Nudging*" die Aufmerksamkeit auf endogene Verzerrungsfaktoren gelenkt werden und eine risikobewusste Entscheidung des Betroffenen für die Einwilligung zu einer bestimmten personalen Teilidentität erleichtert werden. Folglich könnte die iterative Identitätsverwaltung derart ausgestaltet sein, dass sie die Aufmerksamkeit auf die Kontrollierbarkeit der generierten personalen Identitäten richtet. Hierfür kann das *Dashboard-System* eingesetzt werden, welches eine Gesamtschau über die personalen Identitäten und zugleich die Ausübung der Rechte des Betroffenen ermöglicht. In diesem *Dashboard-System* können die Informationen über die Datenverarbeitungen und die entstandenen personalen Identitäten derart ausgestaltet sein, dass der Betroffene einen Anstoß zu möglichst risikobewussten Entscheidungen erfährt. Demnach würde das „*Nudging*" sich auf der technischen Gestaltungsebene vollziehen, da auf der rechtlichen Ebene eine paternalistische Intervention in einer Differenzierung der Einwilligungsregeln gemäß Art. 6 Abs. 1 a), 4 Nr. 11 DSGVO liegen und die Anforderung einer „risikobewussten Einwilligung" voraussetzen würde. In Anbetracht des Abstraktionsgrades von Rechtsnormen und dem bereits bestehenden Erfordernis, dass die Einwilligung eine informierte freiwillige Entscheidung voraussetzt, wirkt eine solche Regelungserweiterung wenig zielführend für die Steigerung des Schutzniveaus der informationellen Selbstbestimmung.

Somit erscheint ein Kompensationsmechanismus mit Anreizen und „*Nudging*" auf der technischen Gestaltungsebene naheliegend, wenn diese derart ausgestaltet werden, dass sie unterstützend wirken und nicht zum Schaden der Rechte und Freiheiten des Betroffenen führen. Demnach kann das *Dashboard-System* als ein *ex ante*-Kompensationsmechanismus eingesetzt werden, welcher der technischen Gestaltung des Verantwortlichen oder Herstellers unterliegt. Gleichwohl müsste ein rechtlicher Anreizmechanismus geschaffen werden, damit der Verantwortliche und der Hersteller dazu gehalten werden, die technische Gestaltung über ein *Dashboard-System* vorzunehmen. Dies könnte mit einer Regelung im Produkthaf-

602 *Acquisti*, IEEE Security & Privacy Magazine 2009, 72 (74).

tungsrecht und einer Erweiterung des Art. 25 DSGVO mit einem „*identity management by design*"-Konzept erfolgen.[603]

Insgesamt müsste bei der Implementierung eines *Dashboard-Systems* das Kontroll-Paradoxon einbezogen werden, da die Steigerung der Einflussmöglichkeiten des Betroffenen langfristig zu einem Absenken des Schutzes der informationellen Selbstbestimmung führen kann. Folglich erscheint bei einer Identitätsverwaltung über ein *Dashboard-System* eine ausgeglichene Einbeziehung von Kontrollmöglichkeiten, „*Nudging*" und automatisierten Darstellungen erforderlich, um übermäßige Kontrollmöglichkeiten zu vermeiden. Auf diese Weise würde das *Dashboard-System* als eine technische Gestaltungsform zur Kompensation von endogenen und exogenen Einflüssen bei der Einwilligung dienen können. Dabei würde das *Dashboard-System* als „*opacity tool*" und zugleich als „*transparency tool*" fungieren.

5. Ergebnis

Die Identitätsverwaltung mit der informierten freiwilligen Einwilligung unterliegt Verzerrungsfaktoren auf der endogenen und der exogenen Ebene, durch die ein Legititimationsdefizit bei der Einwilligung entstehen kann. Mit der vorliegend vertretenen Darstellung bedarf es der Kompensation dessen durch rechtliche oder technische Maßnahmen. Auf der technischen Ebene könnten aufgrund von verbreiteten Einwilligungsabfragen „*Reading Agents*" eingesetzt werden, mit denen der Betroffene einen Assistenten zur Risikobewertung und Entscheidungsfindung erhalten würde. Dabei könnten auch „*Rating*"-Systeme über das Vergleichsergebnis mit mehreren Datenschutzerklärungen hinzugezogen werden, die bei der Entscheidungsfindung unterstützend wirken. Ebenso könnten aufgrund der Verzerrungsfaktoren bei der Entscheidungsfindung „*Nudging*"-Strukturen zur „Steuerung der Selbststeuerung"[604] einbezogen werden, die zu einer Steigerung des Bewusstseins über endogene und exogene Faktoren führen könnten. Dafür wäre ein *Dashboard-System* geeignet, um die erforderliche Transparenz für die kontextspezifischen Einwilligungen über die personalen Identitäten herbeizuführen, und um eine risikobewusste Entscheidungsfindung zu ermöglichen. Maßgeblich dabei wäre eine iterative Aus-

603 4. Teil, B., IV.; zu einem „*anti-discrimination by design*" vgl. *Wischmeyer*, AöR 143 (2018), 1 (29).

604 *Zippelius*, Das Wesen des Rechts, 2012, S. 34.

gestaltung, damit für den Datenzyklus der personalen Identität die Kontrolle regelmäßig ausgeübt werden kann. Um dem Kontroll-Paradoxon gerecht zu werden, bedarf es eines ausgewogenen Verhältnisses zwischen der absoluten Kontrolle über die Einwilligung mit einer echten Wahlmöglichkeit und den darauffolgenden iterativen Einwilligungsmöglichkeiten. Damit könnte eine kontextspezifische absolute Kontrolle über die personale Identität, iterativ auf den Datenzyklus verteilt, ausgeübt werden, so dass eine Bewusstseinssteigerung für den Schutz der personalen Identität herbeigeführt wird.

Insgesamt wirkt sich die Gestaltung der Einwilligungsstruktur auf den anzuwendenden Stand der Technik im Identitätsverwaltungsmodell aus und sollte auf die Dienste und das Internet der Dinge übertragen werden. Ebenso könnten bei der technischen Gestaltung für die Identitätsverwaltung die Rechtfertigungsgründe gemäß Art. 6 Abs. 1 b) – f) DSGVO einbezogen werden. Sobald eine gerechtfertigte Datenverarbeitung erfolgt, könnten die Rechtfertigungsgründe transparent über das *Dashboard-System* hinsichtlich der generierten personalen Identitäten einsehbar sein. Folglich könnten die Rechtfertigungsgründe gemäß Art. 6 Abs. 1 b) – f) DSGVO ebenso zum Gegenstand des Identitätsverwaltungsmodells werden.

III. Identitätsverwaltung ohne aktive Handlung des Betroffenen, Art. 6 Abs. 1 b) – f) DSGVO

Die Rechtfertigung für die Datenverarbeitung im Rahmen der Identitätsverwaltung kann ohne aktive Handlung des Betroffenen erfolgen. Damit mangelt es zunächst an der Kontrolle für die Begründung der Rechtfertigung und die Kontrollmöglichkeit beschränkt sich auf die Kenntnisnahme der transparenten Datenschutzerklärung und ihre Einbeziehung in die Entscheidungsfindung. Demnach kann *ex post* zur Rechtfertigung ein gesteigerter Bedarf an Identitätsverwaltung bestehen, um das Kontrolldefizit zu einem späteren Zeitpunkt des Datenzyklus zu kompensieren.

Die Rechtfertigung gemäß Art. 6 Abs. 1 b) – d) DSGVO knüpft jeweils an der Erforderlichkeitsprüfung durch den Verantwortlichen in variierender Prüfungsintensität an. Indem die Erforderlichkeitsprüfung im Verbotsvorbehalt wurzelt, verlangt die Rechtfertigung mit der Erforderlichkeit

eine gewisse Alternativlosigkeit der Datenverarbeitung.[605] Mit der Rechtfertigungsprüfung durch den Verantwortlichen erfolgt eine implizite Risikobewertung in der Erforderlichkeit, da die konkreten Umstände der Identitätsverwaltung und der Zweck der Datenverarbeitung einbezogen werden müssen.[606] Etwa im Beschäftigtendatenschutzrecht kann gemäß Art. 88 DSGVO i. V. m. § 26 BDSG die Datenverarbeitung für die Durchführung der Beschäftigung gerechtfertigt sein, was die Begründung, die Durchführung und die Beendigung der Beschäftigung umfasst, wenn die Datenverarbeitung aufgrund der beschäftigungsspezifischen Interessen erforderlich ist.

Die Abgrenzung im Einzelnen, wann die Rechtfertigung über die Einwilligung oder die Erforderlichkeit zu erfolgen hat, richtet sich nach dem Vorliegen oder dem Fehlen eines Entscheidungsspielraumes für den Betroffenen. Sobald kein Entscheidungsspielraum zur Verfügung steht, spricht dies für die Erforderlichkeit der Datenverarbeitung, wohingegen beim Bestehen eines granularen Entscheidungsspielraumes die Rechtfertigung nach Art. 6 Abs. 1 a) DSGVO für vorzugswürdig gehalten wird.[607] Die Definitionsmacht über die Bestimmung, wann ein Entscheidungsspielraum beim Betroffenen besteht, obliegt dem Verantwortlichen, so dass die Erwägungen über die Bestimmung des geeigneten Rechtfertigungsgrundes für den Betroffenen undurchsichtig sind. Der Betroffene verbleibt mit der Feststellung über das Bestehen einer Einwilligungsmöglichkeit oder dem Fehlen dieser.

Die mit dem öffentlichen Interesse gerechtfertigte Datenverarbeitung bringt das Fehlen eines Entscheidungsspielraums besonders deutlich zum Ausdruck. Danach besteht kein Raum für die Freiwilligkeit der betroffenen Person, sondern wegen des öffentlichen Interesses oder der Ausübung öffentlicher Gewalt kann die Datenverarbeitung als erforderlich eingeordnet werden, Art. 6 Abs. 1 e) DSGVO. In dem *Dashcam*-Urteil des Bundesgerichtshofes[608] wurden aufgrund des überwiegenden Beweisinteresses des Staates an einer funktionierenden Zivilrechtspflege die *Dashcam*-Aufnahmen im Straßenverkehr auch ohne Einwilligung als gerechtfertigt angesehen. Die informationelle Selbstbestimmung trat in der Gesamtabwägung

605 *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 6 DSGVO Rn. 15.
606 4. Teil, B., II., 2., a), bb).
607 www.ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ (Zuletzt aufgerufen 20.06.2020).
608 BGH, Urt. v. 15.05.2018 – VI ZR 233/17.

zurück. Darin kommt deutlich zum Ausdruck, dass bei Bestehen eines öffentlichen Interesses die Wahlmöglichkeit des Betroffenen ausgeschlossen ist und die Rechtfertigung der Datenverarbeitung mit der Erforderlichkeit eintritt. Für die Identitätsverwaltung bedeutet dies, dass mit einer Rechtfertigung über das öffentliche Interesse gemäß Art. 6 Abs. 1 e) DSGVO die freiwillige Entscheidung und die Kontrollmöglichkeit des Betroffenen ausbleibt und diese zu einem späteren Zeitpunkt im Datenzyklus erfolgt. Demnach ist das Identitätsverwaltungsmodell nicht auf die Kontexte beschränkt, bei denen eine Einwilligungsmöglichkeit besteht, sondern erstreckt sich auf sämtliche Rechtfertigungsgründe. Die Kontrollmöglichkeit über die personalen Identitäten besteht dann *ex ante* zur Rechtfertigung auf der Ebene der Transparenz und *ex post* zur Rechtfertigung bei den Betroffenenrechten.

Eine vergleichbare Sachlage erscheint ebenso bei der Rechtfertigung über das berechtigte Interesse gemäß Art. 6 Abs. 1 f) DSGVO. Dieser Erlaubnistatbestand tritt in der Rechtsbeziehung zwischen Verbraucher und Unternehmer als ein verbreiteter Rechtfertigungsgrund[609] auf, da er aus der Perspektive des Verantwortlichen vorzugswürdig ist und in der Umsetzung allein die dokumentierte Begründung vom Verantwortlichen verlangt. Gemäß Art. 6 Abs. 1 f) DSGVO muss das berechtigte Interesse zugleich ein legitimes Interesse sein, welches im Einklang mit nationalem und europäischem Recht steht. Die Bestimmung des legitimen Interesses ist ebenso Gegenstand einer Abwägung, die unter Einbeziehung des risikobasierten Ansatzes erfolgt und einer eigenständigen Risikobewertung unterliegt.[610] Denn mit der Identifikation eines hohen Risikos bei der Datenverarbeitung geht ein gesteigertes Rechtfertigungsbedürfnis einher, welches zu einem Einwilligungserfordernis führen kann. Somit kommt die Rechtfertigung über das berechtigte Interesse allein bei solchen Datenverarbeitungen in Betracht, die mit einem geringen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden sind. Weiter müssen die Datenverarbeitungen, die auf dem legitimen Interesse basieren, von der „vernünftigen Erwartung" des Betroffenen gedeckt sein, so dass unvorhersehbare und überraschende Datenverarbeitungen ausgeschlossen sind, EWG 47 S. 1. Die Voraussetzung für das Vorliegen der Datenverarbeitung im Rahmen der vernünftigen Erwartung lässt sich vergleichen mit der *contra*

609 *Herfurth*, ZD 2018, 514.

610 *Quelle*, European Journal of Risk Regulation 2018, 502 (515); *Art. 29 Data Protection Working Party*, WP 217, Opinion 6/2014 on the notion of legitimate interest of the data controller (9. April 2014), S. 33–37.

proferentem-Regel aus dem Recht der allgemeinen Geschäftsbedingungen gemäß § 305c Abs. 2 BGB, wonach Zweifel bei der Auslegung zu Lasten des Verwenders gehen. Übertragen auf die datenschutzrechtliche Rechtfertigung mit dem berechtigten Interesse würde die Rechtfertigung einer Datenverarbeitung außerhalb der vernünftigen Erwartung zu Lasten des Verantwortlichen gehen und möglicherweise einen sanktionsbewehrten Sachverhalt begründen.

Dennoch ist mit der Abwägungsverantwortung des Verantwortlichen eine erhebliche Gestaltungsmacht verbunden, die zu einer Verfestigung von Verhandlungsungleichgewichten und bestehenden Informationsasymmetrien beitragen kann. Denn die Abwägung erfolgt in der Vorbereitung zur Datenverarbeitung und nur das Abwägungsergebnis wird für den Betroffenen erkennbar, was die bestehende Informationsasymmetrie verstärkt. Folglich erlangen die Informationspflichten bei der Rechtfertigung mit dem berechtigten Interesse ebenso ein gesteigertes Gewicht, indem die Informationen der alleinige Anknüpfungspunkt für die Kontrolle durch den Betroffenen sind. Dabei können von den Informationspflichten die Benennung des berechtigten Interesses und darüber hinaus die Einbeziehung des Abwägungsvorgangs zur Begründung des berechtigten Interesses erfasst sein, was im Einzelnen aber umstritten ist.[611] Insgesamt kommt in der Rechtfertigung über das berechtigte Interesse wegen der vorangegangen Abwägung erneut der prozedurale Charakter im Datenschutzrecht zum Ausdruck.

Die Rechtfertigung der Datenverarbeitung für die Identitätsverwaltung kann ohne aktive Handlung durch den Betroffenen erfolgen. Die Rechtfertigung ergibt sich dabei aus der Erforderlichkeit, dem öffentlichen Interesse und dem berechtigten Interesse über die Datenverarbeitung. Jeweils obliegt die Entscheidung und Abwägung zur Identifikation des bestehenden Rechtfertigungsgrundes dem Verantwortlichen. Dabei tritt das *Konzept des Selbstdatenschutzes* aufgrund der fehlenden aktiven Handlung des Betroffenen zurück, verlangt aber gleichzeitig für die Wahrung der informationellen Selbstbestimmung eine restriktive Auslegung der Rechtfertigungsgrundlage.[612] Insgesamt kommt in diesen Rechtfertigungsgründen eine Verfestigung des bestehenden Verhandlungsungleichgewichts und der Informationsasymmetrie zum Ausdruck. Die Folge kann eine Steigerung der Marktmacht sein und langfristig kann die Rechtfertigung der Datenverar-

611 *Veil*, NJW 2018, 3337 (3339).

612 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 13.

beitung mit dem berechtigten Interesse zu einer marktbeherrschenden Stellung von Intermediären beitragen.

Den Rechtfertigungsgründen ohne Zutun des Betroffenen ist gemein, dass sie keine Grundlage für die aktive kontrollierte Identitätsverwaltung durch den Betroffenen ermöglichen. Vielmehr können durch die Datenverarbeitungen personale Identitäten generiert werden, die erst nach der Rechtfertigung auf der *ex post*-Ebene der Betroffenenrechte zum Gegenstand der Kontrolle werden können. Entsprechend ist in einem Identitätsverwaltungsmodell auf der Ebene der Transparenz über die Datenverarbeitung und anschließend der Transparenz über die generierten personalen Identitäten die Kontrolle einzuräumen, damit das Kontrolldefizit auf den Ebenen *ex ante* und *ex post* zur Rechtfertigung ausgeglichen werden kann.

IV. Zusammenfassung

Das Rechtfertigungserfordernis für die Identitätsverwaltung wurzelt in dem Verbot mit Erlaubnisvorbehalt und setzt das Vorliegen eines Rechtfertigungstatbestandes für die Verwaltung der personalen Identitäten voraus. Das Verbotsprinzip wird in seiner Funktionalität bei der Datenverarbeitung im Verhältnis zwischen Staat und Bürger deutlich, wonach eine Ermächtigungsgrundlage für die staatliche Datenverarbeitung gegeben sein muss. In diesem Subordinationsverhältnis können personale Identitäten ohne aktive Handlung durch den Betroffenen begründet werden. Gleichzeitig gilt das Verbotsprinzip für die Rechtsbeziehung zwischen Privaten ungeachtet dessen, ob es sich um eine P2C-, B2B-, B2C- oder C2C-Rechtsbeziehung handelt. Zwar lässt sich in der B2C-Rechtsbeziehung eine zum Subordinationsverhältnis vergleichbare Asymmetrie feststellen, jedoch kann die grundrechtliche Abwehrdimension gegenüber staatlichen Eingriffen schwerlich auf die Rechtsbeziehung Privater übertragen werden. Diese ist von der mittelbaren Drittwirkung der Grundrechte geprägt, durch die eine einfachrechtliche Kompensation von ungleichen Verhandlungspositionen erfolgen könnte.

Weiter könnte die paternalistische Schutzwirkung des Verbotsvorbehaltes in Frage gestellt werden, denn es konnte nachgewiesen werden, dass mit der Einwilligung keine Bestätigung oder Steigerung der informationellen Selbstbestimmung einhergeht. Vielmehr ist die Realität davon geprägt, dass die Einwilligung ohne umfassende Kenntnisnahme der Datenschutzerklärung erteilt wird und das Interesse des Betroffenen an unmittelbaren Gratifikationen überwiegt. Somit scheint mit dem Verbotsvorbehalt eine

vermeintliche Kontrollmöglichkeit über die rechtfertigende Einwilligung zu bestehen, mit der generierte personale Identitäten über den Datenzyklus hinweg vermeintlich kontrollierbar sind.

Auch aus verhaltensökonomischer Perspektive kann das Verbotsprinzip in seiner Wirkung angezweifelt werden, denn dieses lässt sich als eine Ausprägung des aus amerikanischer Perspektive vorherrschenden Vorsichtsprinzips in Europa[613] einordnen. Danach soll mit dem Vorsichtsprinzip grundsätzlich das Schadensrisiko vermieden werden, obwohl das datenschutzrechtliche Verbotsprinzip nicht zwingend zu einem gesteigerten Schutz für die informationelle Selbstbestimmung und damit zur Schadensminderung führt. Daraus könnte sich eine Beschränkung des Verbotsprinzips auf den öffentlich-rechtlichen Kontext ableiten lassen, so dass im privatrechtlichen Kontext die Datenverarbeitung der einfachrechtlichen Ausgestaltung unterliegen würde. Ferner kommt als weiche paternalistische Intervention die Implementierung eines Identitätsverwaltungsmodells in Betracht, mit dem das legitimatorische Defizit der Einwilligung kompensiert werden kann. Dabei könnte in rechtlicher und technischer Hinsicht ein *Dashboard-System* als Lösung fungieren.

Die Risiken aufgrund des legitimatorischen Defizits der Einwilligung durch die endogenen und exogenen Entscheidungsfaktoren können in einem *Dashboard-System* mit Transparenzanforderungen, Zugangsrechten und der rechtfertigenden Einwilligung gebündelt werden. Ebenso kommen *„reading agents"* für den Betroffenen in Frage, um die maßgeblichen Informationen für die Identitätsverwaltung aus den Datenschutzerklärungen extrahieren zu können. Weiter könnte das *Dashboard-System* leichte Anreizmechanismen in Gestalt von *„Nudging"* enthalten, da spiegelbildlich zu den Anreizmechanismen über die Einwilligungserteilung ein Schutzmechanismus für die personalen Identitäten erforderlich ist. Dieses paternalistische *„Nudging"* müsste mit der Prämisse ausgestaltet sein, dass die Privatheitspräferenzen und die kontextspezifischen Risiken gegenüber personalen Identitäten tatsächlich in der Entscheidungsfindung einbezogen werden. Damit müssten die Datenschutzerklärungen als Konzept neu definiert werden und möglicherweise Gegenstand einer *iterativen Verhandlung* werden. Auf diesem Wege würde der prozeduralisierten Rechtfertigung entsprochen werden und diese könnte in ein prozedural geprägtes Identitätsverwaltungsmodell überführt werden.

Sobald die Rechtfertigung ohne aktive Handlung durch den Betroffenen erfolgt, kommt ein eigenständiger rechtlicher Schutzmechanismus gegen-

613 *Kahneman*, Schnelles Denken, langsames Denken, 2012, S. 432.

über nachteiligen Bestimmungen in den Datenschutzerklärungen in Betracht, der parallel zu den Schutzregelungen im Recht der allgemeinen Geschäftsbedingungen ausgestaltet sein könnte. Dieser kann in einer datenschutzrechtlichen *contra proferentem*-Regel liegen, mit der die Spezifika der Informationsasymmetrien über ein differenziertes Regelungsregime für P2C-, B2B-, B2C- und C2C-Rechtsbeziehungen einbezogen werden. Damit könnte eine Kompensation des Verhandlungsungleichgewichtes und der Informationsasymmetrie erfolgen. Gerade bei der Rechtfertigung ohne aktive Handlung des Betroffenen erscheint eine Verfestigung des Ungleichgewichts möglich, so dass die Kontrolle *ex ante* aufgrund der Informationspflichten und *ex post* zur Rechtfertigung auf der Ebene der Betroffenenrechte erfolgen würde.

D. Ex post Rechtfertigung personaler Identitäten in der DSGVO

Die Identitätsverwaltung *ex post* zur Rechtfertigung verlangt zunächst einen Einblick des Betroffenen in die personalen Identitäten aus den Datenverarbeitungen, wozu das Auskunftsrecht gemäß Art. 15 DSGVO dient (I.). Mit der Kenntnis über die personalen Identitäten wird der Abgleich im Rahmen des Rechts auf informationelle Selbstbestimmung ermöglicht, was die Grundlage für die Entscheidung über das geeignete Betroffenenrecht zur Wiedererlangung der Kontrolle über die personalen Identitäten ist. Dies lässt sich insbesondere über das Recht auf Löschung gemäß Art. 17 DSGVO (II.) und das Recht auf Datenübertragbarkeit gemäß Art. 20 DSGVO vornehmen (III.). Weiter kann zu einem späteren Zeitpunkt des Datenzyklus der Bedarf nach Transparenz und Kontrolle bei einem Datenschutzverstoß (IV.) und dem Recht auf Kontrolle bei automatisierten Entscheidungen entstehen (V.). Als zeitlich letztes Recht des Betroffenen kommt die Geltendmachung eines gerichtlichen Rechtsbehelfs wegen eines materiellen oder immateriellen Schadens gemäß Art. 79 DSGVO in Betracht (VI.).

I. Auskunft als Zugangsrecht für die Identitätsverwaltung, Art. 15 DSGVO

Das Recht auf Auskunft ist in Art. 8 Abs. 2 S. 2 GRC primärrechtlich verankert und stellt die Voraussetzung zur informierten Ausübung der Betroffenenrechte dar. In dem Recht auf Auskunft gemäß Art. 15 DSGVO liegt

die Vorstufe in Gestalt der Informationsbeschaffung, mit der die Entscheidung über die Notwendigkeit der Ausübung eines Betroffenenrechts und die Entscheidung über die Wahl des geeigneten Betroffenenrechts ermöglicht werden. Dabei lässt sich das Auskunftsrecht zugleich als Zugangsrecht einordnen, wie es bereits die englischsprachige Überschrift des Art. 15 DSGVO als „*right of access by the data subject*" mit der Übersetzung des Begriffs „*access*" als Zugang[614] nahelegt. Mit dem Verständnis des Auskunftsrechts als Zugangsrecht erlangt dieses die Funktion eines Rechts zur absoluten Kontrolle der personalen Identitäten.

Die Voraussetzung für eine wirksame Identitätsverwaltung ist zunächst der Zugang zu den Daten im Rahmen der Auskunft, um anschließend *ex post* zur Rechtfertigung eine Entscheidung über die Ausübung der Betroffenenrechte vornehmen zu können. Auf diese Weise wird die Steuerungsmöglichkeit über die personalen Identitäten im Datenzyklus über Art. 15 DSGVO zurückerlangt und kann in regelmäßigen „angemessenen Abständen" ausgeübt werden, EWG 63 S. 1. Von dem Recht auf Auskunft sind die spiegelbildlichen Informationen aus den Informationspflichten gemäß Art. 12 DSGVO erfasst. Sie sollen dem Betroffenen der wirksamen Ausübung seiner Betroffenenrechte nach der Rechtfertigung dienen. Dabei hat der Verantwortliche eine Kopie der personenbezogenen Daten zur Verfügung zu stellen, woraus sich die Pflicht zur Bündelung der personenbezogenen Daten ableiten lässt, die bereits bei der Planung der technischen und organisatorischen Maßnahmen einzubeziehen ist. Die Ausübung des Auskunftsrechts verlangt zunächst die Authentifizierung des Betroffenen gemäß Art. 12 Abs. 6 DSGVO und umfasst, ob eine Datenverarbeitung stattgefunden hat und welche Daten verarbeitet wurden.

In einem Identitätsverwaltungsmodell mit der technischen Ausgestaltung eines *Dashboard-Systems* kann das Auskunftsrecht unmittelbar zwischen dem Betroffenen und Verantwortlichen wirken. Gleichzeitig ließe sich eine kontextspezifische Erweiterung in Erwägung ziehen, die den Zugang zu einer personalen Identität ermöglicht und diese in anderen Kontexten einsetzbar wäre. Dafür könnte das *Dashboard-System* als iterative Zu-

614 Die Übersetzung des Begriffs „*right of access*" entspricht einem Zugangsrecht. Demgegenüber ist in der deutschen Fassung der DSGVO von einem Auskunftsrecht die Rede, welches auch mit „*the right to information*" übersetzt werden oder dem „*right to be informed*" gleichgesetzt werden kann. Ebenso verwendet die Datenschutzaufsichtsbehörde in England den Begriff des „*right of access*", www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/ (Zuletzt aufgerufen 20.06.2020).

gangs- und Kontrollmöglichkeit mit der Maßgabe dienen, dass die tatsächliche Ausübung des Auskunftsrechts erleichtert wird. Dabei würde das Auskunftsrecht erweitert werden und zur Einräumung eines Zugangsrechts als Kontrollmöglichkeit führen.

Insgesamt offenbart sich das Auskunftsrecht als Transparenzerfordernis *ex post* zur Rechtfertigung und kann durch den Verantwortlichen auch als vertrauensbildende Maßnahme gegenüber dem Betroffenen eingesetzt werden. Denn mit der Kenntnis des Betroffenen über seine personalen Identitäten nach der Rechtfertigung, wird eine reale Kontroll- und Gestaltungsmöglichkeit eingeräumt, die die Bereitschaft zur Fortsetzung der Datenverarbeitung unter den bisherigen Datenverarbeitungsbedingungen steigern kann.

II. Löschungsrecht zur Identitätsverwaltung, Art. 17 DSGVO

Das Löschungsrecht für die Identitätsverwaltung ist als Gegenrecht zur Einwilligung und ihren Konsequenzen im Datenzyklus einzuordnen, da mit der Geltendmachung des Rechts die Datenverarbeitung und ihre Folgen im Datenzyklus der personalen Identität beendet werden können. Der Ursprung des Löschungsrechts geht zurück auf das *Google Spain*-Urteil des EuGHs[615], in dem ein Recht auf Vergessenwerden für den online-Kontext begründet wurde. Dieses Recht auf Vergessenwerden wurde nunmehr vom Bundesverfassunsgsgericht[616] für die nationalen Grundrechte anerkannt und konkretisiert.

Mit dem Recht auf Vergessenwerden aus Art. 17 DSGVO besteht *ex post* zur Rechtfertigung die Möglichkeit, dass ein bestehendes Legitimationsdefizit der Einwilligung mit der Löschungsmöglichkeit personaler Identitäten ausgeglichen wird. Ebenso kann ein vorangegangenes Kontrolldefizit durch die Löschung der Datensätze zur personalen Identität kompensiert und damit die Kontrolle zurückerlangt werden. Weiter können mit dem Recht auf Vergessenwerden und dem Recht auf Datenportabilität zu einem späteren Zeitpunkt im Datenzyklus die Wirkungsfolgen der endogenen und exogenen Entscheidungsfaktoren ausgeglichen werden.[617] Dazu gehört die Kompensation der Einwilligungsfolgen in den sozialen Medien,

615 EuGH, Urt. v. 13.05.2014 – C-131/12, Google Spain Sl ./. Gonzalez.

616 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I; BVerfG, Urt. v. 06.11.2019 – 1 BvR 276/17, Recht auf Vergessen II.

617 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 19 f.

die sich in Gestalt von Bewertungen oder Fehlbewertungen auf das Bild der personalen Identität aufgrund ihrer Dauerhaftigkeit auswirken und ein nachträgliches Interventionsinteresse begründen können.

Aus grundrechtlicher Perspektive geht es daher um ein *Recht auf Neubeginn* im online-Kontext, welches mit der Löschung von Kommentaren und Attributen zu personalen Identitäten im online-Kontext durch den Verantwortlichen realisiert wird. Inwieweit das Recht auf Vergessenwerden eine geeignete Kompensation darstellt und essentieller Bestandteil eines Identitätsverwaltungsmodells zu sein hat, soll im Folgenden analysiert werden. Dazu gehören die Einräumung einer Kontrollmöglichkeit für den Betroffenen durch das Recht auf Löschung (1.), die Durchführung der Löschpflichten durch den Verantwortlichen (2.), die mögliche Kompensation des Legitimationsdefizits mit einem Konzept der Informationsverjährung (3.) und einer abschließenden Bewertung (4.).

1. Kontrolle mit dem Recht auf Löschung, Art. 17 Abs. 1, Alt. 1 DSGVO

Der Betroffene hat das Recht gegenüber dem Verantwortlichen, die unverzügliche Löschung der ihn betreffenden personenbezogenen Daten zu verlangen und kann damit die Kontrolle über den Bestand der mit den Datensätzen verbundenen personalen Identitäten ausüben. Es geht bei dem Recht auf Löschung demnach um ein „Ur-Abwehrinstrument“[618] gegenüber dem Verantwortlichen als private oder staatliche Institution. Der Begriff des Löschens wurde gemäß § 3 Abs. 4 Nr. 5 BDSG a. F. definiert und umfasst das „Unkenntlichmachen gespeicherter personenbezogener Daten“. Demgegenüber bleibt der Begriff der Löschung in der DSGVO undefiniert und wird allein in der Legaldefinition der „Verarbeitung“ nach Art. 4 Nr. 2 DSGVO als das „Löschen oder die Vernichtung“ dem Vorgang der Verarbeitung personenbezogener Daten zugeordnet. Die Löschung der Daten werde insgesamt realisiert, wenn die personenbezogenen Daten unkenntlich gemacht werden, ohne dass dabei die Datenträger in physischer Hinsicht zerstört werden müssen.[619] Gleichwohl kann von dem Löschungsrecht der Informationsgehalt von Daten nur beschränkt erfasst werden, so dass sich die Frage nach dem Umfang und der Wirksamkeit des Löschungsrechts stellt.

---

618 *Spiecker gen. Döhmann*, KritV 2014, 28 (34).

619 *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2019, § 4 Rn. 47.

Im *Google Spain*-Urteil des EuGHs wurde die Verantwortlichkeit der Typisierungen und Erkenntniserlangung beim Suchmaschinenbetreiber gesehen und entsprechend die Notwendigkeit der Einräumung einer Löschoption durch den Verantwortlichen festgestellt.[620] Die Löschoption würde nicht unbeschränkt gelten, sondern bedarf der Abwägung des Schutzes der informationellen Selbstbestimmung gemäß Art. 7, 8 GRC mit der Meinungsfreiheit oder dem Informationsinteresse, Art. 17 Abs. 3 a) DSGVO. Gleichwohl hat der EuGH das Recht auf Vergessenwerden im online-Kontext anerkannt, indem bestimmte Informationen nach der Interessenabwägung nicht mehr mit dem Namen in Verbindung gebracht werden dürfen.[621]

Die Ausübung des Rechts auf Vergessenwerden ermöglicht keine absolute Kontrolle über die Informationen, sondern nur die relative Kontrolle, da die Informationen allein gegenüber dem datenverarbeitenden Verantwortlichen gelöscht werden können und nicht gegenüber Dritten. Jedoch suggeriere das Recht auf Vergessenwerden die absolute Kontrolle und damit den Optimismus, dass eine vollständige Löschung der personenbezogenen Daten möglich sei, was auf der Rechtfertigungsebene wiederum zu einer gesteigerten Einwilligungsbereitschaft auch gegenüber sensiblen Informationen führen kann und das Kontroll-Paradoxon wirken könne.[622] Damit geht es bei dem Recht auf Löschung auch um die Vermeidung der Perpetuierung des Erinnerns dahingehend, dass das Nicht-Erinnern ausgelöst werden solle, was aber kaum realisierbar sei.[623] Erschwerend kommen die Ubiquität der Datenverarbeitung und die vielfältigen Rekombinationsmöglichkeiten hinzu, nach denen die Datensätze vermehrt dezentral gespeichert werden und das Recht auf Vergessenwerden kaum umfassend umgesetzt werden könne, zumal die Speicherung in Typisierungen durch den Verantwortlichen erfolge und der Betroffene davon keine Kenntnis erlangen könne.[624] Somit wirkt sich das Recht auf Löschung allein gegenüber den Datensätzen als Kontrollrecht aus, schließt aber einen damit verbundenen Informationsgehalt oder das Fortbestehen von gewonnenen Erkenntnissen aus früheren Datenverarbeitungen nicht aus. Folglich wirken sich die Relativität der Informationen und ihre eingeschränkte Kontrollier-

620 EuGH, Urt. v. 13.05.2014 – C-131/12, Google Spain Sl ./. Gonzalez, Rn. 28, 37–39.
621 EuGH, Urt. v. 13.05.2014 – C-131/12, Google Spain Sl ./. Gonzalez, Rn. 99.
622 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 7 f.
623 *Spiecker gen. Döhmann*, KritV 2014, 28 (36).
624 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 71 Fn. 267.

barkeit nicht nur auf der Ebene der Einwilligungsfolgen aus, sondern auch auf der Ebene des Rechts auf Vergessenwerden.

Der mit dem Recht auf Vergessenwerden intendierte Zweck, einen *Neubeginn* für die personale Identität zu gewährleisten, unterliegt Beschränkungen, da die Rechtsausübung zu einem eigenen Informationsgehalt über den Rechtsausübenden führen kann. Dies könne zu einer unerwünschten Perpetuierung von Informationen über diesen führen, dem sog. Streisand-Effekt.[625] Nach diesem Effekt erlangen Informationen, die als unerwünscht gelten und möglichst vermieden werden sollen, eine gesteigerte Aufmerksamkeit und werden auf diese Weise bekannter als voher. Insgesamt besteht demnach kein Schutz dahingehend, welche Erkenntnisse aus den Daten generiert werden und welches Bild von einer personalen Identität erstellt wird, worin die eingeschränkte Wirkkraft des Rechts auf Vergessenwerden liegt. Folglich ist mit der relativen Kontrolle über das Recht auf Löschung nach der Sprachgebung des Bundesverfassungsgerichts von einer „Chance auf Vergessen"[626] auszugehen und bedarf zudem eines Verhaltens, das von einem „Vergessenwollen" getragen ist.[627] Erschwerend kann hinzukommen, dass der Verantwortliche zwar die Löschung der personenbezogenen Daten vornimmt, aber die vorgenommenen Typisierungen der Daten durch den Verantwortlichen und die damit verbundenen Erkenntnisse bestehen bleiben, worin *Spiecker gen. Döhmann* ein Vollzugsdefizit des Rechts auf Vergessenwerden sieht.[628]

2. Löschpflichten durch den Verantwortlichen, Art. 17 Abs. 1, Alt. 2, Abs. 2 DSGVO

Die Löschpflichten durch den Verantwortlichen werden ausgelöst durch die Zweckerreichung, den Widerruf der Einwilligung, wenn ein Widerspruch gegen die Datenverarbeitung eingelegt wurde, wenn die Datenverarbeitung unrechtmäßig war oder wenn ein datenfreier Eintritt in die Volljährigkeit ermöglicht werden soll, Art. 17 Abs. 1 a) – f) DSGVO. Darin sind die Eigenschaften der Identitätsverwaltung durch Kontrollmöglichkeiten

625 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 300 f.; *Spiecker gen. Döhmann*, KritV 2014, 28 (32).
626 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 123; *Masing*, NJW 2012, 2305 (2308).
627 BVerfG, Urt. v. 06.11.2019 – 1 BvR 16/13, Recht auf Vergessen I, Rn. 123.
628 *Spiecker gen. Döhmann*, KritV 2014, 28 (40 f.).

mit dem Widerruf der Einwilligung, dem Widerspruch gegen die Datenverarbeitung und die Chance auf einen datenfreien *Neubeginn* mit der Volljährigkeit abgebildet, so dass die Löschpflichten in diesen Konstellationen mit technischen Maßnahmen durch den Verantwortlichen realisiert werden müssen. Diese beginnen bereits *ex ante* zur Rechtfertigung bei den technischen und organisatorischen Maßnahmen, die eine wirksame Realisierung der Datenlöschung umfassen müssen, denn „Computer kennen keine Gnade des Vergessens“[629]. Dazu gehört die separate Speicherung von Datensätzen zu den personalen Identitäten und den generierten Profilen durch Aussonderung, so dass eine wirksame Löschung umsetzbar ist (EWG 26 S. 3) und den Anforderungen der Identitätsverwaltung Rechnung getragen werden kann. Im Einzelnen kann es um die Löschung von Berechtigungen und Nutzungsprotokollen gehen, mit denen die Auswertung des Nutzungsverhaltens möglich ist.[630] Dies lässt sich technisch mit dem Einsatz eines „digitalen Radiergummis“[631], der in bestimmten Zeitabständen aktiv wird, realisieren. Ebenso könnte es um die Verneinung bestehender Datensätze gehen, so dass die ursprünglichen Informationen mit dem Zusatz einer Negation versehen werden.[632] Diese Methoden könnten etwa bei der Auswertung des Nutzungsverhaltens von Arbeitnehmern und den Zugriff auf bestimmte Datenbanken eingesetzt werden, um nach der Zweckerreichung die Profile zu löschen. Auch wäre im „*Smart Home*“ der Einsatz von derartigen Löschungstechniken denkbar, um die Betroffenen vor der umfassenden Profilerstellung zu schützen.

Insgesamt hat der Verantwortliche den Löschanspruch nicht absolut umzusetzen. Der Löschanspruch erstreckt sich allein auf den Verantwortlichen und nicht auf Dritte. Gleichwohl war in der Fassung des EU-Parlaments der Wortlaut vorgesehen, dass die „Löschung *aller* Querverweise auf die personenbezogenen Daten bzw. aller Kopien und Replikationen“ von Dritten umfasst sein sollen, Art. 17 Abs. 1 DSGVO-E. Dieser vorgesehene Wortlaut wurde jedoch aufgegeben. Somit befindet sich der Verantwortliche in einem Spannungsfeld zwischen dem Recht auf Vergessenwerden und der wirksamen Umsetzung des *Rechts auf Neubeginn*. Denn es lassen sich die Daten löschen, ohne dabei die Informationen und Erkenntnisse über die personale Identität zu erfassen.

---

629 *Steinmüller*, Information, Modell, Informationssystem, S. 43.
630 *Lehnert/Luther/Christoph u.a.*, Datenschutz mit SAP, 2018, S. 129, 133, 287 f.
631 *Kalabis/Selzer*, DuD 2012, 670 (672 f.).
632 *Haft*, Einführung in die Rechtsinformatik, 1977, S. 31.

Folglich kann sich die Löschpflicht allein auf eine mögliche Leistung des Verantwortlichen beziehen, wozu die Löschung der Daten gehört. Weiter könne sich aus der Löschpflicht eine von *Spiecker gen. Döhmann* vorgeschlagene Beweislastumkehrregelung ergeben, mit der ein „ersichtliches Bemühen" über die Löschmaßnahmen nachgewiesen werden müsse.[633] Dies steht im Einklang mit der in Art. 17 Abs. 2 DSGVO enthaltenen Wertung, dass eine Löschpflicht gegenüber Dritten nicht bestehen kann und nur solche Maßnahmen ergriffen werden müssen, die „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten" möglich sind. Damit muss der Verantwortliche nachweisen, welche Maßnahmen zur Löschung möglich waren. Schließlich kommen die Einreden des Verantwortlichen gemäß Art. 17 Abs. 3 DSGVO in Betracht, die der Wirkkraft des Rechts auf Vergessenwerden gerade aufgrund von gesetzlichen Aufbewahrungspflichten oder der Meinungsfreiheit entgegenstehen können.

3. Kontrolle durch Informationsverjährung

Die Kontrollmöglichkeit aus dem Recht auf Vergessenwerden könnte in das bisher begründete Identitätsverwaltungsmodell mit dem von *Drackert* entwickelten Rechtsinstitut der Informationsverjährung erweitert werden. Die Informationsverjährung wird aus der Verjährungsdogmatik abgeleitet, wonach das Motiv, den Rechtsfrieden herbeizuführen, auf Informationen übertragen und ein Schutzmechanismus gegen die Verwendung veralteter Informationen geschaffen werden soll.[634] Darin kommt der Grundsatz *venire contra factum proprium* zum Ausdruck, dass der geschaffene Vertrauenstatbestand über die Verwendung der Informationen nicht überraschend durch Entkontextualisierung aufgehoben werden darf und vergessen gedachte Informationen doch noch zum Einsatz kommen können.

Wenn die Datenverarbeitung lange zurückliegt, könnten die Informationen nach einem bestimmten Zeitpunkt nicht mehr verwertbar sein. Wobei mit der Einrede der Informationsverjährung kein absolutes Verarbeitungsverbot einherginge, da Informationen relativ wirken und das Recht nur gegenüber dem Verantwortlichen geltend gemacht werden kann.[635] Die Einrede der Informationsverjährung könnte bei der Identitätsverwal-

633 *Spiecker gen. Döhmann*, KritV 2014, 28 (37).
634 *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 301.
635 *Ders.*, Die Risiken der Verarbeitung personenbezogener Daten, 2014, S. 70 f.

tung gegen Datenverarbeitungen zu einer personalen Identität ausgeübt werden, die nicht mehr auf aktuellen Datensätzen basieren. Demnach wäre eine auf die Identitätsverwaltung konzipierte Informationsverjährung in Gestalt der Befristung von personalen Identitäten denkbar, die den Schutz kontextspezifischer personaler Identitäten zeitlich beschränkt und nach einem bestimmten Zeitraum die personale Identität neu begründet werden würde.

Die Befristung personaler Identitäten stünde im Gleichlauf zu einem iterativen Einwilligungskonzept mit einer technischen Unterstützung durch ein *Dashboard-System*, welches dafür eingesetzt werden könnte, bestehende aktive kontextspezifische personale Identitäten einzusehen, um die (automatische) Löschung der Identitäten vorzunehmen. Damit könnte der kontextübergreifenden Verbindung von personalen Identitäten und der Entkontextualisierung von personalen Identitäten begegnet werden.

Insgesamt könnte mit der Notwendigkeit einer Befristung bestimmter personaler Identitäten das Legitimationsdefizit der Einwilligung oder der Rechtfertigung ohne aktive Handlung ausgeglichen werden. Denn es besteht aus verhaltensökonomischer Perspektive die Möglichkeit, dass die Ausübung der Rechte „vergessen“[636] werde und die Asymmetrie zwischen Verantwortlichem und Betroffenen zu einem späteren Zeitpunkt der Datenverarbeitung eine Verstärkung erfährt. Zudem besteht für den Betroffenen die Schwierigkeit, die Verwendung veralteter Datensätze in einer neuen personalen Identität zu erkennen und entsprechend sein Einrederecht geltend zu machen. Vielmehr ist es wahrscheinlich, dass der Betroffene eine vage Vermutung über das Fortwirken veralteter Datensätze hat und dies aber für die Geltendmachung der Einrede selten ausreichen wird. Demnach ist das Rechtsinstitut der Informationsverjährung dem Grunde nach vielversprechend, stößt jedoch auf Umsetzungsschwierigkeiten und sollte für die Identitätsverwaltung in eine Befristung personaler Identitäten umgewandelt werden.

4. Bewertung

Die Identitätsverwaltung umfasst Löschungsrechte, die durch das Recht auf Vergessenwerden gemäß Art. 17 DSGVO und den Widerruf der Einwilligung gemäß Art. 7 Abs. 3, 17 Abs. 1 b) DSGVO ausgeübt werden können. Die Einwilligung und das Recht auf Löschung stehen damit in direk-

636 *Hermstrüwer/Dickert*, Tearing the Veil of Privacy Law, 2013, S. 23.

ter Verbindung und können sich einander dahingehend bedingen, dass die Kenntnis über eine „*default*"-Option mit dem Recht auf Vergessenwerden zu einer gesteigerten Einwilligungsbereitschaft führen könne.[637] Genauso könnte die Kenntnis über eine automatische Löschung der Daten zu einem leichtfertigeren Umgang mit der Erteilung von Einwilligungen führen, wohingegen die Ausübung des Rechts auf Vergessenwerden und die Einrede der Informationsverjährung eine aktive Handlung voraussetzen, und damit einer bewußten Enstscheidung unterliegen würden. Wenn aber das Recht auf Vergessenwerden selbst vergessen werde, müsste für die Wirksamkeit von Löschungsrechten eine Einbeziehung dieses Phänomens im Identitätsverwaltungsmodell erfolgen.

Dieses könnte in einer technischen Gestaltung durch sog. „*information hiding*"[638] zur Risikominimierung über die Erkenntnismöglichkeiten liegen, mit der eine Überführung in den Schutzmechanismus der Intransparenz vorgenommen werden kann. Von der Einwilligung könnte umfasst sein, dass nach der Datenverarbeitung für eine personale Identität konstituierende Informationen unabhängig von der Zweckerreichung gelöscht werden. Dabei geht es um die Verzerrung von Erkenntnismöglichkeiten auch durch das Hinzufügen von sog. *Dummydaten*[639], die zu einem Gesamtbild einer personalen Identität zusammengeführt werden, mit dem die Schutzdimensionen über die informationelle Selbstbestimmung wiederhergestellt werden können. Demnach würde eine Ausgestaltung des Identitätsverwaltungsmodells mit der „Kontrolle von Intransparenz" die *Big Data*-Phänomene einbeziehen, so dass mit der Identitätsverwaltung die informationelle Selbstbestimmung in einer schützenden Variante ausgeübt werden kann. Mit der kontrollierten Intransparenz über den Gesamtdatensatz könne die mögliche Erkenntnis aus einer falschen Schlussfolgerung bestehen,[640] die einen eigenständigen Schutzbedarf auslöst aber keinen abschließenden Schutz entfaltet. Damit sei eine „*Symphonie der Intransparenz*"[641] durch das Blockieren und Freigeben von Daten[642] und dem damit einhergehenden Differenzierungsmonopol beim Betroffenen als Bestandteil eines Identitätsverwaltungsmodells in Erwägung zu ziehen, um damit eine Steigerung der Kontrolle über die Daten und Erkenntnismög-

637 *Dies.*, Tearing the Veil of Privacy Law, 2013, S. 16.
638 *Buchmann*, DuD 2015, 510 (511).
639 *Ders.*, DuD 2015, 510 (511).
640 *Spiecker gen. Döhmann*, KritV 2014, 28 (35); zum kalkulierbaren Nichtwissen als Schutzgegenstand, *Albers*, Informationelle Selbstbestimmung, 2005, S. 115.
641 *Luhmann*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 96.
642 *Ders.*, in: Baecker (Hrsg.), Die Kontrolle von Intransparenz, 2017, 96 (101).

lichkeiten herbeizuführen. Dies verlangt Differenzierungsentscheidungen über die Zusammensetzung der Datensätze der personalen Identitäten durch den Betroffenen und ist als Bestandteil der Identitätsverwaltung einzuordnen.

Das Risiko falscher Erkenntnisse kann mit einem Recht auf Vergessenwerden oder mit dem Recht auf Berichtigung gemäß Art. 16 DSGVO ausgeglichen werden. Damit lässt sich der Datensatz zu einer personalen Identität berichtigen, Art. 16 S. 1 DSGVO, vervollständigen oder mit einer Erklärung ergänzen, Art. 16 S. 2 DSGVO, was zwar zu einer faktischen Mehrverarbeitung führen würde, aber mit dem Interesse der Richtigstellung zu rechtfertigen ist. Ebenso ist als Vorrecht zum Recht auf Vergessenwerden das Recht auf einschränkende Verarbeitung gemäß Art. 18 DSGVO einzuordnen, wonach das Begehren eines Löschanspruches zu weitgehend wäre und etwa für die Verteidigung von Rechtsansprüchen der Erhalt bestimmter Daten begehrt wird.

Neben der Informationsverjährung und Befristung von personalen Identitäten sollte ein Recht auf Vergessenwerden als „Chance auf Vergessen" im Identitätsverwaltungsmodell einbezogen werden. Gleichwohl besteht bei der Informationsverjährung die praktische Schwierigkeit für den Betroffenen, die Verwendung veralteter Datensätze für eine wirksame Rechtsausübung zu erkennen. Demnach sollte für ein Identitätsverwaltungsmodell die Befristung personaler Identitäten einbezogen werden, womit man den praktischen Umsetzungsschwierigkeiten eines Informationsverjährungsrechts begegnen kann. Weiter können in Anbetracht wirkender verhaltensökonomischer Verzerrungen über das Recht auf Vergessenwerden bewusste Differenzierungsentscheidungen über die Intransparenz zu einer Gestaltung personaler Identitäten im online-Kontext führen und das Recht auf Vergessenwerden würde als Steuerungsinstrument fungieren. Denn die Intransparenz und das Vergessen seien die Voraussetzung und Grundlage für den Prozess der Evolution und des Lernens,[643] welches sich auf die „Evolution der Identität" im Sinne eines Neubeginns übertragen lässt.

Das Recht auf Vergessen findet seine Erweiterung in Gestalt des Vergessens bei einem bestimmten Verantwortlichen durch das „Schwesterrecht"[644] der Datenübertragbarkeit gemäß Art. 20 DSGVO. Mit diesem Recht wird die Übertragung der Datensätze an einen neuen Verantwortlichen ermöglicht.

643 *Spiecker gen. Döhmann*, KritV 2014, 28 (34) mwN.
644 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (72).

III. Datenübertragbarkeit zur Identitätsverwaltung, Art. 20 DSGVO

Das Recht auf Datenübertragbarkeit enthält mit dem Recht zur Übertragung der Datensätze über eine personale Identität die Grundlage für die Identitätsverwaltung. Mit diesem Recht wird einerseits die informationelle Selbstbestimmung gemäß Art. 7, 8 GRC geschützt und andererseits erfolgt die Stärkung des Betroffenen gegenüber dem ökonomischen Phänomen der „*lock in*"-Effekte, wonach Betroffene nur unter erschwerten Bedingungen den Dienst wechseln können.[645] Demnach soll mit dem Recht auf Datenübertragbarkeit ein „*empowerment*"[646] der Betroffenen erfolgen und zugleich der Wettbewerb zwischen den Diensten zur Bereitsstellung von Wechselmöglichkeiten gefördert werden, so dass Art. 20 DSGVO auch als „Nutzerschutzrecht" fungiere.[647] Denn mit der umfangreichen Nutzung eines Dienstes etwa in sozialen Netzwerken kann eine faktische Sogkraft einhergehen, in die mit dem Recht auf Datenübertragbarkeit interveniert werden kann. Gleichzeitig lässt sich mit dem Recht auf Datenübertragbarkeit ein Anreizmechanismus für den Markt schaffen, etwa um Mitarbeiterdaten von dem ursprünglichen Arbeitgeber zu einem neuen Arbeitgeber zu übertragen oder den Wechsel von beruflichen online-Netzwerken erleichtern zu können.

Mit dem Recht auf Datenübertragbarkeit soll somit eine „bessere Kontrolle über die eigenen Daten" mit „automatischen Mitteln" ermöglicht werden, mit denen der Betroffene die Daten in einem „strukturierten, gängigen, maschinenlesbaren und interoperablen Format" erhalten kann, EWG 68 S. 1. Damit wird dem Betroffenen die Kontrolle über die Kontextänderung eingeräumt, so dass das Recht ein Minus zum Recht auf Vergessenwerden darstellt. Da gegenüber dem ursprünglichen Verantwortlichen die Datensätze zur personalen Identität vergessen werden müssen, aber gegenüber dem neuen Verantwortlichen die Datensätze verfügbar sein sollen, unterliegen die Daten einer Wiederverwendbarkeit. Demnach soll zunächst das Kontrollrecht des Betroffenen dargestellt werden (1.), anschließend die Durchführung der Datenübertragbarkeit durch den Verantwortli-

645 *Veil*, in: Gierschmann/Schlender/Stentzel u.a. (Hrsg.), Kommentar Datenschutz-Grundverordnung, 2017, Art. 20 DSGVO Rn. 3.

646 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 5.

647 *Reinhardt*, AöR 142 (2017), 528 (557) spricht von faktischer Sogkraft; *Roßnagel/Richter/Nebel*, ZD 2013, 103 (107).

chen (2.) und schließlich die Datenübertragbarkeit als Grundlage der Identitätsverwaltung begründet werden (3.).

1. Kontrolle mit dem Recht auf Datenübertragbarkeit

Die Ausübung des Rechts auf Datenübertragbarkeit begründet gegenüber dem Verantwortlichen die Kontrolle zur Übertragung der Datensätze in einen anderen Kontext und ermöglicht die kontextbezogene Verwaltung der Datensätze zu personalen Identitäten. Die Kontrolle liegt in dem Recht auf Geltendmachung der Datenübertragbarkeit und in dem „qualifizierten Herausgabeanspruch der betroffenen Person bezüglich ihrer Daten“[648]. Dazu gehört, dass die betroffene Person die bereitgestellten Daten in einem strukturierten und maschinenlesbaren Format erhält. Gemäß Art. 20 Abs. 1 DSGVO sind von dem Recht solche Daten erfasst, die „bereitgestellt“ wurden und als „*user-generated content*“ gelten. Der Wortlaut „bereitgestellt“ setzt eine aktive Handlung voraus, so dass durch physische Bewegung entstandene passiv generierte Daten etwa von einem Fitnesstracker oder Profildaten möglicherweise nicht erfasst sind, wie es von *Janal*[649] vertreten wird.

Für die Identitätsverwaltung mit dem Recht auf Datenübertragbarkeit ist die vollständige Übertragbarkeit der Daten und Erkenntnisse erforderlich, um die Verwaltung der *Idem*- und *Ipse*-Anteile personaler Identitäten umfassend realisieren zu können. Folglich könnte mit der Einwilligung oder der Nutzung des Dienstes die mit dem Begriff „bereitgestellt“ geforderte aktive Handlung konsumiert sein, so dass alle kausal auf die Einwilligung folgenden Datenverarbeitungen von dem Recht auf Datenübertragung erfasst wären. Eine derartige Auslegung wäre zwar zum Schutz der personalen Identitäten wünschenswert, erscheint aber in Anbetracht des eindeutigen Wortlautes und Gesetzeszwecks, „*lock in*“-Effekte zu mindern, konstruiert. Demnach sind von Art. 20 Abs. 1 DSGVO die Übertragung der erhobenen Daten, Metadaten und Nutzungsdaten umfasst,[650] wohingegen die Transaktionsdaten, Daten mit gesetzlicher Speicherungspflicht gemäß Art. 6 Abs. 1 c) – f), Art. 9 Abs. 2 b) – j) DSGVO und Kommunikationsdaten mit Dritten vom Übertragungsrecht ausgeschlossen sein sol-

648 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 21.
649 *Janal*, JIPITEC 2017, 59 (61) Rn. 8.
650 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 18 f.

len.[651] Demgegenüber wären die vom Verantwortlichen erlangten Erkenntnisse aus den Daten und die generierten Profile vom Recht auf Datenübertragbarkeit nicht erfasst, da sie nicht aktiv bereitgestellt wurden.

Gleichwohl ist dem Schutzzweck des Rechts auf Datenübertragbarkeit zu entnehmen, dass die vom Verantwortlichen erlangten Erkenntnisse ein Faktor für die Steigerung der „*lock in*"-Effekte sind, und demnach es dem Schutz der informationellen Selbstbestimmung entspräche, diese Erkenntnisse dem neuen Dienstanbieter „mitzugeben". Insgesamt ist aber der Wortlaut des Art. 20 DSGVO dahingehend eindeutig, dass sich das Recht auf die aktiv „bereitgestellten" Daten beschränkt. Zwar wird mit dem Recht auf Datenübertragbarkeit ein hohes Kontrollmaß über die personalen Identitäten geschaffen, da sich aber die Kontrolle auf die Datensätze im ursprünglichen Kontext bezieht, lässt sich die Kontrolle nicht auf die umfassenden personalen Identitäten in ihren *Ipse*-Anteilen ausweiten.

2. Datenübertragung durch den Verantwortlichen

Die Datenübertragung muss in organisatorischer und technischer Hinsicht durch den Verantwortlichen umgesetzt werden. Dazu gehört die Aussonderungsfähigkeit der zu dem Betroffenen gehörenden Daten von dem Gesamtdatensatz und spezifizierte Schnittstellen zur Übertragung der Datensätze über eine personale Identität an den neuen Verantwortlichen. Mit der Beschränkung des Rechts auf Datenübertragbarkeit auf die „bereitgestellten" personenbezogenen Daten ist eine differenzierte Strukturierung und Speicherung der Nutzer-, Transaktions- und Metadaten erforderlich, damit der Datenexport nach der Geltendmachung des Rechts auf Datenübertragbarkeit ermöglicht werden kann. Bei dem exportierenden Verantwortlichen müssen interoperable Formate zur Gewährleistung der Datenübertragbarkeit eingerichtet werden und der importierende Verantwortliche muss die technischen Bedingungen zur Annahme der Daten herstellen. Dabei wird in EWG 68 S. 2 der Verantwortliche dazu aufgefordert, interoperable Formate zu entwickeln, worin aber keine Verpflichtung erkennbar ist. Vielmehr liegt aufgrund des Wortlautes „sollen" ein Empfehlungscharakter in der Regelung, wozu es gehöre, sich mit dem importierenden Verantwortlichen in Verbindung zu setzen.[652] Eine weitere Be-

651 *Janal*, JIPITEC 2017, 59 f.

652 *Veil*, in: Gierschmann/Schlender/Stentzel u.a. (Hrsg.), Kommentar Datenschutz-Grundverordnung, 2017, Art. 20 DSGVO Rn. 55.

schränkung des umfassenden Übertragungsrechts liegt in dem technischen Machbarkeitsvorbehalt gemäß Art. 20 Abs. 2 a. E. DSGVO, EWG 68 S. 8. Danach könnte das Recht auf Datenübertragbarkeit eine Einschränkung erfahren, wenn die Bereitstellung und Übertragung der Datensätze mit unverhältnismäßigem Aufwand verbunden sind. Folglich erscheint es wünschenswert, wenn sich die bereits bestehenden Interoperabilitätsregelungen in der eIDAS-VO zur grenzüberschreitenden Identifizierung für die umfassende Übertragung der personalen Identitäten im Datenschutzrecht als Regelungsvorbild heranziehen ließen.

Die von dem Verantwortlichen gewählte Interoperabilitätsmethode kann in einer detaillierten Form zum Bestandteil der Informationspflichten gemäß Art. 13 Abs. 2 b) DSGVO werden, so dass bei der Löschung oder Sperrung des „*Accounts*" von dem Recht auf Datenübertragbarkeit Gebrauch gemacht werden kann. Damit könnte ein Anreiz für den Verantwortlichen geschaffen werden, um an einem hohen Interoperabilitätsniveau mitzuwirken und dieses transparent zu machen. Diese Umsetzung der Anforderungen nach Art. 20 DSGVO könnte zu einer wettbewerblichen Dynamik führen, in der Dienstanbieter mit der Gewährleistung eines ausdifferenzierten Datenübertragbarkeitssystems eine gesteigerte Nachfrage erfahren könnten. Gleichzeitig ist eine Beeinflussung des Wettbewerbes mit dem Verlangen eines Entgeltes für die Datenübertragbarkeit denkbar und wird als rechtlich nicht ausgeschlossen angesehen.[653] Gleichwohl wurde festgestellt, dass sich Verhalten an Gratifikationen orientiert,[654] so dass die Zahlung eines Entgeltes den Betroffenen von der Geltendmachung des Rechts auf Datenübertragbarkeit abhalten könnte. Demnach erscheint ein Anreizmechanismus für den Betroffenen mit monitären Gratifikationen, wie es etwa bei dem Wechsel von Finanzdienstleistern verbreitet ist, naheliegender. Folglich könnte etwa ein berufliches online-Netzwerk damit werben, dass bei einem Wechsel zu diesem eine bestimmte Gratifikation in Gestalt von Prämien erfolgt.

3. Datenübertragbarkeit als Grundlage der Identitätsverwaltung

Das Recht auf Datenübertragbarkeit fungiert durch die Kontrolle der Kontextänderung als Grundlage für die Identitätsverwaltung. Sobald sich zwi-

653 *Ders.*, in: Gierschmann/Schlender/Stentzel u.a. (Hrsg.), Kommentar Datenschutz-Grundverordnung, 2017, Art. 20 DSGVO Rn. 15, 44.

654 4. Teil, C., II., 1., d).

schen dem Verantwortlichen und dem Betroffenen das Machtungleichgewicht derart manifestiert hat, dass die Ausübung des Rechts auf Datenübertragbarkeit zu einer „*re-balance*“[655] zugunsten des Betroffenen führe, kann von einer zumindest partiellen Wiederherstellung der informationellen Selbstbestimmung ausgegangen werden. Damit würde das Recht auf Datenübertragbarkeit seine Funktion als Nutzerschutzrecht entfalten.

In Anbetracht der *Big Data*-Phänomene des Internets der Dinge erscheint die Interoperabilität aus der ökonomischen Perspektive wegen der gesteigerten Nutzbarkeit von Daten über mehrere Komponenten hinweg als Wettbewerbsvorteil.[656] Dies kann einerseits zu erneuten „*lock in*“-Effekten und andererseits zu einer Steigerung des Kontrollniveaus bei dem Betroffenen führen. Dieses Kontrollniveau lässt sich in dem *Dashboard-System* abbilden. So schlägt die Artikel-29-Gruppe vor, dass extrahierte Daten aus einem Datenset in ein „*Tool*“ übertragen werden sollen, mit dem die Zugangsverwaltung ermöglicht wird,[657] was über das *Dashboard-System* zur Identitätsverwaltung abgebildet werden könnte. Denn über das *Dashboard-System* lässt sich der Zugang zu den extrahierten Datensätzen einräumen, die im Rahmen des Rechts auf Datenübertragbarkeit von dem Betroffenen kontrolliert in einen anderen Kontext überführt werden.

Solch ein Konzept würde eine Bündelung der Funktionalitäten von Diensten umfassen und wäre vergleichbar mit Passwortmanagern, die als Assistenzsystem für die Verwaltung einer hohen Anzahl von Passwörtern zu diversen online-Kontexten dienen. Die von Intermediären angebotenen *Single Sign-On*-Lösungen gewährleisten bereits eine interoperable Übertragung personaler Identitäten über die Benutzerdaten. Mit der Klarnamenpflicht und dem damit verbundenen Vertrauensmaß schaffen *Facebook* und *Google* eine diensteübergreifende Identifizierungsmöglichkeit und bündeln die Funktion der Identifizierung.

In Anbetracht der Marktmacht über die generierten personalen Identitäten durch einen Intermediär erscheint die Öffnung gegenüber weiteren Identitätsverwaltungsdiensten vorzugswürdig. Entsprechend ist die Identitätsverwaltung mit staatlich zertifizierten Identitätsattributen denkbar, wie es etwa der elektronische Personalausweis vorsieht. Damit enthalten die *Idem*-Anteile einer personalen Identität im online-Kontext ein hohes Ver-

655 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 4.
656 *Kerber/Schweitzer*, JIPITEC 2017, 39 (42) Rn. 11.
657 *Art. 29 Data Protection Working Party*, WP 242, Guidelines on the right to data portability (5. April 2017), S. 16.

trauens- und Sicherheitsniveau, was sich auch auf den privaten Rechtsverkehr übertragen ließe.

In rechtlicher Hinsicht könnte eine Erweiterung des Rechts auf Datenübertragbarkeit durch die Umwandlung der Soll-Vorschrift des Art. 20 DSGVO, EWG 68 in eine Muss-Vorschrift mit der Aufhebung des technischen Machbarkeitsvorbehalts erfolgen. Ebenso wären auf der rechtlichen Gestaltungsebene entsprechende Nutzungsbedingungen mit den Interoperabilitätsanforderungen als wettbewerbsfördernder Vertragsbestandteil denkbar, so dass sich der Betroffene bei der Wahl des Dienstes an dem potentiellen Interoperabilitätsniveau orientieren könnte. Damit würden Kontrollmöglichkeiten über personale Identitäten eingerichtet und gesteigert werden, wie sie aus Art. 17, 20 DSGVO abgeleitet wurden.

Mit der Kontrollmöglichkeit aus dem Recht auf Datenübertragbarkeit verbleibt gerade bei einem hohen Interoperabilitätsmaß das Risiko eines Angriffes etwa auf die Integrität, Authentizität und Vertraulichkeit von Schnittstellen. Dies gilt besonders, wenn die Bestimmung der Verantwortlichkeiten im Rahmen der „systemischen Digitalisierung“[658] hinsichtlich der Zuständigkeit über die Vermeidung eines IT-Sicherheitsvorfalles erschwert sein kann.

Für ein Identitätsverwaltungsmodell könnte etwa das Risiko korrumpierter personaler Identitäten bestehen, welches in einem *Dashboard-System* mit entsprechenden IT-Sicherheitsmaßnahmen einzubeziehen wäre. Insbesondere könnte eine unmittelbare Verbindung von dargestellten personalen Identitäten mit dem Widerspruchsrecht gemäß Art. 21 DSGVO eine Lösung für den Schutz der informationellen Selbstbestimmung darstellen. Denn mit diesem Recht könnte die personale Identität in Gestalt eines Profils mit dem Zusatz „unwahr“ versehen werden, wodurch die Authentizität einer personalen Identität in Frage gestellt und dies für Dritte erkennbar gemacht werden würde. Damit könnte das auf Zugangsrechte beschränkte Identitätsverwaltungsmodell erweitert werden, so dass über die Daten hinaus die Erkenntnisse zur personalen Identität in relativer Hinsicht kontrollierbar werden.

4. Ergebnis

Das Recht auf Datenübertragbarkeit sollte hinsichtlich der bestehenden Soll-Vorschrift des Art. 20 DSGVO, EWG 68 in eine Muss-Vorschrift um-

658 *Spiecker gen. Döhmann*, CR 2016, 698 (703).

gewandelt werden, damit die verantwortlichen Stellen die Interoperabilität für einen Wechsel gewährleisten. Dabei könnte als Interoperabilitätsschnittstelle ein *Dashboard-System* fungieren, das den Zugang zu den Datensätzen über den *Ipse-* und *Idem*-Anteil personaler Identitäten ermöglicht. Hierbei wäre es *de lege ferenda* wünschenswert, wenn über die „bereitgestellten" Daten hinaus auch die Profile erfasst werden. Damit würde dem Betroffenen ein Recht eingeräumt werden, das ein echtes Gegengewicht zu Machtungleichgewichten darstellt und die Kontrolle über die Kontextänderung und damit verbundene Informations- und Erkenntnismöglichkeiten erleichtert. Dabei könnten für einen Wechsel etwa finanzielle Prämien durch den neuen Dienstanbieter in Aussicht gestellt werden. Somit enthält das Recht auf Datenübertragbarkeit nach derzeitiger Rechtslage eine wesentliche Grundlage für die Identitätsverwaltung im Hinblick auf die ermöglichte Kontextänderung.

IV. Kontrolle gegen automatisierte Entscheidungen, Art. 22 Abs. 2 DSGVO

Für die Identitätsverwaltung bedarf es neben der Kontrolle der Daten und Erkenntnisse über eine personale Identität der Kontrolle über das Ergebnis einer automatisierten Verarbeitung, die eine unmittelbare rechtliche Wirkung entfaltet. Von der automatisierten Entscheidung ist gemäß Art. 4 Nr. 4 DSGVO jegliche Form einer automatisierten Verarbeitung personenbezogener Daten zur Analyse oder Prognose von Aspekten bezüglich der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben oder Interessen, der Zuverlässigkeit oder des Verhaltens, des Aufenthaltsortes der betroffenen Person, soweit dies eine rechtliche Wirkung für den Betroffenen entfaltet, umfasst. Damit kann die personale Teilidentität, die auf der automatisierten Einzelentscheidung im Kontext des Arbeitsplatzes oder im Gesundheitskontext basiert, zum Gegenstand einer Entscheidung mit unmittelbarer rechtlicher Wirkung[659] werden, so dass es jeweils um den Schutz der kontextspezifischen personalen Teiliden-

659 Der Streit, ob positive rechtliche Wirkungen vom Wortlaut erfasst sind, wird von der Literatur (*Schulz*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 22 DSGVO Rn. 22; *Buchner*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 22 DSGVO Rn. 25) mit dem Argument des Wortlauts gemäß Art. 22 Abs. 1 DSGVO „*rechtliche Wirkung oder eine in ähnlicher Weise erhebliche Beeinträchtigung*" verneint. Dieser würde auf eine negative rechtliche Wirkung abstellen. Demgegenüber ließe

tität geht. Die mit der automatisierten Einzelentscheidung begründete Identität darf nicht dazu führen, dass die natürliche Person mit ihren Persönlichkeitsmerkmalen zum Objekt der Entscheidung gemacht wird. Folglich bedarf es einer weiteren Prüfung über die „besondere Richtigkeitsgewähr“[660] dieser automatisierten Entscheidung als generierte personale Identität, die den Wahrheitsgehalt der personalen Identität und den Schutz vor einer vom Algorithmus ausgelösten diskriminierenden Entscheidung umfasst, die sich in dem digitalen Identitätsbild manifestieren kann. Darin wird ein entscheidender Schutzbedarf bei der automatisierten Einzelentscheidung und der damit generierten personalen Identität gesehen.[661]

Auch an dieser Stelle kann die Kontrolle durch die Transparenz über die involvierte Logik des automatisierten Entscheidungsprozesses gemäß Art. 13 Abs. 2 f) DSGVO erfolgen. Ebenso ermöglicht die Rechtfertigung über die Einwilligung die Kontrolle des Betroffenen, die sich auf die systematische Stellung des Art. 22 DSGVO als spezifisches Betroffenenrecht[662] und der damit verbundenen Kontrollmöglichkeit erstreckt. Dagegen bedarf es der Einräumung einer weiteren Kontrollmöglichkeit für den Betroffenen bei der Rechtfertigung der automatisierten Entscheidung ohne aktive Handlung über den Vertragsabschluss oder eine Rechtsvorschrift etwa einer Kollektivvereinbarung, Art. 22 Abs. 2 a) – b) DSGVO. Weiter hat der Verantwortliche gemäß Art. 22 Abs. 3 DSGVO die erforderlichen Maßnahmen zur Wahrung der berechtigten Interessen des Betroffenen zu treffen, etwa durch einen einzurichtenden Anspruch auf Eingreifen in die automatisierte Einzelentscheidung. Gemäß EWG 71 S. 4 wäre dieser Anspruch des Betroffenen auf ein Eingreifen durch den Verantwortlichen iterativ auszugestalten und umfasst die Darlegung des eigenen Standpunkts, den Anspruch auf Erläuterung der Entscheidung und das Recht auf Anfechtung dieser Entscheidung. Aus diesem iterativen Konzept kann eine Verhandlungsstruktur abgeleitet werden, die eine Intervention in die automatisierte Entscheidung und die daraus generierte personale Identität er-

---

sich für die Annahme des Schutzes gegen positive rechtliche Wirkungen anführen, dass mit der automatisierten Entscheidung eine „neue“ auf dem Algorithmus basierende personale Identität generiert werden könne und eine gravierende Abweichung zur realen personalen Identität darstellen kann, vgl. *Brecht/Steinbrück/Wagner*, PinG 2018, 10.

660 *Albers*, Informationelle Selbstbestimmung, 2005., S. 535.

661 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (48).

662 *Schulz*, in: Gola/Eichler/Franck u.a. (Hrsg.), Kommentar, Datenschutz-Grundverordnung, 2018, Art. 22 DSGVO Rn. 6.

möglicht. Das darin abgebildete Recht auf Begründung des Ergebnisses der automatisierten Entscheidung erscheint nach *Edwards/Vaele* nur als ein schwaches Recht, da dieses iterative Konzept als Soll-Vorschrift und nicht als Muss-Vorschrift geregelt ist.[663] Dennoch könnte EWG 71 S. 4 als Vorlage für ein *iteratives Verhandlungskonzept* herangezogen werden und als risikominimierende Maßnahme in der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 3 a) DSGVO in die Gesamtrisikobewertung einfließen. Ebenso könnte das *iterative Verhandlungskonzept* in technischer Hinsicht in das *Dashboard-System* integriert werden, so dass die technische Komplexität der automatisierten Einzelentscheidung über die personale Identität transparent wird und sich die Maßnahmen zum Schutz des Betroffenen treffen lassen.

Weil mit der automatisierten Einzelentscheidung aufgrund der hohen Komplexität des Entscheidungsverfahrens gegenüber dem Betroffenen Einschüchterungseffekte[664] eintreten können, bedarf es der Wiederherstellung des Kontrollniveaus über die personale Identität aus der automatisierten Einzelentscheidung. Denn bei dieser generierten personalen Identität ist ein Kontrollverlust eingetreten, der kompensationsbedürftig ist. Diese Kompensation könnte durch das beschriebene *iterative Verhandlungsmodell* in einem *Dashboard-System* erfolgen, mit dem eine Angleichung zwischen personaler Identität aus der automatisierten Entscheidung und aus der informationellen Selbstbestimmung erfolgen würde.

V. Transparente Datenschutzverstöße als Bestandteil der Identitätsverwaltung, Art. 33 DSGVO

Nach der Rechtfertigung der Datenverarbeitung kann die Verletzung des Schutzes personenbezogener Daten direkten Handlungsbedarf bei dem Verantwortlichen oder Betroffenen auslösen. Dafür bedarf es der Transparenz über den Datenschutzverstoß, wie es in Art. 33, 34 DSGVO geregelt wird. Diese Regelungen gehören zu dem zweiten Abschnitt des vierten Kapitels, wonach die „Sicherheit personenbezogener Daten" geregelt wird, die bereits zu den Grundsätzen der Datenverarbeitung gehört, Art. 5 Abs. 1 f) DSGVO. Dazu gehören die Meldepflicht durch den Verantwortlichen gemäß Art. 33 DSGVO gegenüber der Aufsichtsbehörde und gemäß Art. 34 DSGVO bei einem hohen Risiko für die Rechte und Freiheiten na-

663 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (50).
664 *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 47.

türlicher Personen gegenüber dem Betroffenen. Weiter hat der Betroffene gemäß Art. 77 Abs. 1, Art. 57 Abs. 1 f) DSGVO ein direktes Beschwerderecht bei der Aufsichtsbehörde, wenn die Ansicht eines mutmaßlichen Verstoßes gegen die Verordnung besteht.

Wann eine „Verletzung des Schutzes personenbezogener Daten" und damit der personalen Identitäten gegeben ist, wird gemäß Art. 4 Nr. 12 DSGVO legaldefiniert und umfasst „eine Verletzung der Sicherheit, die (…) zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt (…)". Für die Gewährleistung der *ex post* Transparenz einer Verletzung durch den Verantwortlichen ist der risikobasierte Ansatz über die Prognose des Schadens und der Eintrittswahrscheinlichkeit einzubeziehen,[665] da der Verletzungsbegriff das eingetretene Risiko umschreibt.

Für die Realisierung eines effektiven Schutzes ist die Schaffung der Transparenz über die Verletzung der personalen Identität maßgeblich. Dabei muss nicht zwingend ein materieller oder immaterieller Schaden vorliegen, sondern es genügt einer der in Art. 4 Nr. 12 DSGVO aufgelisteten Vorgänge. Insbesondere kann gemäß EWG 85 S. 1 der Kontrollverlust über die personenbezogenen Daten bereits eine Verletzung des Schutzes personenbezogener Daten bedeuten. Erst mit der Transparenz über diese neue Risikolage im Datenzyklus kann der Betroffene gemäß Art. 34 DSGVO, EWG 86 S. 2, basierend auf einer Empfehlung durch den Verantwortlichen, die notwendigen Vorkehrungen zum Schutz seiner personalen Identität treffen. Weiter sind Informationen über die „betroffenen Kategorien" personenbezogener Daten, die „ungefähre(n) Zahl der betroffenen personenbezogenen Datensätze" und die Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen an die Aufsichtsbehörde mitzuteilen, Art. 33 Abs. 3 a) 2. Hs., Art. 33 Abs. 3 d) DSGVO. Gleichzeitig unterliegt die Informationsmitteilungen dem Machbarkeitsvorbehalt des Verantwortlichen.[666]

Die Vorkehrungen des Betroffenen können konkret etwa zu einer Passwortänderung oder innerhalb der Identitätsverwaltung zu der Geltendmachung des Rechts auf Vergessenwerden oder des Rechts auf Datenübertragbarkeit führen. Mit dem Transparenzerfordernis aus Art. 33, 34 DSGVO

665 *Jandt*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 33 DSGVO Rn. 9.

666 *Martini*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 33 DSGVO Rn. 47.

über die Verletzungen und der damit einhergehenden Schutzmöglichkeit des Betroffenen wird nachträglich zur Datenverarbeitung ein „vorbeugender Persönlichkeitsschutz“[667] gewährleistet. Hierin liegt erneut ein verfahrensrechtlich ausgestaltetes Schutzkonzept[668] *ex post* zur Rechtfertigung vor, welches in dem Identitätsverwaltungsmodell einzubeziehen wäre. Es könnten konkrete Handlungsoptionen etwa über ein *Dashboard-System* für den Betroffenen zum Schutz gegen korrumpierte personale Identitäten durch die Verletzung personenbezogener Daten eingeräumt und damit ein weiteres Schutzregime geschaffen werden. Insgesamt enthalten die Vorgaben der Art. 33, 34 DSGVO eine indirekte Kontrollmöglichkeit, die mit der *ex post* Transparenz zu einem späteren Zeitpunkt des Datenzyklus dem Betroffenen dienen können.

Darüber hinaus setzen Art. 33, 34 DSGVO die Dokumentation der Datenverarbeitung gemäß Art. 5 Abs. 2 DSGVO voraus, die die Vorbereitung der Datenverarbeitung und die fachliche Auseinandersetzung zur Maßnahmenfindung für den gesamten Datenverarbeitungsvorgang umfasst. Diese Dokumentation kann in der Zusammenarbeit mit der Aufsichtsbehörde gemäß Art. 31, 33 DSGVO hinsichtlich des Verstoßes gegen die Sicherheit personenbezogener Daten einbezogen werden. Hiermit wird ein kooperativer Austausch über die Ursachen des Sicherheitsverstoßes und die möglichen Abhilfemaßnahmen auch unter Offenlegung der Datenverarbeitungsvorgänge vorgenommen. Nach *Martini* werden die Strategien zur Einhaltung der datenschutzrechtlichen Vorgaben ebenso von der Dokumentationspflicht umfasst,[669] was in Anbetracht unternehmerisch motivierter Geschäftsgeheimnisse als weitgehend eingeordnet werden kann. Gleichzeitig wird damit die Verantwortungszuschreibung im Sinne des Konzeptes der „*Accountability*“ zur wirksamen Umsetzung der datenschutzrechtlichen Pflichten sichergestellt. Indem die Rechenschaftspflicht sich auch auf die Exkulpationsmöglichkeit gegenüber der Aufsichtsbehörde bezieht, aber in Anbetracht der praktischen Unmöglichkeit, jeden Schritt dokumentieren zu können, sei der Umfang der Dokumentationspflicht restriktiv auszulegen.[670] Eine Einschränkung der Dokumentationspflichten gilt ebenfalls, wenn der Verantwortliche gemäß Art. 42 DSGVO zertifiziert ist, da mit

667 *Ders.*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 33 DSGVO Rn. 1.
668 *Ders.*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 33 DSGVO Rn. 10.
669 *Ders.*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 24 DSGVO Rn. 40.
670 *Veil*, ZD 2018, 9 (16).

der Zeritifizierung bereits der Nachweis und die Rechenschaft über die Umsetzung der zertifizierungsrelevanten Vorgaben erfolgt ist.

VI. Kontrolle durch gerichtlichen Rechtsbehelf, Art. 79 DSGVO

Als *ultima ratio* der Kontrolle nach der Rechtfertigung und bei einem Verstoß gegen die Datenschutzgrundverordnung kann die Durchsetzung möglicher Schadensersatzansprüche über den Gerichtsweg erfolgen. Die Kontrolle der personalen Identitäten lässt sich mit dem in Art. 79 Abs. 2 S. 2 DSGVO statuierten Wahlrecht über den Gerichtsort darstellen, da der Betroffene sich über den Gerichtsort mit einem für ihn günstigen Schutzregime informieren und den Ort der Klageeinreichung wählen kann, sog. „*forum shopping*". Der Betroffene hat ein Wahlrecht zwischen dem Gerichtsort, in dem der Verantwortliche seine Niederlassung hat und dem Gerichtsort, bei dem der Betroffene seinen Aufenthaltsort hat, Art. 79 Abs. 2 S. 1, 2 DSGVO.[671] Dieses Wahlrecht ist entscheidend, wenn der Ort der Niederlassung des Verantwortlichen und der Aufenthaltsort des Betroffenen auseinanderfallen und an dem jeweiligen Gerichtsort ein unterschiedliches Schutzniveau von den Gerichten entschieden wird.

Insofern wirkt sich in der Identitätsverwaltung die Wahl des Gerichtsortes aus, die sich auf das zu erzielende datenschutzrechtliche Schutzniveau der personalen Identitäten bezieht. Sobald der Betroffene die Verletzung seiner Rechte und Freiheiten gerichtlich geltend macht, würde das Schutzniveau der personalen Identitäten in der gerichtlichen Bewertung in gewissem Maße ebenfalls der Kontrolle des Betroffenen unterliegen. Demnach könnte zu einem Identitätsverwaltungsmodell die Transparenz über den hypothetischen Gerichtsort bei der konkreten Datenverarbeitung gehören.

671 Ebenso wurde ein Wahlrecht bei der Geltendmachung einer Verletzung von Persönlichkeitsrechten, die durch Inhalte auf der Webseite erfolgt sind, in der eDate-Entscheidung des EuGHs anerkannt. Demnach könne zwischen dem Gerichtsort, an dem der Zugang zur Webseite besteht, oder dem Gerichtsort, an dem der Urheber niedergelassen ist, oder dem Gerichtsort, in dem der Schwerpunkt der Interessen des Geschädigten liegt, gewählt werden; EuGH, Urt. v. 25.10.2011 – C-509/09 und C-161/10, eDate Advertising, Rn. 52.

VII. Zusammenfassung

Die Identitätsverwaltung *ex post* zur Rechtfertigung personaler Identitäten setzt chronologisch zunächst die Auskunftsmöglichkeit über die personalen Identitäten und ihren Status im Datenzyklus voraus. Dafür muss durch den Verantwortlichen der Zugang zu den personalen Identitäten gewährt werden, womit das Auskunftsrecht gemäß Art. 15 DSGVO des Betroffenen eine absolute Kontrollmöglichkeit über die personalen Identitäten nach der Rechtfertigung einräumt. Mit dem Auskunftsrecht wird die Transparenz *ex post* zur Rechtfertigung geschaffen und lässt sich als vertrauensbildende Maßnahme des Betroffenen einordnen.

Dem folgend, sind das Recht auf Vergessenwerden und das Recht auf Datenübertragung als Kernrechte eines Identitätsverwaltungsmodells anzusehen. Mit dem Recht auf Vergessenwerden wird eine Löschpflicht über die verarbeiteten personenbezogenen Daten ausgelöst, wobei die Annahme eines tatsächlichen Vergessens der personenbezogenen Daten ausgeschlossen werden muss, da die Erinnerungen und die aus der Datenverarbeitung generierten Erkenntnisse nicht zwingend umfasst sind. Somit wirkt das Recht auf Vergessen nur relativ, weshalb von einer „Chance des Vergessens" auszugehen ist. Auch beim Recht auf Vergessenwerden wirken verhaltensökonomische Verzerrungen, so dass es der Einbeziehung weiterer Schutzmechanismen über die Löschung der Daten hinaus bedarf. Das Konzept einer „*Symphonie der Intransparenz*" fungiert als ein solcher Schutzmechanismus, da mit der Löschung und Verzerrung von bestimmten Datensätzen der Erkenntnisgehalt über eine personale Identität verfälscht werden kann. Demnach dient die Intransparenz als Gestaltungs- und Steuerungsinstrument in einem Identitätsverwaltungsmodell, zumal für den Schutz des allgemeinen Persönlichkeitsrechts auf diesem Weg die „Evolution der Identität" und das *Recht auf Neubeginn* gewährleistet werden. Daneben lässt sich mit dem Recht auf Datenübertragbarkeit als Minus über das Löschungsrecht die personale Identität direkt verwalten, indem der Kontext einer personalen Identität geändert wird. Die Effektivität des Rechts könnte jedoch zweifelhaft werden, da die Gewährleistung technischer Schnittstellen durch den Verantwortlichen einer Soll-Vorschrift und dem technischen Machbarkeitsvorbehalt unterliegen, so dass *de lege ferenda* eine Muss-Vorschrift möglicherweise sogar mit Sanktionsvorbehalt wünschenswert ist und sich auf den Wettbewerb der Dienstanbieter positiv auswirken könnte. Damit würde sich die Funktion des Rechts auf Datenübertragbarkeit als Nutzerschutzrecht tatsächlich realisieren lassen.

Weiter ist bei Datenschutzverstößen gemäß Art. 33, 34 DSGVO die Transparenz dieser vorgesehen, die es dem Betroffenen ermöglicht, die geeigneten Maßnahmen zum Schutz seiner Rechte und Freiheiten zu treffen. Darin liegt eine Kontrollmöglichkeit des Betroffenen, die sich als ein Verfahren infolge der Informationen über den Datenschutzverstoß darstellt. Sobald der Betroffene der Ansicht ist, dass ein Verstoß gegen die Verordnung vorliegt, kommt neben dem Beschwerderecht gemäß Art. 77 Abs. 1 DSGVO die gerichtliche Geltendmachung gemäß Art. 79 Abs. 2 DSGVO in Frage, bei der der Betroffene ein Wahlrecht hat und die Identitätsverwaltung sich sogar auf die Entscheidung über den Ort des anzurufenden Gerichts erstreckt.

Insgesamt lassen sich die rechtlichen Anforderungen in ein *Dashboard-System* übertragen, mit dem eine iterative Zugangs- und Kontrollmöglichkeit *ex post* zur Rechtfertigung eingeräumt wird. Dabei könnten die personalen Identitäten zum Gegenstand von Löschoptionen, der kontrollierten Intransparenz und der Kontrolle über die kontextübergreifende Datenübertragung werden. Ebenso wären im gesamten Datenzyklus die Transparenz über den Status einer personalen Identität und ein mögliches Verletzungsrisiko in einem *Dashboard-System* zu gewährleisten. Damit könnte der Schutz von personalen Identitäten in ihrem *Ipse-* und *Idem*-Anteil erfolgen, welches mit einem iterativen Begründungskonzept aus dem Recht gegen die automatisierte Entscheidung gemäß EWG 71 S. 4 ermöglicht wird. Folglich würden die personalen Identitäten iterativ in einem *Dashboard-System* aktualisiert werden können.

E. Identitätsverwaltung im Telemedien- und Telekommunikationsgesetz

I. Identitätsverwaltung im Telemediengesetz

Die Identitätsverwaltung im Telemedienrecht erfolgt im Kontext der Telemediendienste. Davon erfasst sind Dienste, die über die bloße Signalübertragung hinaus einen Kommunikationsprozess zur Informationsübertragung begründen und darin der Schwerpunkt der Leistungserbringung liegt, § 3 Nr. 24 TKG.[672] Mit der Geltung der Datenschutzgrundverordnung ist von dieser ebenfalls der Schutz von personenbezogenen Informationsübertragungen erfasst, so dass der Anwendungsbereich des Telemedi-

672 *Kremer*, CR 2012, 438 (440 f.).

engesetzes hinter dem der Datenschutzgrundverordnung zurücktreten könnte. Hinzu kommt, dass an sich die künftige EPrivacy-VO den Schutz der Nutzung von Telemediendiensten umfassen sollte und wiederum die Regelungen der DSGVO verdrängen würde. Solange eine EPrivacy-VO jedoch noch nicht gilt, ist auf die DSGVO und die Fortgeltungsmaßgabe gemäß Art. 95 DSGVO abzustellen, wonach die Richtlinie für elektronische Kommunikation 2002/58/EG weiterhin neben der Datenschutzgrundverordnung Anwendung findet.[673] Folglich soll das Telemediengesetz weiterhin als anwendbar eingestuft werden und die Identitätsverwaltung aus diesem Blickwinkel der TMG-Regelungen einbezogen werden. Für die Identitätsverwaltung sind demnach die Datensätze über die personalen Teilidentitäten im Telemedienrecht relevant (1.), die Kontrollmöglichkeiten durch den Betroffenen (2.), die Identitätsverwaltung durch den Dienstanbieter (3.) und weiter soll ein abschließender Ausblick erfolgen (4.).

1. Personale Teilidentitäten im Telemedienrecht

Die personalen Teilidentitäten im Telemedienrecht lassen sich einem Nutzer zurechnen, wenn über einen Nutzungsvertrag die Datensätze freigeschaltet werden und sich damit die Nutzung auf den Nutzer zurückführen lässt. Dazu gehört die Verarbeitung von Datensätzen beim Einsatz des Telemediendienstes, die einen eigenständigen Erkenntnisgehalt mit sich bringen können. Dieser leitet sich aus den Bestandsdaten (a), den Nutzungsdaten (b) und Profildaten (c) ab.

a) Personale Teilidentität durch Bestandsdaten, § 14 Abs. 1 TMG

Die personale Teilidentität aus den Bestandsdaten bildet sich in ihren statischen und dynamischen Ausprägungen ab und führt zu einem eigenständigen Erkenntniswert. Von den Bestandsdaten sind diejenigen Daten erfasst, die für die Begründung, die inhaltliche Ausgestaltung oder die Änderung eines Vertragsverhältnisses zwischen dem Dienstanbieter und Nutzer erforderlich sind, § 14 Abs. 1 TMG. Demnach ist der Gegenstand der Bestandsdaten über die Vertragsauslegung zu ermitteln und ist begrenzt

673 *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, Vor §§ 11 ff. TMG Rn. 23.

durch die Erforderlichkeit für die Vertragsgestaltung.[674] Zu den Bestandsdaten können die Identifizierungsdaten, Anschrift, E-Email-Adresse, Rufnummer und der Zweck des Vertrages, die Kenn- und Passwörter, der Vertragszeitraum, der Ort der Nutzung des Telemediendienstes, die Leistungsmerkmale und die Zahlungsart gehören.[675] Demnach generiert sich die personale Teilidentität aus den Bestandsdaten mit dem Vertragsschluss und wird mit der „strikten Erforderlichkeit" gerechtfertigt, so dass die Entstehung der personalen Teilidentität ohne eine aktive Handlung über den Vertragsschluss hinaus erfolgt und keine eigenständige Einwilligung[676] verlangt. Der damit verbundene Datenzyklus der personalen Teilidentität in ihrem überwiegenden *Idem*-Anteil ist auf den vertraglich bestimmten Zeitraum begrenzt und erfährt mit der Lösch- und Sperrpflicht am Vertragsende gemäß § 13 Abs. 4 S. 2 TMG eine zeitliche Begrenzung. Aus dieser temporären Ausgestaltung der personalen Teilidentität im Telemedienrecht und dem damit verbundenen Erkenntnisgehalt hat der Nutzer allein im Rahmen des Vertragsschlusses eine Kontrollmöglichkeit. Gleichwohl lässt sich die Kontrollmöglichkeit über die Transparenz des bestehenden Vertragsverhältnisses in einem *Dashboard-System* abbilden, womit für den Nutzer der statische *Idem*-Anteil der personalen Teilidentität sichtbar wird.

b) Personale Teilidentität durch Nutzungsdaten, § 15 Abs. 1 TMG

Im Telemedienrecht wird infolge der Nutzung des Dienstes durch die Datenverarbeitung eine personale Teilidentität über die Nutzungsdaten begründet. Die Nutzungsdaten umfassen solche Daten, mit denen die Inanspruchnahme der Telemediendienste ermöglicht wird und die Abrechnung erfolgt, § 15 Abs. 1 S. 2 TMG. Danach sind Identifikationsdaten, Angaben über den Zeitraum der Nutzung und der in Anspruch genommene Telemediendienst von den Nutzungsdaten erfasst[677] und gehören zur personalen Teilidentität in ihrem überwiegenden dynamischen *Ipse*-Anteil, § 15 Abs. 1 S. 2 Nr. 1–3 TMG. Weiter gehören die Log-in Daten, die statischen oder dynamischen IP-Adressen, die Kommunikationspartner, die abgerufenen Informationen und Downloads zu der personalen Teilidentität in ihrem *Ipse*-Anteil dazu. Die Verarbeitung dieser Daten ist gerechtfertigt,

674 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 14 TMG Rn. 15.
675 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 14 TMG Rn. 73.
676 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 14 TMG Rn. 9.
677 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 42.

wenn sie nach der Datenschutzrichtlinie „erforderlich" war, was nach dem *Breyer*-Urteil[678] des EuGHs nunmehr bei Maßnahmen zur Gewährleistung der Datensicherheit auch gilt.[679]

Folglich stellen die Nutzungsdaten die Grundlage für die Begründung einer personalen Teilidentität über das Nutzungsverhalten in dem Kontext des Telemediendienstes dar. Es handelt sich um eine dynamische zeitlich beschränkte personale Teilidentität, die so lange gilt bis der Zweck erreicht wurde und die Lösch- und Sperrpflichten wirken. Mit diesen Nutzungsdaten ist ein kontextabhängiger Erkenntnisgewinn aus dem Nutzungsverhalten möglich, über den der Nutzer durch die Rechtfertigung mit der Erforderlichkeit und damit ohne aktive Handlung keine Kontrolle ausüben kann. Im Gleichlauf zu den Bestandsdaten wäre für die Transparenz an den Nutzer daher die Einbeziehung der Nutzungsdaten in dem *Dashboard-System* wünschenswert.

c) Personale Teilidentität durch Nutzungsprofil, § 15 Abs. 3 TMG

Die personale Teilidentität kann aus einem pseudonymisierten Nutzungsprofil bestehen und zum Zweck der Werbung und der Marktforschung eingesetzt werden, § 15 Abs. 3 TMG. Dieses Nutzungsprofil lässt sich in ein kurzzeitiges Momentprofil, Kurzzeitprofil und Langzeitprofil unterscheiden, wobei die umfassende und langfristige Speicherung und Auswertung von Daten zu einem Langzeitprofil führt.[680] Mit jedem dieser Profiltypen wird ein kontextspezifisches Bild über die personale Teilidentität in ihrem *Ipse*-Anteil erstellt. Aus diesen Bildern lassen sich Erkenntnisse etwa über das Konsumverhalten, die Interessen und Aktivitäten der Nutzer ziehen, die auf algorithmischen Vermutungen und Korrelationen beruhen, so dass es sich um konstruierte Bilder einer personalen Teilidentität handelt. Zwar basiert diese personale Teilidentität auf einem Pseudonym, welches gemäß § 15 Abs. 3 S. 3 TMG mit dem Nutzer nicht zusammengeführt werden darf, jedoch den Schutz für die personale Identität gewährleistet. Denn in der Profilerstellung liegt ein Eingriff in die informationelle Selbstbestimmung. Dieser Eingriff ist einerseits von der Erforderlichkeit aus der Ver-

678 EuGH, Urt. v. 19.10.2016 – C-582/14, Breyer ./. BRD, Rn. 55, 60.

679 *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 58 f.

680 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 92–94.

tragsbeziehung heraus gerechtfertigt und andererseits unterliegt er einer teleologisch erweiternden Auslegung in Gestalt des Erfordernisses eines aktiven *opt-ins*. Damit genügt die konkludente Einwilligung nach den Vorgaben aus Art. 6 Abs. 1 a) DSGVO für ein rechtfertigendes *opt-in* zur Profilerstellung.[681]

Die personale Teilidentiät aus dem pseudonymisierten Nutzungsprofil unterliegt durch die Annahme des Erfordernisses eines aktiven *opt-ins* der relativen Kontrollmöglichkeit. Denn der Dienstanbieter setzt den Algorithmus für den Erkenntnisgewinn aus den Nutzungsdaten ein, womit die personale Teilidentität von dem Dienstanbieter begründet wird. Demnach besteht die Kontrolle nicht mehr über das erstellte Profil des Dienstanbieters und das damit verbundene Bild der personalen Teilidentität. Die Transparenz über die Logik für die Profilerstellung und die Risiken für die informationelle Selbstbestimmung könnten durch die pseudonymisierten Nutzungsprofile wiederum in dem *Dashboard-System* transparent gemacht werden, und damit der Kontrollmöglichkeit unterliegen.

d) Personale Teilidentität durch *Cookies*

Die personale Teilidentität wird auch durch den von Cookies generierten Datensatz[682] begründet. Die Cookies unterscheiden sich in Verfolgungs-Cookies zur Informationserlangung über das Nutzungsverhalten und in Dienste-Cookies zur Erbringung der Dienste. In beiden Varianten wird durch das Setzen von Cookies der Nutzer wiedererkannt. Sein vorheriges Nutzungsverhalten wird abrufbar und erlaubt über die statische oder dynamische IP-Adresse die Identifizierung des Nutzers.[683] Folglich ist mit Cookies die Erstellung einer personalen Teilidentität in ihrem *Ipse*-Anteil verbunden, die Erkenntnisse über das Nutzungsverhalten hinsichtlich der je-

681 *Ders.*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 15 TMG Rn. 25, 36, 98.

682 Ebenso als digitale Identität einordnend, *Windley*, Digital Identity, 2005, S. 51 f. Zur Funtionsweise: Mit dem ersten Aufrufen einer Webseite, die Cookies verwendet, werden diese Informationen bei dem verwendeten Browser des Nutzers hinterlegt und beim nächsten Aufrufen der gleichen Webseite an den Server zurückgeschickt. Dieser erhält damit die Informationen über das Nutzungsverhalten auf dieser Webseite, welches die Verknüpfung von bereits beim ersten Aufrufen eingegebenen Informationen ermöglicht.

683 *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 13 TMG Rn. 12 f.

weiligen Webseiten ermöglicht. Dies setzt voraus, dass der Nutzer nicht nur gemäß Art. 5 Abs. 3 S. 1 der RL 2002/58[684] vor Beginn des automatisierten Verfahrens der Cookie-Setzung unterrichtet wird, sondern nach dem Urteil des EuGHs eine wirksame Einwilligung durch aktives Verhalten vorliegen muss und ein vorangekreuztes Kästchen demnach für die Annahme einer Einwilligung unzureichend ist.[685] Dabei stützt sich der EuGH auf Art. 4 Nr. 11 und Art. 6 Abs. 1 a) DSGVO, die eine freiwillige und unmissverständliche Einwilligung voraussetzen.[686]

Insgesamt erfolgt die Wirkung der Cookies im Verborgenen („*Hidden Identifiers*")[687] und der Nutzer hat über die Inhalte der Cookies mit Ausnahme der Browser-Einstellung keine absolute oder relative Kontrollmöglichkeit. Die mit Cookies generierten personalen Teilidentitäten über den *Ipse*-Anteil befinden sich damit in der Sphäre des Dienstanbieters und entfalten dort ihre Wirkung hinsichtlich der Erkenntnis- und Werbemöglichkeiten. Eine Kompensation des Kontrolldefizits könnte durch Erweiterung des Unterrichtungserfordernisses zu einem späteren Zeitpunkt im Datenzyklus erfolgen. Hierbei könnte mit einem *Dashboard-System* ein erleichterter Zugang zu der personalen Teilidentität und der Kontrolle dieser ermöglicht werden. Damit lässt sich die Transparenz über die logische Struktur und das Bild der personalen Teilidentität aus den Cookies erstellen.

2. Kontrolle durch den Nutzer im Datenzyklus

Die personalen Teilidentitäten unterliegen der Kontrolle durch den Nutzer, wenn dieser eine Kontrollmöglichkeit im Datenzyklus erlangt. Das TMG als einfachrechtliche Konkretisierung der Datenschutzrichtlinie und der „Cookie"-Richtlinie[688] würde durch die *EPrivacy*-VO eine Konkretisie-

684 Europäische Richtlinie vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

685 EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 54.

686 EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 61–63; nach deutscher Rechtslage wurde bislang für Verfolgungs-Cookies die Einwilligung gemäß § 13 Abs. 2 Nr. 2 TMG vorausgesetzt, *Schmitz*, in: Spindler/Schmitz (Hrsg.), Kommentar, TMG, 2018, § 13 TMG Rn. 19.

687 EWG 24 Datenschutzrichtlinie für elektronische Kommunikation.

688 Richtlinie (EU) vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der

rung erfahren. Solange diese noch nicht gilt, finden die Vorschriften der DSGVO Anwendung, so dass für die Unterrichtungspflichten wiederum Art. 12, 13 Abs. 2 f) DSGVO gerade im Hinblick auf die Profilerstellung klarstellend wirken und eine Kontrollmöglichkeit einräumen. Daneben kommt die Kontrollmöglichkeit durch die elektronische Einwilligung gemäß den Anforderungen § 13 Abs. 2 Nr. 1–3 TMG in Betracht. Demgegenüber unterliegen die personalen Teilidentitäten in ihren *Idem*- und *Ipse*-Anteilen, die auf den Bestandsdaten, Nutzungsdaten und den Dienste-Cookies basieren, der Rechtfertigung im Rahmen der Erforderlichkeit. Folglich kann der Nutzer seine Kontrollmöglichkeit erst zu einem späteren Zeitpunkt des Datenzyklus ausüben. Diese Kontrolle könnte etwa über das Widerrufsrecht gemäß § 13 Abs. 2 Nr. 4 TMG, die Beendigung der Nutzung gemäß § 13 Abs. 4 Nr. 1 TMG und das Recht auf Vergessenwerden gemäß Art. 17 DSGVO im Wege der europarechtskonformen Auslegung gegenüber den Nutzungsdaten und dem Nutzungsprofil ausgeübt werden. Neben dem Kontrollrecht über die Löschung kann die Sperrung der personalen Teilidentitäten gemäß §§ 13 Abs. 4 Nr. 2, 15 Abs. 4 TMG verfolgt werden.

Folglich ergeben sich aus dem TMG im Gleichlauf zur DSGVO durch die Informationspflichten, die Einwilligung und die Löschungsrechte für den Nutzer relative Kontrollmöglichkeiten über die personalen Teilidentitäten. Gleichwohl sind die personalen Teilidentitäten, die auf der Erforderlichkeit gemäß §§ 14, 15 Abs. 1, 3 TMG basieren, in einem Kontrollsystem bislang nicht integriert, so dass der Bedarf an der Einrichtung einer Kontrollmöglichkeit zu einem späteren Zeitpunkt der personalen Teilidentität in einem *Dashboard-System* besteht, indem die Transparenz über die entstandenen personalen Teilidentitäten hergestellt wird.

3. Identitätsverwaltung durch den Dienstanbieter

Die Identitätsverwaltung durch den Dienstanbieter erfolgt im Gleichlauf zu den Maßgaben nach der DSGVO *ex ante* zur Rechtfertigung der personalen Teilidentitäten. Danach hat der Dienstanbieter bei der Begründung des Dienstangebotes die technischen und organisatorischen Maßnahmen im Rahmen des wirtschaftlich Zumutbaren zum Schutz für die personenbezogenen Daten sicherzustellen und den Stand der Technik zu berück-

elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

sichtigen, § 13 Abs. 4, 7 S. 2 TMG.[689] Dabei bestehen in § 13 Abs. 6 TMG Vorgaben, mit denen der Dienstanbieter die Nutzung und Bezahlung anonym oder durch ein Pseudonym im Rahmen des technisch Zumutbaren zu ermöglichen hat, worin implizite Vorgaben für ein Identitätsverwaltungsmodell enthalten sind. Denn mit dem Pseudonym wird eine personale Teilidentität in ihrem *Idem*-Anteil geschaffen, die einen geringen Erkenntniswert mit sich bringt und durch den Nutzer kontrolliert werden kann. Zu diesem Schutzkonzept der personalen Teilidentitäten gehört, dass die Nicht-Verkettbarkeit der generierten personalen Teilidentitäten gewährleistet werden muss, wie es aus §§ 13 Abs. 4 Nr. 4, 15 Abs. 3 S. 3 TMG hervorgeht. Diese technischen und organisatorischen Maßnahmen durch den Dienstanbieter gehen als Ergebnis aus einer vorangegangen Risikobewertung hervor, bei der die Popularität eines Dienstes zu einer Steigerung der wirtschaftlichen Zumutbarkeitsgrenze führen und weitere Schutzpflichten für die personalen Teilidentitäten voraussetzen kann.

Insgesamt hätte der Dienstanbieter den Einschätzungsspielraum über die Gestaltung des Identitätsverwaltungsmodells unter Wahrung der Datenschutzprinzipien innerhalb des Dienstes, wozu der differenzierte Einsatz von Anonymisierungs- und Pseudonymisierungsmethoden, die Transparenz über den Dienst und die generierten personalen Teilidentitäten gehören. Schließlich ist dieses Transparenzkonzept zu einem späteren Zeitpunkt des Datenzyklus auf die Betroffenenrechte zu erweitern, was mit einem *Dashboard-System* umgesetzt werden kann.

4. Ausblick

Die Grundlagen für die Identitätsverwaltung aus dem Telemedienrecht sind vorübergehender Natur und würden von einer künftigen EPrivacy-VO verdrängt werden. Mit dieser Verordnung würde etwa die Einwilligung für die Rechtmäßigkeit der Kommunikation beim Einsatz elektronischer Dienste gemäß Art. 9 EPrivacy-VO-E geregelt werden, worin ein Gleichlauf zur DSGVO liegen würde. Ebenso sind Löschpflichten gemäß Art. 7 EPrivacy-VO-E vorgesehen, mit denen die Anonymisierung oder Löschung der Daten durch den Betreiber vorgesehen wäre.[690] Diesen Vorgaben übergeordnet können die Rechtsanforderungen und Technikanforde-

689 3. Teil, A., I., 5.–6.

690 Zu dem Entwurf im Einzelnen kritisch *Härting/Gössling*, CRi 2018, 6 (8).

rungen der NIS-Richtlinie[691] und des BSIG wirken, wenn es um den Schutz und die Realisierung von personalen Teilidentitäten und der Identitätsverwaltung im Kontext kritischer Infrastrukturen geht. Dabei wirkt sich neben den rechtlichen Anforderungen die technische Gestaltung deutlich auf das mögliche Nutzungsverhalten aus, indem das Schutzniveau über den Einsatz von Anonymisierungs- und Pseudonymisierungsmethoden die Entscheidung des Betroffenen für einen bestimmten Dienst beeinflussen kann. Ebenso könnte für die Stärkung des Nutzers eine Struktur des „*Nudgings*" eingesetzt werden, mit dem die Aufmerksamkeit auf die Schutzmöglichkeiten gelenkt wird. Dennoch beschränkt sich eine derartige Identitätsverwaltung auf den Zugang zu bestimmten personalen Teilidentitäten nach dem TMG, ohne die Erkenntnisdimension aus den Bestands- und Nutzungsdaten einzubeziehen. Diese Ebene ist der Identitätsverwaltung *de lege ferenda* vorbehalten, könnte jedoch in der technischen Gestaltung durch eine Transparenzsteigerung über ein *Dashboard-System* als ein Konzept des „*identity management by design*" erfolgen. Dieses könnte durch eine eigenständige Hardware- und Softwaregestaltung für die Identitätsverwaltung umgesetzt werden, so dass ein dem TMG und zukünftig der EPrivacy-VO unterliegender Kommunikationsdienst die Grundlage für die Identitätsverwaltung darstellen könnte. Dem stünde jedoch entgegen, dass der Anbieter eines solchen Dienstes als *Trusted Third Party* fungieren würde und bei einem Angriff die informationelle Selbstbestimmung von vielen Nutzern verletzt werden könnte. Folglich wäre ein *Dashboard-System* als Kommunikationsdienst derart auszugestalten, dass die Datensätze selbst bei dem ursprünglichen Dienstanbieter verbleiben würden, und auf Anfrage des Nutzers die aktuelle personale Teilidentität über eine Schnittstelle in einem *Dashboard-System* sichtbar wird. Diese personalen Teilidentitäten könnten im Sinne der dargestellten rechtlichen Kontrollmöglichkeiten beibehalten, modifiziert oder gelöscht werden. Im Ergebnis erscheint dabei ein *Dashboard-System* als Kommunikationsdienst für die Identitätsverwaltung naheliegend, jedoch müsste dieses nur zur Transparenz der personalen Identitäten über Schnittstellen beitragen, ohne dabei die personalen Identitäten zu speichern.

691 Richtlinie (EU) 2016/1148 des europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

II. Identitätsverwaltung im Telekommunikationsgesetz

Die Identitätsverwaltung im Telekommunikationsrecht richtet sich nach den Datensätzen aus der Telekommunikation, mit denen Informationen über die personalen Teilidentitäten erlangt werden können. Gemäß dem *ISO-OSI-Schichtenmodell* betrifft dies im Telekommunikationsrecht die Signalübertragung und die mit dem Telekommunikationsdienst verbundenen Vertragsbeziehungen zum Teilnehmer. Demnach richtet sich die Identitätsverwaltung im Telekommunikationsrecht danach, ob der Anwendungsbereich des bereichsspezifischen Datenschutzrechts bei dem Vorliegen von elektronischen Informations- und Kommunikationsdiensten eröffnet ist. Dafür muss der Schwerpunkt des Dienstes in der Signalübertragung liegen und diese muss gegenüber der Inhaltsübermittlung im Vordergrund stehen, § 3 Nr. 24 TKG. Folglich sind die Signalübertragung und der vertragliche Rahmen für die Bestimmung der personalen Identität im Telekommunikationsrecht grundlegend. Gleichzeitig bedarf es der Einordnung von personalen Identitäten, die auf den Kommunikationsmöglichkeiten über das Internet, sog. *over the top*-Dienste (OTT-Dienste), beruhen. Als OTT-Dienste gelten solche Dienste, deren Inhalte und Anwendungsmöglichkeiten über das offene Internet erbracht werden. Diese OTT-Dienste sind aufgrund ihrer Funktionalität ohne die elektronische Signalübertragung ausgestattet und dienen der Inhaltsübertragung mittels einer Verbindungsstelle zwischen den Teilnehmern in einer „*Client-Server*"-Architektur.[692] Gleichwohl besteht eine Parallelität zwischen dem vom TKG geregelten Verhalten der Nutzung von Telekommunikationsdiensten und dem Nutzungsverhalten von OTT-Diensten, so dass die Kontrolle personaler Identitäten in OTT-Diensten ebenfalls nachvollzogen werden soll.

Insgesamt wird die personale Identität im Telekommunikationsrecht auf der unteren Schicht des *ISO-OSI-Modells* neben den Vertragsdaten eingeordnet und in den Ausprägungen der jeweiligen personalen Teilidentitäten herausgearbeitet (1.). Damit sollen die Kontrolle des Teilnehmers innerhalb des Datenzyklus (2.) und die Identitätsverwaltung durch den Anbieter (3.) verdeutlicht werden.

692 *Maier/Schaller*, ZD 2017, 373 (374).

1. Personale Teilidentitäten im Telekommunikationsrecht

Die personalen Teilidentitäten im Telekommunikationsrecht können mit den Bestandsdaten (a), den Verkehrsdaten (b) und den Standortdaten (c) begründet werden.

a) Personale Teilidentität durch Bestandsdaten, §§ 95, 3 Nr. 3 TKG

Die personale Teilidentität, die auf den Bestandsdaten basiert, setzt sich aus solchen Daten zusammen, die für die Begründung, die inhaltliche Ausgestaltung, Änderung oder Beendigung des Vertragsverhältnisses über einen Telekommunikationsdienst erforderlich sind, §§ 3 Nr. 3, 95 Abs. 1 S. 2 TKG. Dazu gehören im Gleichlauf zu den Bestandsdaten im TMG etwa der Name, Adresse und die Abrechnungsdaten, aus denen die personale Teilidentität mit ihrem *Idem*-Anteil im TKG-Kontext begründet wird und die von der entsprechenden personalen Teilidentität im TMG abweichen kann. Die Begründung dieser Teilidentität wird mit der Erforderlichkeit für die Vertragserfüllung gerechtfertigt und bedarf für die Weitergabe der Bestandsdaten an Dritte der Einwilligung des Teilnehmers. Für die Identifizierung bei der Nutzung eines im Voraus bezahlten Mobilfunkdienstes kann die Richtigkeit der Angaben durch die Überprüfung etwa des Personalausweises erfolgen, § 111 Abs. 1 S. 2 TKG. Damit wird das Vertrauen über die Richtigkeit der Angaben im Personalausweis auf den Telekommunikationsdienst erweitert, so dass die personale Teilidentität in ihrem *Idem*-Anteil über die Bestandsdaten ein hohes Vertrauensniveau auslösen und zugleich Anknüpfungspunkt für strafrechtliche Ermittlungen gegen den Anschlussinhaber sein kann.

Wegen des hohen Vertrauensniveaus über die Richtigkeit der Identitätsinformationen in den Bestandsdaten könnte diese personale Teilidentität in einem Identitätsverwaltungsmodell in Gestalt eines interoperablen „*Identity Ecosystem*“ eingesetzt werden. Demnach würde die personale Teilidentität über die Bestandsdaten in Kontexten mit dem gleichen Vertrauensniveau übertragbar sein und eine kontextübergreifende Identitätsverwaltung ermöglichen. Denn sobald einmal die Identifizierung eines Teilnehmers erfolgt, könnte es dem Grundsatz der Datenminimierung entsprechen, diese einmal generierte personale Teilidentität wiederzuverwerten.

b) Personale Teilidentität durch Verkehrsdaten, §§ 96, 3 Nr. 30 TKG

Die personale Identität, die auf den Verkehrsdaten basiert, umfasst die mit der Erbringung des Telekommunikationsdienstes verbundenen Datenverarbeitungen, § 3 Nr. 30 TKG. Dazu gehören die Verbindungsdaten, die IP-Adresse, die MAC-Adresse und die Kennung über die Berechtigung mit den Log-in-Daten, so dass der *Idem*-Anteil personaler Teilidentitäten von den Verkehrsdaten erfasst ist. Die Erhebung der Verkehrsdaten ist für den Zweck gemäß § 96 Abs. 1 TKG zum Aufbau und der Nutzung der Verbindung gerechtfertigt und zum Zwecke der Vermarktung durch die Einwilligung erforderlich, § 96 Abs. 3 S. 1 TKG. Die Verkehrsdaten sind in ihrem Erkenntnisgehalt dadurch gekennzeichnet, dass sie als eine zeitlich gebundene Momentaufnahme erscheinen und dynamisch sind. Sie sind damit abhängig von dem Nutzungsverhalten und können als verhaltensgeprägte personale Teilidentität in ihrem überwiegenden *Ipse*-Anteil eingestuft werden.

Gleichwohl kann die Speicherung der Verbindungsdaten für das sog. „*Abuse-Handling(s)*“[693] und der Strafverfolgung dienen. Damit können die personalen Teilidentitäten, basierend auf den Verkehrsdaten, einem Vergangenheitsbezug unterliegen und gleichzeitig in die Zukunft wirken. Darin liegt eine Parallele zu dem festgestellten Phänomen von Profilen als Ergebnis von dem in der Vergangenheit liegenden Verhalten, die ebenfalls eine personale Teilidentität begründen können. Dennoch muss zwischen solchen Profilen als *Ipse*-Anteile personaler Teilidentitäten differenziert werden, die zum Schutz des Teilnehmers aus Gründen der IT-Sicherheit eingesetzt werden und solchen Profilen, die aus ökonomischen Motiven für gezielte Werbemaßnahmen begründet werden. Erstere personale Teilidentität mit Vergangenheitsbezug wird bei der Grundrechtsabwägung gegenüber der informationellen Selbstbestimmung aufgrund eines übergeordneten Sicherheitsinteresses gerechtfertigt sein. Dagegen unterliegt die ökonomisch motivierte Profilbildung den Rechtfertigungsgründen aus Art. 6 Abs. 1 DSGVO.

c) Personale Teilidentität durch Standortdaten, §§ 98, 3 Nr. 19 TKG

Die personale Teilidentität aus Standortdaten ist ebenfalls mit dem Verhalten des Teilnehmers verbunden und besteht aus solchen Daten, die in

693 *Kühling/Schall/Biendl*, Telekommunikationsrecht, 2014, Rn. 639.

einem Telekommunikationsnetz erhoben und verwendet werden und den Standort des Endgeräts eines öffentlich zugänglichen Telekommunikationsdienstes angeben, §§ 98, 3 Nr. 19 TKG. Gleichwohl sind die Standortdaten ebenfalls gemäß Art. 4 Nr. 1 DSGVO als personenbezogene Daten und damit als Inhaltsdaten geschützt, so dass sie innerhalb des *ISO-OSI-Schichtenmodells* nicht auf der unteren Ebene der Signale einzuordnen sind. Dies stellt eine Anomalie im Telekommunikationsrecht dar. Gleichwohl soll im Folgenden die Darstellung in Übereinstimmung mit den Standortdaten als personenbezogene Daten und ihrem *Ipse*-Anteil der personalen Teilidentität erfolgen.

Insgesamt lässt sich mit den Standortdaten ein genaues Profil über das Bewegungsverhalten des Teilnehmers nachbilden, so dass die personale Teilidentität in ihrem *Ipse*-Anteil, basierend auf dem Bewegungsverhalten, einen umfangreichen Erkenntniswert über den Teilnehmer hinsichtlich der Dauer, Häufigkeit und des Zeitpunktes seines Aufenthaltes ermöglicht. Darin kann ein erheblicher Eingriff in die informationelle Selbstbestimmung liegen, so dass die unverzügliche Anonymisierung dieser Daten gemäß § 98 Abs. 1 S. 2 TKG vorgesehen ist und in anderen Fällen die entsprechende Einwilligung einzuholen wäre.[694] Weiter werden nach dem EWG 2 der EPrivacy-VO-E die Standortdaten als hochsensible Informationen eingeordnet, worin eine Anerkennung der umfangreichen Erkenntnismöglichkeiten aus kontextübergreifenden Datensätzen liegt. Folglich ist die erleichterte Ortung von Mobilfunktelefonen und der Standortverlauf durch Intermediäre, die über die Privatheitseinstellung deaktiviert werden können, ein Phänomen, welches in die Identitätsverwaltung aufgenommen und in einen eigenen Schutzmechanismus zu überführen wäre. Entsprechend werden in Art. 4 Abs. 3 c) EPrivacy-VO-E die Standortdaten als elektronische Kommunikationsmetadaten eingeordnet und stellen gleichzeitig die elektronischen Kommunikationsdaten gemäß Art. 4 Abs. 3 a) EPrivacy-VO-E dar. Diese müssen gemäß Art. 7 Abs. 2 EPrivacy-VO-E anonymisiert oder gelöscht werden und dürfen nur unter den Maßgaben des Art. 6 Abs. 2 EPrivacy-VO-E gespeichert werden, wenn die gesonderten Rechtfertigungsanforderungen vorliegen.

Das Phänomen der Speicherung von Standortdaten durch Intermediäre ist für die Teilnehmer in ihrer Tragweite nicht unmittelbar transparent. Dies betrifft etwa die Speicherung des Standortverlaufes, die der Nutzer bei einer Suchmaschine erst durch vertiefte Auseinandersetzung mit den Privatheitseinstellungen transparent und damit kontrollierbar macht.

694 *Dies.*, Telekommunikationsrecht, 2014, Rn. 641.

Demgegenüber ist nach § 98 Abs. 1 S. 2 TKG und Art. 7 Abs. 2 EPrivacy-VO-E vorgesehen, dass bei einer Speicherung die Einwilligung erteilt werden muss, die wiederum eine Transparenz über die Speicherung der Standortdaten voraussetzt. Insgesamt kann die personale Teilidentität aus den Standortdaten einer hohen Sensibilität unterliegen, so dass es zunächst der Transparenz über diese Teilidentität bedarf, um entsprechende Schutzmaßnahmen vornehmen zu können. In einem *Dashboard-System* ginge es um die Transparenz und den technischen Schutz der personalen Teilidentität, die auf den Standortdaten basiert. Damit würde dem Teilnehmer eine reale Kontrollmöglichkeit eingeräumt werden.

2. Kontrolle durch den Teilnehmer im Datenzyklus

Die Kontrolle über die personalen Teilidentitäten nach dem Telekommunikationsrecht erfolgt im Gleichlauf zu den Feststellungen im Telemedienrecht. Maßgeblich ist die Kontrollmöglichkeit über die personale Teilidentität mit der Einwilligung hinsichtlich der Standortdaten und der Vermarktung der Verkehrsdaten. Im Übrigen unterliegen die personalen Teilidentitäten, die auf den Bestandsdaten, Verkehrsdaten und den erforderlichen Standortdaten basieren, der Kontrolle durch die Informationspflichten gemäß § 93 TKG über die Verwendung der personenbezogenen Daten im Einzelnen. Auf dieser Grundlage kann die Einwilligung mit einer vorformulierten Einwilligungsklausel gemäß § 94 TKG als Kontrollmittel abgefragt werden. Zu einem fortgeschrittenen Zeitpunkt bei der Verarbeitung personenbezogener Daten kommen das Auskunftsrecht gemäß § 93 Abs. 1 S. 4 TKG und die Benachrichtigungspflicht bei der Verletzung des Schutzes personenbezogener Daten gemäß § 109a Abs. 1 S. 2 i.V.m. Abs. 2 TKG in Betracht. Damit kann der Teilnehmer nach der Rechtfertigung der Speicherung die Kontrolle über die personale Teilidentität im Rahmen der Transparenz ausüben.

Dagegen ist die Einordnung der Kontrollmöglichkeit über die personalen Teilidentitäten aus OTT-Diensten differenzierter. Bislang war unklar, ob die Kommunikation über das Internet unter das Tatbestandsmerkmal der Signalübertragung im Telekommunikationsrecht subsumierbar ist.[695] Nun hat der EuGH einen technischen Ansatz gewählt[696] und differenziert zwischen zweistufigen OTT-0-Diensten und einstufigen OTT-1-Diensten.

695 *Kühling/Schall*, CR 2015, 641; *Gersdorf*, K&R 2016, 91.
696 *Wüsthof*, N&R 2019, 275 (277–279).

Bei den zweistufigen OTT-0-Diensten wird die Signalübertragung in der zweiten Stufe angenommen, da etwa *SkypeOut* in einem ersten Schritt von einem Engerät innerhalb der Internetverbindung bis zum Gateway die Informationen überträgt und in einem zweiten Schritt aufgrund einer Zusammenschaltungsvereinbarung in das öffentliche Telefonnetz eine Signalübertragung erfolgt.[697] Demgegenüber wurde *Gmail* nicht als elektronischer Kommunikationsdienst mit Signalübertragung eingeordnet, da die Übertragung der Datenpakete über einen Dritten, nämlich den Internetbetreiber erfolgt, sog. OTT-1-Dienst.[698] Aus diesen technikbezogenen Differenzierungen ergibt sich für den Schutz personaler Identitäten, dass das rechtliche Schutzniveau von dem verwendeten Dienst abhängt. Gleichwohl wird der Schutz mit den zukünftigen Regelungen der Richtlinie zum Kodex für elektronische Kommunikation[699] und der EPrivacy-VO umfasst, so dass spezifische Regelungen zur Kontrollierbarkeit der personalen Teilidentitäten aus OTT-Diensten bevorstehen.

3. Identitätsverwaltung durch den Anbieter

Die Identitätsverwaltung könnte durch den Dienstanbieter im Gleichlauf zu den Anforderungen nach der DSGVO und dem TMG mit der Gewährleistung entsprechender technischer Schutzvorkehrungen erfolgen, die ebenfalls unter dem Wirtschaftlichkeitsvorbehalt gemäß § 107 Abs. 2 S. 4 TKG stehen. Im Hinblick auf die Verwaltung der personalen Teilidentitäten würde diese eine Separierung der Datensätze zu den Bestandsdaten, Verkehrsdaten und Standortdaten verlangen, damit diese in die Transparenz überführt werden können. Damit erlangt der Teilnehmer über die Kenntnis der generierbaren und generierten personalen Teilidentitäten eine Kontrollmöglichkeit, die über das *Dashboard-System* gewährleistet werden könnte. Neben der Kontrolle über die Transparenz der personalen Teilidentität und den Informationspflichten kommt die Kontrolle über die rechtfertigende Einwilligung in Betracht. Insgesamt wird die Identitätsverwaltung durch den Telekommunikationsanbieter mit der Transparenz, der Einwilligung und dem Auskunftsrecht ermöglicht, wobei die Anzahl der TKG-Kontexte für eine Einwilligung gering sein würde. Weiter unterliegt

697 EuGH, Urt. v. 05.06.2019 – C142/18, „Skype“, Rn. 34–38.
698 EuGH, Urt. v. 13.06. 2019 – C193/18, „Gmail“, Rn. 38.
699 Art. 2 Nr. 1 a. E. Richtlinie 2018/1972 über den europäischen Kodex für die elektronische Kommunikation.

etwa die personale Teilidentität über die Standortdaten dem Anonymisierungsvorbehalt, so dass der Anbieter die geeignete Anonymisierungsmethode zu bestimmen hätte und der Teilnehmer auf diesem Wege nicht über diese personale Teilidentität in Kenntnis gesetzt werden müsste.

4. Ausblick

Das Identitätsverwaltungsmodell lässt sich mit der personalen Teilidentität in ihrem *Ipse*-Anteil aus den Standortdaten nach dem Telekommunikationsgesetz erweitern. Dabei unterliegt diese verhaltensbezogene personale Teilidentität einem hohen Schutzbedarf, der im Telekommunikationsrecht für die elektronische Signalübertragung gilt, aber noch nicht die Kommunikation mit OTT-Diensten einbezieht. Der Schutz personaler Teilidentitäten aus OTT-Diensten unterliegt einer technischen Betrachtung des konkreten Dienstes und würde bei einem OTT-0-Dienst von dem Telekommunikationsrecht umfasst sein. Bei einem OTT-1-Dienst ist auf das künftige Regelungsregime aus der Richtlinie zum Kodex für elektronische Kommunikation und der EPrivacy-VO abzustellen.

Für ein Konzept der Identitätsverwaltung kann die personale Teilidentität über die Bestandsdaten, die mit einem Personalausweis abgeglichen werden, einen Anker über eine personale Teilidentität begründen, der über ein hohes Vertrauensmaß verfügt und sich möglicherweise kontextübergreifend einsetzen lässt. Demgegenüber ist aus der personalen Teilidentität aus den Verkehrsdaten und den Standortdaten ein enger Verhaltensbezug bei der Identitätsbildung festzustellen, so dass ein ausgeprägtes Transparenzbedürfnis zur Kontrolle der personalen Teilidentitäten in ihren *Ipse*-Anteilen besteht.

Insgesamt ist die Identitätsverwaltung nach dem TKG zwischen dem Telekommunikationsanbieter und Teilnehmer ausgestaltet, wohingegen die Kommunikation im Internet über den Intermediär, der eine Applikation zur Verfügung stellt, erfolgt. Für die Identitätsverwaltung kommt ebenfalls eine solche Applikation etwa in Gestalt eines *Dashboard-Systems* in Betracht, das vergleichbar wäre mit dem „*Mobile Payment*“ über einen „*NFC-Badge*“ („*Near Field Communication*“-Plakette)[700] zur Zahlung mit einer entsprechenden Applikation. Mit dieser Applikation würden die personalen Teilidentitäten in einem anderen Kontext einsetzbar werden und, ver-

700 *Steinacker/Krauß*, in: Bräutigam/Rücker, E-Commerce - Rechtshandbuch, 2016, 13. Teil, C. Rn. 2–9.

gleichbar mit der Funktionalität der Zahlung eines Geldbetrages in einem spezifischen Kontext, die wiederholte Verwendung personaler Teilidentitäten erfolgen. Dabei scheint eine hybride Schnittstellen-Struktur, mit der gleichzeitig die elektronische Kommunikation im online-Kontext kontrolliert werden könnte, ohne dass eine *Trusted Third Party* erforderlich wäre, für die informationelle Selbstbestimmung eine schonende technische Ausgestaltung zu sein.

III. Zusammenfassung

Aus dem TMG und TKG konnten die rechtlichen Grundlagen für ein Identitätsverwaltungsmodell herausgearbeitet werden. Dabei wurde die personale Identität aus der Datenschutzgrundverordnung um die personalen Teilidentitäten aus dem TMG und TKG erweitert, die aus den Bestandsdaten, Nutzungsdaten, Verkehrsdaten und Standortdaten zu einem eigenständigen Erkenntnisgehalt führen können. Die Kontrollmöglichkeit vor der Rechtfertigung beschränkt sich auf die Transparenz. Auch bei der Rechtfertigung erstreckt sich die Kontrolle über die Einwilligung auf die Verarbeitung der personenbezogenen Daten und implizit auf den mit ihnen verbundenen Erkenntnisgehalt, wobei für die Profile eine separate Einwilligung erforderlich sein sollte.

Nach der Rechtfertigung wird zu einem späteren Zeitpunkt im Datenzyklus mit den Nutzer- und Teilnehmerrechten durch das Auskunftsrecht der Zugang als absolute Kontrollmöglichkeit zur personalen Identität gewährt. Gleichzeitig handelt es sich um dienstabhängige Kontexte, ohne dass der Nutzer oder der Teilnehmer einen Gesamtüberblick über die personalen Teilidentitäten im online-Kontext hat. Dieser Gesamtüberblick kann über ein *Dashboard-System* hergestellt werden. Da auch bei diesem System die maßgebliche Kontrollmöglichkeit über die Transparenz und rechtfertigende Einwilligung erfolgt, könnte mit einem *Dashboard-System* eine Stärkung des Schutzes der informationellen Selbstbestimmung erfolgen. Dabei könnte das *Dashboard-System* als eine Applikation eingesetzt werden, die die Kontrolle der personalen Teilidentitäten und Kommunikation, vergleichbar mit dem „*Mobile Payment*“, ermöglicht, ohne dabei als *Trusted Third Party* zu fungieren.

F. Ergebnis: Identitätsverwaltung im IKT-Recht

Das Identitätsverwaltungsmodell nach der Datenschutzgrundverordnung umfasst *ex ante* zur Rechtfertigung die Kontrolle über den Datenzykyklus durch die Informationen zur Datenverarbeitung und die damit verbundenen Risiken. Dazu gehören zunächst die personenbezogenen Daten und das Identifizierungsrisiko der natürlichen Person.[701] Weiter unterliegt jede Datenverarbeitung der vorherigen Zweckfestlegung, auf der die Generierung der personalen Identität mit den personenbezogenen Daten möglich wird. Mit der Zweckfestlegung erfolgt zugleich die *Instruktion* für die Erkenntnismöglichkeiten über die personale Identität, was dem Betroffenen eine Kontrollmöglichkeit einräumt. Diese Kontrollmöglichkeit wird jedoch mit der Zweckänderung gemäß Art. 6 Abs. 4 DSGVO im Laufe des Datenzyklus eingebüßt und es wird ein neues Risiko für die Rechte und Freiheiten der natürlichen Person ausgelöst. Die Kontrollmöglichkeit beschränkt sich dabei allein auf die Informationen über die Zweckänderung. Weiter geht es *ex ante* zur Rechtfertigung um die Risikoallokation bei der Datenverarbeitung über die Informationspflichten und die Konkretisierung der Datenverarbeitungsgrundsätze. Mit diesen datenschutzrechtlichen Anforderungen vor der Datenverarbeitung besteht gerade über die Informationen eine erste Kontrollmöglichkeit für den Betroffenen. Gleichzeitig hat der Verantwortliche zur Gewährleistung der Identitätsverwaltung technische und organisatorische Maßnahmen vorzunehmen, die in einem „*identity management by design*"-Konzept münden können.[702]

Die Identitätsverwaltung erlangt bei der Rechtfertigung ihren Kerngehalt über die Kontrollmöglichkeit mit der Einwilligung. Es konnte nachgewiesen werden, dass die Einwilligung kognitiven Verzerrungsfaktoren unterliegt und die rationale Entscheidung darin besteht, dass der Betroffene in der Vorstellung einer rationalen Entscheidung handelt. Das damit verbundene Legitimationsdefizit über die rechtfertigende Einwilligung könnte mit einem „*layered approach*" über iterative Einwilligungen gelöst werden. Dies gilt in besonderem Maß, wenn die Rechtfertigung ohne eine aktive Handlung durch den Betroffenen erfolgt. Daher lässt sich in der technischen Realisierung an ein *Dashboard-System* denken, das einen Überblick über die Datenverarbeitung mit den verbundenen Betroffenenrechten schafft und die personalen Teilidentitäten zusammenführt, damit diese kontrollierbar werden. Es wäre denkbar, ein „*Nudging*"-System für den

701 4. Teil, A., I.
702 4. Teil, B.

Schutz der Rechte und Freiheiten des Betroffenen einzusetzen. Gleichwohl würde damit eine indirekte Beeinflussung der freiwilligen Entscheidungsfindung erfolgen, die zunächst intransparent wäre und keinen unmittelbaren Beitrag für einen gesteigerten Schutz der informationellen Selbstbestimmung bedeuten würde.[703]

Weiter kann die Identitätsverwaltung *ex post* zur Rechtfertigung zunächst über das Auskunftsrecht als Zugangsrecht zu den personalen Identitäten erfolgen. Auf dieser Grundlage wäre die Kontrollmöglichkeit insbesondere mit dem Recht auf Vergessenwerden und dem Recht auf Datenübertragbarkeit gegeben. Weiter kommt das Recht gegen automatisierte Entscheidungen und damit automatisiert generierte Bilder personaler Identitäten in Betracht. Dabei lässt sich aus dem EWG 71 S. 4 ein *iteratives Verhandlungssystem* zwischen Verantwortlichem und Betroffenen nachweisen, welches als Verfahren für eine dynamisch ausgestaltete Identitätsverwaltung in einem *Dashboard-System* herangezogen werden kann. Ebenso lassen sich die Risikolagen als Gegenstand der Identitätsverwaltung einbeziehen und der Verantwortliche kann mit der Einrichtung eines iterativen Verhandlungskonzeptes *ex ante* über die Datenschutzerklärung und *ex post* über die personale Identität mit ihren Attributen selbst die Risiken neu ordnen.[704]

Die Identitätsverwaltung, basierend auf dem TMG und dem TKG, unterliegt dem Vorbehalt, dass die zu der DSGVO komplemäntere EPrivacy-VO noch nicht in Kraft getreten ist und demnach die bereichsspezifischen Datenschutzregeln im TMG und TKG unter der Maßgabe der datenschutzrechtlichen Vorgaben nach der DSGVO fortgelten. Aus dem TMG geht eine personale Teilidentität aus den Bestandsdaten, den Nutzungsdaten, dem Nutzungsprofil und den „Cookies" hervor. Ebenso geht aus dem TKG jeweils eine personale Teilidentität aus Bestandsdaten, Verkehrsdaten und Standortdaten hervor, wobei letztere gemäß Art. 4 Nr. 1 DSGVO auch dem Anwendungsbereich der DSGVO unterliegen. Aus jeder dieser personalen Teilidentitäten lässt sich ein eigener Erkenntniswert ableiten, so dass die Transparenz darüber mit einem *Dashboard-System* zu einer Schutzsteigerung der informationellen Selbstbestimmung führen würde.[705] Innerhalb dieses *Dashboard-Systems* sind „*Nudges*" als Anstöße für eine risikobewusste Entscheidungsfindung des Betroffenen auf der Rechtfertigungsebene und *ex post* zur Rechtfertigung denkbar, ohne dass die „*Nudges*" die Ent-

703 4. Teil, C.
704 4. Teil, D.
705 4. Teil, E.

scheidungsfindung negativ beeinflussen oder gar eine nachteilige Wirkung auf den Betroffenen haben. Weiter sollte das *Dashboard-System* mit einem iterativen Verhandlungssystem ausgestaltet sein, welches bereits auf der Ebene der Informationspflichten in Gestalt von iterativ verhandelten Datenschutzerklärungen und auf der Ebene *ex post* zur Rechtfertigung durch das Zugangsrecht als Kontrollmöglichkeit wirken kann. Diese technische Gestaltung könnte durch eine *Trusted Third Party* erfolgen, vorzugswürdig erscheint jedoch ein mit Schnittstellen ausgestaltetes *Dashboard-System*, ohne den Datensatz der personalen Teilidentitäten zu speichern. Demnach könnte ein *Dashboard-System* derart ausgestaltet sein, dass ein Intermediär die Interoperabilität personaler Identitäten vergleichbar mit der Bezahlung im „*Mobile Payment*" über eine Schnittstelle ermöglicht. Dies würde einem „*Identity Ecosystem*" als eine Plattform für personale Identitäten mit einem gestuften Vertrauensniveau entsprechen. Damit lässt sich auch der Grundsatz der Datenminimierung wirksam realisieren, da die personalen Teilidentitäten einmalig gespeichert würden. Weiter handelt es sich jeweils bei den aus dem IKT-Recht abgeleiteten personalen Teilidentitäten um Agenten aus den Datensätzen, die der natürlichen Person zurechenbar sind. Zugleich kann diese Zurechnungsbeziehung in gradueller Intensität ausgestaltet sein und das Vertrauensniveau variieren, wenn etwa die ursprüngliche Identifizierung mit dem Personalausweis erfolgte.

Aus dem IKT-Recht konnten die einzelnen Datenverarbeitungen und personalen Teilidentitäten nachgewiesen werden, die nunmehr in eine funktionsfähige Einheit zusammengeführt und mit dem *Dashboard-System* für die Verwaltung transparent gemacht werden kann. Dahingehend fungiert die *Identitätsverwaltung als Metamethode*[706] und verlangt ein Verfahren, wie es aus den Phasen der Datenverarbeitung *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung hergeleitet wurde. Damit fungiert die Identitätsverwaltung als ein Programm und ist eine *Metamethode* über die Gesamtheit der personalen Teilidentitäten. Dieses Programm kann in Gestalt eines *Dashboard-Systems* mit einer interoperablen Struktur umgesetzt werden. Darin läge neben einem normativen und administrativen Schutz auch ein technischer, der als Erweiterung zu einem möglicherweise rechtlich ausgeschöpften Schutzmechanismus[707] dient. Damit könnte sich die Wirksamkeit des IKT-Rechts zum Schutz der informationellen Selbstbestimmung in Gestalt der Identitäten auf einer überge-

706 2. Teil, B., III; 3. Teil, B., II., 2.

707 *Roßnagel*, in: Roßnagel/Abel (Hrsg.), Handbuch Datenschutzrecht, 2003, 3.4. Rn. 42.

ordneten Gestaltungsebene mit einem Meta-Programm als effektiv und das IKT-Recht hinsichtlich der Transparenz- und Einwilligungsanforderungen als durchsetzbares Recht erweisen. Wie das *Identitätsverwaltungsmodell auf der Metaebene als Verfahren* weiter differenziert werden kann, soll im 5. Teil durch Einbeziehung der *spieltheoretischen Perspektive* herausgearbeitet werden. Damit soll die Untersuchung um eine Perspektive erweitert werden und die Annahme eines Meta-Programms der Identitätsverwaltung mit einem *Dashboard-System* eine weitere Fundierung erfahren.

5.Teil: Spieltheoretische Modellierung des IKT-Rechts

Die Identitätsverwaltung soll mit den Anforderungen an ein Verfahren auf der Metaebene konkretisiert werden. Dieses Verfahren im Rahmen der Identitätsverwaltung im online-Kontext dient dem Zweck eines umfassenden Schutzes der informationellen Selbstbestimmung und bedarf der Sicherstellung durch ein Schutzregime, das in seiner Ausgestaltung zu spezifizieren ist. Folglich sind die grundrechtlichen und IKT-rechtlichen Wertungen in dem Verfahren einzubeziehen, damit die ergebnisoffene Verhandlung der Bilder personaler Identitäten ermöglicht wird. Dafür soll als Verfahren die Mediation im Hinblick darauf analysiert werden, ob sich diese für einen umfassenden Schutz der informationellen Selbstbestimmung einsetzen lässt. Wenn spieltheoretisch nachgewiesen werden kann, dass die Mediation ein schonendes Verfahren für das Schutzgut der informationellen Selbstbestimmung darstellt, ist eine Einbeziehung in das Identitätsverwaltungsmodell naheliegend. Diese könnte darin bestehen, dass ein technischer Mediationsagent für die Verhandlung der Bilder personaler Identitäten eingesetzt wird und insgesamt eine mediative Identitätsverwaltung als förderungswürdig gilt.

Für die Konkretisierung eines Identitätsverwaltungsmodell zum Schutz der informationellen Selbstbestimmung soll die spieltheoretische Perspektive demnach einbezogen werden, da in ihr eine Querschnittsperspektive über zwischenmenschliche Kommunikation und den Informationsaustausch aus der Rechtsinformatik zum Ausdruck kommt.[708] Dabei liegt der spieltheoretischen Modellierung die Prämisse zugrunde, dass die IKT-rechtlichen Phänomene im online-Kontext nicht nur rechtlich geprägt sind, sondern auch vom Marktverhalten der Akteure beeinflusst werden. Denn die Entscheidungen der Akteure werden nicht nur durch rechtliche Vorgaben bestimmt, sondern auch durch das Interesse an Gewinnen, an der Nutzung eines Dienstes oder an den Gratifikationen. Damit bestehen

708 *Steinmüller*, Information, Modell, Informationssystem, S. 2 Fn. 6, S. 4 Fn. 32; *Watzlawick/Beavin/Jackson*, Menschliche Kommunikation, 2016, S. 249–252. In dem technischen Informationsaustausch wird die kommunikationspsychologische Dimension benannt und ebenso wird die zwischenmenschliche Kommunikation als spieltheoretisch modellierbar angesehen, was die Verbindung dieser Fachdisziplinen verdeutlicht.

auch ökonomische Wirkmechanismen. Zwar ließe sich konstatieren, dass sich eine ökonomische Betrachtung der Grundrechte und des einfachen Rechts verbiete, jedoch soll mit der spieltheoretischen Modellierung der rechtliche Wirkmechanismus zur Lösungsfindung für einen umfassenden Schutz der informationellen Selbstbestimmung einbezogen werden.

Darüber hinaus wird der Zweck verfolgt, den Lösungsmechanismus für die Identitätsverwaltung auf eine möglichst breite fachübergreifende Grundlage zu stellen. Damit sollen die IKT-rechtlich indizierten Entscheidungen, die Informationslagen und die Auszahlungen für die Akteure im Rahmen des Datenzyklus analysiert werden. Dies verlangt die Einbeziehung der chronologischen Abfolge von anzuwendenden Rechtsvorschriften *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung, um die Wirkungen für den Schutz der informationellen Selbstbestimmung zu verdeutlichen. Dafür sollen im Folgenden die Entscheidungen des Verantwortlichen und des Betroffenen näher betrachtet werden. Dabei werden der Verantwortliche und der Betroffene als Synonym für die jeweils im Telemedienrecht agierenden Dienstanbieter und Nutzer und im Telekommunikationsrecht agierenden Telekommunikationsanbieter und Teilnehmer im Folgenden verwendet.

Insgesamt sind in der spieltheoretischen Modellierung, die sich an den rechtlichen Vorgaben orientiert, die Entscheidungen und das Verhalten des Verantwortlichen und des Betroffenen zu analysieren. Dies bedarf der Bestimmung des Verhandlungsgegenstandes der persönlichen Informationen als öffentliches Gut (A.) und der Darstellung des spieltheoretischen Modells im IKT-Recht (B.). Weiter soll die Diskussion eines technischen Mediationsagenten als Lösungsmodell (C.) erfolgen und abschließend ein Mediationsagent zur Identitätsverwaltung (D.) herausgearbeitet werden.

A. Persönliche Informationen als öffentliches Gut

Die spieltheoretische Modellierung des Spielerverhaltens, basierend auf den Regeln des IKT-Rechts, setzt einen Verhandlungsgegenstand voraus, der das online-Phänomen einer hohen Offenlegungsbereitschaft persönlicher Informationen umfasst. Indem die Zugangsgewährung zu persönlichen Informationen mit der rechtfertigenden Einwilligung oder ohne aktive Handlung des Betroffenen erfolgt, geht damit die Offenlegung persönlicher Informationen einher und der Schutz des Privatlebens dieses Nutzers erfährt eine Beschränkung. Dies wird in einem sozialen Netzwerk besonders deutlich, wenn die Nutzer nach Erteilung der Einwilligung ihre priva-

ten Interessen und Erlebnisse austauschen und andere Nutzer sich dazu veranlasst sehen, ebenso Einzelheiten aus ihrem Privatleben zu offenbaren. Darin kommt eine Dynamik zum Ausdruck, die zu einem Absinken des Schutzniveaus über die informationelle Selbstbestimmung führt.

Sobald das Schutzniveau über das Privatleben insgesamt abnimmt, wirkt sich dies gleichzeitig auf den Schutz des grundrechtlich gewährleisteten öffentlichen Gutes der persönlichen Informationen aus. Bei dem Begriff des öffentlichen Gutes handelt es sich um einen ökonomischen, der für diejenigen Konstellation als anwendbar gilt, in denen die Nutzung des Gutes keiner Gegenleistung unterliegt.[709] Mit der Offenlegung persönlicher Informationen etwa in einem sozialen Netzwerk ist keine Gegenleistung verbunden, höchstens in der Gestalt der beidseitigen Offenlegung persönlicher Informationen im Rahmen der Kommunikationsbeziehung. Folglich wirkt sich etwa in einem sozialen Netzwerk die Offenlegungsbereitschaft auf den grundrechtlichen Schutz des Privatlebens gemäß Art. 7 GRC aus. Demnach gelten persönliche Informationen für den weiteren Gang der Untersuchung als öffentliches Gut,[710] welches als Verhandlungsgegenstand zwischen dem Betroffenen und Verantwortlichen fungiert. Gleichwohl handelt es sich nach *Hermstrüwer* nicht um einen Gegenstand von Allokationen und distributiven Verhandlungen über begrenzte Ressourcen, sondern die persönlichen Informationen gelten als Primärrechtsgut, was der Persönlichkeitsentfaltung und der Selbstdarstellung in der Öffentlichkeit dient und unbegrenzt zur Verfügung stehe.[711]

Auch wenn die Verbindung zwischen den grundrechtlich geschützten persönlichen Informationen und der Ökonomie nach dem dargestellten IKT-Recht zunächst fernliegend erscheint, soll in Anbetracht von Geschäftsmodellen zu persönlichen Informationen für die Begründung des Schutzkonzeptes eine ökonomische Betrachtung herangezogen werden. Denn es zeigt sich mit dem Wirken endogener und exogener Entscheidungsfaktoren beim Betroffenen, dass Gratifikationen und Netzwerkeffekte mit der Entscheidung über die persönlichen Informationen im Zusammenhang stehen.[712] Dabei können Datenverarbeitungen durch den Ver-

709 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 134.

710 Von *Hermstrüwer* werden „persönliche Informationen" als öffentliche Güter eingeordnet, die nach ihrer Veröffentlichung nicht mehr kontrollierbar sind, aber jederzeit genutzt werden können, vgl. *ders.*, Informationelle Selbstgefährdung, 2016, S. 134–136. Von *Roßnagel* wurde die informationelle Selbstbestimmung als öffentliches Gut eingeordnet, *Roßnagel*, MMR 2005, 71 (75).

711 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 142 Fn. 87.

712 4. Teil., C., II., 1., a)–c).

antwortlichen erfolgen, mit denen entsprechend der *Mosaik-Theorie*[713] umfangreiche Erkenntnismöglichkeiten über die personalen Identitäten entstehen. Somit bringt die Einwilligung unbekannte oder unerwünschte negative Externalitäten mit sich, die sich ökonomisch abbilden lassen.[714]

Schließlich erscheint eine klare Aufteilung zwischen der privaten und öffentlichen Sphäre im online-Kontext faktisch aufgehoben, was den grundrechtlichen Schutz des Privatlebens erschwert und für die Annahme des öffentlichen Gutes persönlicher Informationen im online-Kontext spricht. Folglich bilden die Regelungen des IKT-Rechts die Anreizmechanismen über das öffentliche Gut der persönlichen Informationen, die sich unmittelbar auf das Verhalten des Betroffenen und Verwantwortlichen auswirken. Auf dieser Grundlage soll ein Schutzmechanismus für die personale Identität bestimmt werden.

B. Spieltheoretisches Modell im IKT-Recht

Die spieltheoretische Betrachtung des IKT-Rechts setzt voraus, dass die Akteure miteinander in Beziehung stehen und aufeinander reagieren. Denn die Spieltheorie geht von einem Verhalten des einen Spielers aus, welches eine Reaktion auf das vorangegangene Verhalten des anderen Spielers darstellt und sich damit die Verhaltensweisen aufeinander auswirken.[715] Indem es sich bei der Einwilligung oder den ausgeübten Betroffenenrechten nicht um solipsistische Entscheidungen handelt, sondern diese von dem Verhalten des Verantwortlichen als Spieler geprägt sind, liegt im IKT-Recht ein Interdependenzcharakter zwischen dem Verantwortlichen und Betroffenen vor.[716] Dabei richtet sich das Strategieverhalten der Spieler nach den erreichbaren Gratifikationen oder Sanktionen, so dass die Auszahlungswerte in Gestalt von Kosten oder Nutzen als Anreize für ein bestimmtes Verhalten fungieren. Ebenso reagiert der Spieler auf den vorangegangenen Spielzug des Gegenspielers, so dass die Strategieentscheidung reziprok zum vorangegangenen Spielzug ist und sich dieses auf die folgenden Spieliterationen auswirkt. Zusammengefasst besteht die Spieltheorie aus Spielern, Handlungen, Auszahlungen und Informationen („*Players, Ac-*

713 2. Teil, A., III.
714 *Hermstrüwer*, JIPITEC 2017, 9 (12) Rn. 12.
715 *Rasmusen*, Games and information, 2009, S. 12.
716 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 158.

tions, Payoffs and Information-PAPI") unter der Anname, dass die Spieler versuchen, ihre Auszahlungen zu maximieren.[717]

Die Handlungen der Spieler können in einer bestimmten Kombination zu einem neutralen Gleichgewicht führen, in dem die Strategien miteinander das Optimum einer „effizienten Güterverteilung"[718] bilden, sog. *Nash*-Gleichgewicht. Weiter wirkt sich die Dauer des Spiels mit endlichen Iterationen oder unendlichen Iterationen der Spielzüge auf das Strategieverhalten und den gesamten Verlauf des Spiels aus.[719] Bei den Spielregeln des IKT-Rechts handelt es sich nach den Rechten und Pflichten um ein endliches Spiel, da spiegelbildlich zum Datenzyklus *ex ante* zur Rechtfertigung, mit der Rechtfertigung und *ex post* zur Rechtfertigung die Strategiemöglichkeiten aus den beschränkt zur Verfügung stehenden Rechten und Pflichten erwachsen. Demgegenüber können die Folgen der Datenverarbeitung in ihren Erkenntnismöglichkeiten über eine personale Identität unendlich sein. Dies kann sich auf das Strategieverhalten der Spieler über die persönlichen Informationen auswirken, wenn eine geringe Anzahl von Spieliterationen zu defektivem Verhalten verleitet und eine hohe Anzahl von Spielzügen kooperatives Verhalten begünstigt. Demnach sollen die spieltheoretischen Annahmen (I.), ein von defektivem (II.) und ein von kooperativem Verhalten geprägtes Spiel (III.) diskutiert werden.

I. Annahmen zur spieltheoretischen Modellierung

Zur Angleichung der spieltheoretischen Betrachtung mit dem IKT-Recht bedarf es stipulativer Annahmen, die sich aus dem Gleichlauf mit dem IKT-Recht ableiten lassen. Diese bestehen aus der Informationsasymmetrie zwischen Verantwortlichem und Betroffenem (1.), der verhaltensökonomisch motivierten Entscheidungsfindung durch den Betroffenen im „*Rational Choice*"-Ansatz (2.), und dem Bestehen widerstreitender Interessen als Konflikt und Grundlage für das Gefangenendilemma (3.).

717 *Rasmusen*, Games and information, 2009, S. 12 f.
718 *Eidenmüller*, in: Breidenbach/Henssler (Hrsg.), Mediation für Juristen, 1997, 31 (33).
719 *Rasmusen*, Games and information, 2009, S. 137, 362.

1. Informationsasymmetrien

Die Informationsasymmetrie zwischen dem Verantwortlichen und Betroffenen geht auf den jeweiligen Informationsstand im Datenzyklus über eine personale Identität zurück. *Ex ante* zur Rechtfertigung hat der Verantwortliche die Kenntnis über die tatsächliche technische und organisatorische Gestaltung des Dienstes und die Entscheidungsmacht darüber, welche Informationen gemäß Art. 12, 13 DSGVO transparent gemacht werden. Dabei werden die mit der Datenverarbeitung verbundenen Risiken aus einer vorangegangenen Risikobewertung oder Datenschutz-Folgenabschätzung gemäß Art. 25 DSGVO typischerweise nur rudimentär in den Informationspflichten erscheinen und können im Übrigen zum Geschäftsgeheimnis des Verantwortlichen gehören. Die Informationsasymmetrie zugunsten des Verantwortlichen besteht somit bereits mit Beginn des Datenzyklus zu Lasten des Betroffenen und wird durch bevorstehende Gratifikation ausgelöst. Auf der Rechtfertigungsebene kann eine Kompensation der Informationsasymmetrie erfolgen, wenn die Informationen aus der Datenschutzerklärung in den Entscheidungsprozess einbezogen werden, was in Anbetracht endogener und exogener Entscheidungsfaktoren als fraglich erscheinen dürfte. Nach der Rechtfertigung wird der Ausgleich der Informationsasymmetrie durch das Auskunftsrecht und die weiteren Betroffenenrechte möglich. Obwohl innerhalb des Datenzyklus regelmäßig die Chance für eine Kompensation der Informationsasymmetrie besteht, wirkt die anfängliche Informationsasymmetrie über die begründete personale Identität in ihrem Erkenntniswert fort. Mit jeder Kontrolle der personalen Identitäten nach der Rechtfertigung wird eine Korrektur der personalen Identität möglich, wobei selbst bei der Ausübung des Rechts auf Vergessenwerden gemäß Art. 17 DSGVO ein eigener Erkenntnisgehalt verbleiben kann.

Insgesamt wirkt somit die anfängliche Informationsasymmetrie in abweichender Intensität fort und könne durch den Einsatz von Algorithmen zur Profilerstellung zu einer weiteren „gigantische(n) Asymmetrie des Wissens“[720] führen. Gleichwohl ist ein Ausgleich der Informationsasymmetrie *ex post* zur Rechtfertigung durch einen öffentlich gewordenen Datenskandal oder negative Bewertungen in Datenschutzbewertungsportalen[721]

720 *Graf von Westphalen*, IWRZ 2018, 9 (12); ebenso zur Informationsasymmetrie *Hoffmann-Riem*, in: Augsberg (Hrsg.), Ungewissheit als Chance, 2009, 17; *Acquisti*, ACM 2004, 21 (24); *Shapiro*, Negotiating the nonnegotiable, 2017, S. 167.

721 *Ben-Shahar/Strahilevitz*, The Journal of Legal Studies 2016, S1–S11, (S4 f.).

möglich, sofern sich diese auf das Strategieverhalten des Betroffenen auswirken würden.

Diese beschriebene Informationsasymmetrie im Rahmen der Datenverarbeitung ist parallel zur Informationsasymmetrie in einer Prinzipal-Agenten-Beziehung[722], wonach der Verantwortliche als Prinzipal gilt und über die tatsächlichen Informationen zur Datenverarbeitung verfügt und der Betroffene als Agent den Maßgaben des Prinzipals unterliegt. Folglich ist dem IKT-Recht immanent, dass von dem Verantwortlichen gegenüber dem Betroffenen eine Prinzipal-Agenten-Beziehung besteht, die bereits *ex ante* zur Datenverarbeitung vorliegt. Damit wirkt die Informationsasymmetrie über den Datenzyklus fort und durch das Wirken von Netzwerkeffekten kann unter erleichterten Bedingungen ein „*take it or leave it*"-Angebot entstehen, unter dem sich die Informationsasymmetrie perpetuiert.

Für das Strategieverhalten der Spieler bringt das IKT-Recht damit eine strukturelle Informationsasymmetrie zugunsten des Verantwortlichen mit sich. Der Spielraum für eine Gegenstrategie des Betroffenen, einen adäquaten Schutz der persönlichen Informationen herbeizuführen, ist gering ausgeprägt. Die Verhandlungsmacht des Betroffenen ist damit über den Datenzyklus hinweg als schwach einzuordnen, was einen Kompensationsbedarf auslöst.

2. Rationale Strategieentscheidung

Die Strategieentscheidung basiert auf der Annahme, dass sich das Verhalten der Spieler am maximalen eigenen Nutzen ausrichtet. Der Spieler handelt in dem spieltheoretischen Modell mit einer Kosten-Nutzen-Analyse und orientiert seine Strategie daran, mit welchem Verhalten die höchsten Auszahlungswerte erreicht werden können und an welcher Stelle ein geringes Kostenrisiko besteht. Abhängig davon, ob die Anzahl der Spieliterationen von vornherein bestimmt ist oder nicht, kann die Strategie, *ob* und *wann* ein kooperativer oder defektiver Spielzug erfolgen soll, variieren. Weiter kann sich die Strategie in einem späteren Stadium der Spieliterationen aufgrund eines neuen Informationsstandes oder als Reaktion auf eine vorangegangene Defektion ändern. Darin wird die Interdependenz der Strategieentscheidungen und deren exogene Entscheidungsbeeinflussung deutlich, so dass überraschende und außerhalb der Verhandlungssituation

722 *Rasmusen*, Games and information, 2009, S. 182–185.

liegende Entscheidungen nach dem spieltheoretischen Modell unüblich sind.[723]

Im IKT-Recht wirkt sich die Entscheidung des Verantwortlichen über den eingesetzten Stand der Technik und das Bestehen einer möglichen Zertifizierung auf die Strategiewahl des Betroffenen aus. Der Betroffene wird das Produkt oder den Dienst wählen, mit dem der beste Auszahlungswert verbunden ist. Diese Auszahlung kann in dem Schutz der persönlichen Informationen liegen oder den Zugang zu sozialen Medien durch einen Intermediär darstellen. Die Strategie des Verantwortlichen über die Umsetzung der Informationspflichten in den Datenschutzerklärungen wird sich ebenfalls auf die Entscheidungsfindung des Betroffenen auswirken können. Denn der Verantwortliche kann Datenschutzerklärungen derart gestalten, dass etwa mit einem sog. „*one pager*" bei dem Betroffenen eine Zeitersparnis in der Entscheidungsfindung erreicht und eine effektive Entscheidungsfindung erleichtert wird. Gleichwohl kann sich eine derartige Strategie faktisch nicht als Gratifikation für den Betroffenen erweisen, sondern sich aufgrund einer oberflächlicheren Informationslage auf den Schutz der persönlichen Informationen auswirken und damit zum Kostenfaktor werden. Weiter wird mit der Erteilung der Einwilligung ein Auszahlungswert verbunden sein, dem eine subjektive Annahme des Betroffenen über das folgende Verhalten des Verantwortlichen dahingehend zugrunde liegt, dass die personenbezogenen Daten nach dem Stand der Technik ausreichend geschützt werden. Schließlich folgt *ex post* zur Rechtfertigung die Strategieentscheidung über die Geltendmachung der Betroffenenrechte.

Gegenüber dieser spieltheoretischen Annahme des *rational choice*-Ansatzes lässt sich kritisch anmerken, dass eine ausschließlich rationale Entscheidung unter Einbeziehung der neuen Erwartungstheorie die individuellen Präferenzen und exogenen Entscheidungsfaktoren unberücksichtigt lässt.[724] Gleichwohl wird in der rechtlichen Annahme des *rational choice*-Ansatzes von *van Aaken* eine verhaltenskoordinierende Funktion und damit ein Fokalpunkt gesehen,[725] mit dem neben der rechtlichen Orientierung eine Grundlage für die spieltheoretische Modellierung geschaffen wird. Demnach soll der *rational choice*-Ansatz in seiner verhaltenskoordinierenden Funktion für die spieltheoretische Modellierung herangezogen

723 *Ders.*, Games and information, 2009, S. 13.
724 4. Teil, C., II., 1., b), bb).
725 *Van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (190).

werden, ohne dass endogene und exogene Entscheidungsfaktoren für die Gesamtbetrachtung der Identitätsverwaltung unberücksichtigt bleiben.

3. Konflikt und Eskalationsstufe

Das IKT-Recht regelt divergierende Ausgangspositionen des Verantwortlichen und Betroffenen bereits auf der Ebene des Informationszugangs, so dass die Positionen über den Zugang zu den Informationen der technischen Datenverarbeitung und der generierten personalen Identität asymmetrisch zu Lasten des Betroffenen verteilt sind. Weiter divergieren die Interessen des Verantwortlichen und des Betroffenen dahingehend, dass der Verantwortliche die Datenverarbeitung und Erstellung von personalen Identitäten mit einem wirtschaftlichen Interesse verfolgt und der Betroffene das Interesse an der schlichten Nutzung des Dienstes hat. Dabei kann das Nutzungsinteresse gegenüber dem Interesse am Schutzniveau über die persönlichen Informationen vorrangig sein.

Weiter kann mit der Geltendmachung der Betroffenenrechte der Interessenkonflikt offensichtlich werden. Denn der Verantwortliche wird sich fragen müssen, welche Informationen im Rahmen des Auskunftsrechts offengelegt werden müssen und welche Informationen strategisch offenzulegen sind. Darüber hinaus muss der Verantwortliche klären, welche Informationen von dem Löschanspruch erfasst sind und welche Erkenntnisse über eine personale Identität davon nicht erfasst sind.

Daraus kann sich ein Konflikt über das Bild der personalen Identität aus der Perspektive des Betroffenen gegenüber dem Bild der personalen Identität aus der Perspektive des Verantwortlichen ergeben. Denn es stehen sich das Ergebnis der generierten personalen Identität durch den Verantwortlichen in Gestalt eines Bildes und das Ergebnis des Selbstbildes des Betroffenen gegenüber. Diese Divergenz hat ihren Ursprung in den IKT-rechtlich begründeten Asymmetrien der Verhandlungspositionen und der ökonomisch beeinflussten Interessenlagen des Verantwortlichen und Betroffenen. Insofern divergieren die Interessen des Verantwortlichen an einer umfangreichen Datenverarbeitung und Profilerstellung mit den Interessen des Betroffenen an einem möglichst hohen Schutzniveau über die persönlichen Informationen, so dass zwischen diesen beiden Spielern eine Konfliktlage besteht.

Bei der Bewertung der Konfliktintensität in Gestalt des Eskalationsgrades kommt nach dem Stufenmodell von *Glasl*[726] ein Interessenkonflikt in der zweiten Eskalationsstufe in Betracht. Danach ist der Konflikt von der Debatte und Polemik gekennzeichnet, so dass die Spieler das Interesse an der Durchsetzung ihres Standpunktes verfolgen.[727] In dieser Stufe besteht der Konflikt aus defektiven und kooperativen Elementen, die aber leicht in die dritte Eskalationsstufe übergehen können und der Konflikt dann aus Taten statt Worten bestünde.[728] Mit der weiteren Eskalation des Konflikts entwickelt sich dieser in die Richtung einer „*win-lose*"-Lösung,[729] die zu Lasten des öffentlichen Gutes der persönlichen Informationen ginge.

Für den Verantwortlichen liegt der Nutzen in dem Konflikt darin, dass der Betroffene seine persönlichen Informationen mit der Einwilligung oder durch einen anderen Rechtfertigungsgrund offenlegt. Folglich entsteht ein IKT-rechtlich begründeter Konflikt über die Bilder personaler Identitäten zwischen dem Verantwortlichen und Betroffenen in einer noch frühen Eskalationsstufe, mit der aber eine Lösung noch realisierbar wäre. Sobald der Rechtsbeziehung zwischen dem Verantwortlichen und Betroffenen von vornherein ihre Konflikthaftigkeit mit dieser Eskalationsstufe zugebilligt wird, kann diese ein Anknüpfungspunkt für eine Lösung mit dem Identitätsverwaltungsmodell bilden. Dann würde es um die Umgestaltung und Neubildung der Beziehung zwischen dem Verantwortlichen und Betroffenen[730] über die jeweiligen Bilder personaler Identitäten im Rahmen einer Konfliktlösung gehen. Diese Konfliktlösung könnte eine Stärkung des Schutzes der persönlichen Informationen bedeuten. Damit könnte eine Kompensation der bestehenden Marktmacht von Intermediären gegenüber dem Betroffenen ermöglicht werden.

4. Zusammenfassung

Die Annahmen für eine spieltheoretische Modellierung lassen sich auf das Modell der Identitätsverwaltung im IKT-Recht übertragen. Zwischen dem Verantwortlichen und dem Betroffenen besteht aufgrund der IKT-rechtlichen Regelungen eine Informationsasymmetrie, da die technischen und

726 *Glasl*, Konfliktmanagement, 2020, S. 243 ff.
727 *Ders.*, Konfliktmanagement, 2020, S. 249–260.
728 *Ders.*, Konfliktmanagement, 2020, S. 260 f.
729 *Ders.*, Konfliktmanagement, 2020, S. 269.
730 *Shapiro*, Negotiating the nonnegotiable, 2017, S. 149.

organisatorischen Maßnahmen und die mit der Datenverarbeitung verbundenen Risiken für den Betroffenen über den Datenzyklus der personalen Identität teilweise intransparent sind. Dabei tragen die Betroffenenrechte nur eingeschränkt zu einem Ausgleich der Informationsasymmetrie bei.

Aus spieltheoretischer Sicht könnte gerade in den B2C- und P2C-Konstellationen die Prinzipal-Agenten Beziehung für die Strategieentscheidungen angenommen werden. Diese Strategieentscheidungen werden als dem *rational choice*-Ansatz unterliegende Entscheidungen der Spieler angenommen, die sich an den möglichen Auszahlungswerten orientieren und das potentielle Folgeverhalten des Gegenspielers zu antizipieren versuchen.

Weiter stehen die IKT-rechtlich geprägten Verhandlungspositionen und Interessenlagen des Verantwortlichen und Betroffenen über die Bilder der personalen Identität in einem konflikthaften Verhältnis zueinander. Gleichwohl ist die Eskalationsstufe noch in einem Anfangsstadium, so dass eine „*win-win*"-Lösung noch möglich erscheint. Insgesamt liegt den spieltheoretischen Grundannahmen ein prozedurales Konzept zugrunde, welches die informationsbasierten Strategieentscheidungen und ihre Auswirkungen auf die nächste Iteration des Spiels einbezieht. Dabei gilt es, für das Identitätsverwaltungsmodell die Strategien in den Spieliterationen für die mögliche Lösung konträrer Bilder personaler Identitäten in eine „*win-win*"-Lösung für den Verantwortlichen und den Betroffenen zu überführen.

II. Gefangenendilemma im IKT-Recht

1. Einführung

Das spieltheoretische Modell im IKT-Recht soll für die Identitätsverwaltung am Gefangenendilemma veranschaulicht werden. In diesem Spiel ist die Ausgangssituation davon geprägt, das zwischen den Spielern ein Gut aufgeteilt werden soll. Die Spieler müssen sich bei jeder Spieliteration zwischen Defektion und Kooperation entscheiden. Dabei wirkt sich der Vorteil für einen Spieler zum Nachteil für den anderen Spieler aus, sog. Nullsummenspiel. Am Ende des Spiels würde typischerweise eine distributive „*win-lose*"-Konstellation entstehen. Als berühmtes Beispiel wird als Verteilungsgegenstand eine Orange angeführt, die jeweils von beiden Spielern

benötigt wird und nur einer diese Orange erhalten könne.[731] Bei einer Spieliteration erscheint das defektive Verhalten, eine ganze Orange erhalten zu wollen, für die Spieler vorteilhafter zu sein, so dass dieses gegenüber kooperativem Verhalten vorgezogen wird.[732]

Sobald das Spiel aus mehreren Spieliterationen besteht, kann defektives Spielverhalten folgenreich sein und einen „Schatten auf die Gegenwart"[733] werfen, der sich auf das folgende Spielverhalten unmittelbar auswirkt und zu einer Verhaltensanpassung führen kann. Dabei geht es langfristig darum, ein *Nash*-Gleichgewicht herzustellen, mit dem sich auf beiden Seiten eine Lösung einstellt, die für beide Spieler nicht besser sein kann, sog. Fokalpunkte.[734] Gleichwohl handelt es sich nicht um ein ethisch oder rechtlich anerkanntes Gleichgewicht, sondern allein um das mathematisch beste Ergebnis für beide Spieler.

Im IKT-Recht bestehen mehrere Spieliterationen, die sich im Wesentlichen aus den Rechten und Pflichten *ex ante* zur Rechtfertigung, der Rechtfertigung selbst und *ex post* zur Rechtfertigung zusammensetzen. Dabei geht es zu Beginn des Datenzyklus um die Verteilung des öffentlichen Gutes der persönlichen Informationen in Gestalt eines Zugangs zu den Informationen über die Datenverarbeitung. Im Folgenden geht es *ex post* zur Rechtfertigung darum, dass der Verantwortliche dem Betroffenen eine Zugangsmöglichkeit über die personenbezogenen Daten einräumt, mit dem die personalen Identitäten einsehbar werden. Sobald eine Ablehnung der Zugangsmöglichkeit oder nur ein eingeschränkter Zugang erfolgt, würde dies für den Betroffenen zu einer Einbuße des öffentlichen Gutes der persönlichen Informationen führen. Insoweit kann bei ökonomischer Betrachtung ein „Austauschverhältnis" angenommen werden, bei dem die Einwilligung zur Dienstnutzung mit dem „Gegenwert" von Daten erfolgt.[735]

Demnach soll sich im Folgenden die spieltheoretische Modellierung auf die generierten personalen Identitäten im Sinne einer Allokation von persönlichen Informationen beziehen. Das IKT-Recht bringt als Spieler den Betroffenen und den Verantwortlichen hervor, die in ihrer Strategie nach dem spieltheoretischen Modell zwischen defektivem und kooperativem

731 *Axelrod/Raub*, Die Evolution der Kooperation, 1991, S. 7.
732 *Besemer*, Mediation, 2007, S. 25 f.
733 *Axelrod/Raub*, Die Evolution der Kooperation, 1991, S. 11.
734 *Rasmusen*, Games and information, 2009, S. 32 f.; *Nash*, Econometrica 1950, 155; *Rajbhandari/Snekkenes*, in: IFIP Advances in Information and Communication Technology, vol. 352, 2010, 41.
735 2. Tei, D., II., 2., a).

Verhalten wählen können (2.), (3.). Daher sollen die Kooperationsmöglichkeiten (a) und die Defektionsmöglichkeiten (b) nach den Datenverarbeitungsphasen des IKT-Rechts herausgearbeitet werden. Diese können kontextspezifisch variantenreich sein und sollen im Folgenden für die Verdeutlichung exemplarisch aufgeführt werden.[736]

2. Strategiewahl durch den Betroffenen im IKT-Recht

a) Kooperation über die personale Identität

Mit der Strategieentscheidung des Betroffenen zur Kooperation werden *ex ante* zur Rechtfertigung die Reputation des Verantwortlichen und die Informationen über die Datenverarbeitung in die Entscheidungsfindung einbezogen. Bei den Informationspflichten zu der Datenverarbeitung könnte eine hypothetische Konsultation oder Befragung des Verantwortlichen ermöglicht werden, welche in eine Verhandlung und damit Kooperation münden würde. Weiter kann bei der Rechtfertigung der Datenverarbeitung die Strategieentscheidung dahingehend getroffen werden, dass eine freiwillige Einwilligung nicht erteilt wird und die personale Teilidentität in dem Kontext nicht entstehen soll. Ferner kommt nach der Rechtfertigung ohne aktive Handlung eine kooperative Handlung durch die Geltendmachung des Auskunftsrechts in Betracht und dem folgend die Geltendmachung weiterer Betroffenenrechte. Damit kann der Zugang zu der personalen Identität gewährt werden und über die Betroffenenrechte die personale Identität in relativer Hinsicht kontrolliert werden. Insgesamt wird bei einer kooperativen Strategiewahl des Betroffenen erkennbar, dass dem Grunde nach eine Einwilligung nicht erteilt werden dürfte, und die Nutzung des Dienstes auf ein minimales Maß zu beschränken wäre. Dies käme einer digitalen Abstinenz gleich, die jedoch in Anbetracht der Ubiquität von Datenverarbeitungen in praktischer Hinsicht fernliegend erscheint.

b) Defektion über die personale Identität

Der Betroffene kann sich defektiv gegenüber der entstandenen personalen Identität verhalten, indem *ex ante* zur Rechtfertigung die Informationen

736 Vgl. *Zander/Steinbrück/Birnstill*, DuD 2019, 270.

über die Reputation des Verantwortlichen und die potentiellen Risiken der Datenverarbeitung in die Strategieentscheidung nicht einbezogen werden. Weiter kann in der Rechtfertigung defektives Verhalten liegen, wenn die Einwilligung erteilt wird und wenn ohne aktive Handlung mit der Datenverarbeitung die personale Identität generiert wird. Dies kann mit der unmittelbaren Gratifikation durch den Zugang zum Dienst und dem Wirken von Netzwerkeffekten begünstigt werden. Zum Schutz der personalen Identitäten bei der Nutzung von Diensten kann defektives Verhalten darin liegen, die Angabe des Klarnamens zu umgehen. Ferner liegt nach der Rechtfertigung defektives Verhalten vor, wenn die Strategieentscheidung des Betroffenen sich gegen die Inanspruchnahme des Auskunftsrechts und der weiteren Betroffenenrechte richtet, was sich ebenfalls durch fehlende Anreize und Gratifikationen begründen lässt. Insgesamt würde mit der gerechtfertigten Datenverarbeitung eine personale Identität in der Sphäre des Verantwortlichen entstehen, die aufgrund defektiver Strategieentscheidungen fortbestehen und nicht zum Kontrollgegenstand des Betroffenen werden würde.

3. Strategiewahl durch den Verantwortlichen im IKT-Recht

a) Kooperation über die personale Identität

Die Strategieentscheidung des Verantwortlichen vor der Datenverarbeitung bezieht sich zunächst auf die Gestaltung des Datenverarbeitungsprozesses in technischer und organisatorischer Hinsicht. Dabei würde eine kooperative Strategiewahl in einem besonders ausgeprägten Schutz personenbezogener Daten mit dem Stand der Technik bestehen und den Einsatz von *„privacy enhancing technologies"* umfassen. Ebenso kann die Strategieentscheidung die öffentliche Reputation des Dienstanbieters durch Zertifizierungen einschließen. Damit könnte der Betroffene das Vertrauen über den Schutz der persönlichen Informationen bei den Verbrauchern aufbauen.

Weiter könnte die Strategieentscheidung des Verantwortlichen *ex ante* zur Rechtfertigung solche Datenschutzerklärungen umfassen, die in einer klar verständlichen Sprache und in einem über die Risiken aufklärenden *„one pager"* zusammengefasst sind. Bei der Rechtfertigung könnte vorzugsweise die Rechtfertigung durch die Einwilligung als Strategie gewählt werden, womit eine gesteigerte Kontrollmöglichkeit des Betroffenen herbeigeführt würde. Weiter wäre in die Strategieentscheidung *ex post* zur Rechtfer-

tigung ein umfassendes Konzept zur Gewährleistung der Betroffenenrechte unter verbraucherfreundlichen Bedingungen einzubeziehen. Dabei könnten die Strategieentscheidungen durch den Verantwortlichen über die Regeln des IKT-Rechts hinaus Schutzmechanismen für die persönlichen Informationen enthalten, was sich als Wettbewerbsvorteil auswirken könnte. Diese kooperative Strategiewahl würde einen gesteigerten Kostenaufwand bei dem Verantwortlichen auslösen und zugleich eine Investition darstellen können. Denn mit der Einbeziehung von gesteigerten Schutzmechanismen für die persönlichen Informationen über das rechtlich geforderte Mindestmaß hinaus, kann das Vertrauen der Verbraucher in die datenschutzrechtliche Qualität des Dienstes hergestellt werden. Diese datenschutzrechtliche Qualität könnte zum Gegenstand entsprechender Produkt- und Dienstbeschreibungen werden und sich damit auf die Reputation des Verantwortlichen in der Öffentlichkeit auswirken.

b) Defektion über die personale Identität

Die Strategiewahl des Verantwortlichen über die personale Identität beginnt mit der Entscheidung über den geeigneten Stand der Technik zur Gewährleistung des Schutzes der personenbezogenen Daten. Dieser kann in der öffentlichen Darstellung des Dienstes und in der Entscheidung, sich nicht zum Schutz personaler Identitäten zu äußern, liegen. Die Informationspflichten über die Datenverarbeitung zur personalen Identität sind defektiv gestaltet, wenn Sie entweder nicht den Anforderungen gemäß Art. 12, 13 DSGVO entsprechen oder durch eine unklare Sprache und eine zu lange Datenschutzerklärung gerade noch den rechtlichen Anforderungen entsprechen. Dabei kommt der Zweckbestimmung eine besondere Bedeutung zu. Sobald der Zweck sehr weitgehend bestimmt wird, sinkt der Schutz für den Betroffenen, da die Vorhersehbarkeit der möglichen Datenverarbeitungen erschwert wird.

Weiter kann auf der Rechtfertigungsebene von einer defektiven Ausgestaltung ausgegangen werden, wenn vorzugsweise Rechtfertigungsgründe ohne eine aktive Handlung des Betroffenen gewählt werden. Nach der Rechtfertigung würde eine defektive Strategiewahl vorgenommen werden, wenn der ursprüngliche Zweck gemäß Art. 6 Abs. 4 DSGVO ohne erneute Einwilligung bei bestehender Vereinbarkeit geändert wird. Weiter liegt nach der Rechtfertigung eine defektive Strategiewahl vor, wenn mit der Geltendmachung des Auskunftsrechts dieses durch den Verantwortlichen nicht rechtskonform oder gerade noch rechtskonform realisiert und der

Zugang zu der personalen Identität nur teilweise gewährt würde. Ferner würde die Strategiewahl bei den Betroffenenrechten defektiv ausgestaltet sein, wenn diese nicht rechtskonform oder gerade noch rechtskonform durchgeführt werden und etwa die Löschung oder Übertragung personaler Identitäten unvollständig erfolgen würde. In diesen Strategieentscheidungen wählt der Verantwortliche die Maßnahmen mit einem geringen Kosten- und Organisationsaufwand, so dass das Risiko eines Rechtsverstoßes besteht und möglicherweise in Kauf genommen wird.

4. Bewertung

In dem Gefangenendilemma über die Verteilung des öffentlichen Gutes der persönlichen Informationen wirken sich die Strategien direkt auf die generierbaren personalen Identitäten und ihren Erkenntnisgehalt aus. Dies betrifft einerseits das Verhältnis zwischen dem Verantwortlichen und Betroffenen und andererseits die Gesamtwirkung auf andere Betroffene in Gestalt von Netzwerkeffekten, so dass die defektive Strategiewahl tendenziell zu einer „*win-lose*"-Situation führt. Neben der nachteiligen Verteilung des öffentlichen Gutes für den Betroffenen in dem Nullsummenspiel führt die „*win-lose*"-Situation zu einer Erosion des Schutzes persönlicher Informationen und der personalen Identitäten.

Zum Schutz der persönlichen Informationen führt die kooperative Strategiewahl von beiden Spielern zu dem höchsten Schutzniveau für die personalen Identitäten. Gleichwohl erscheinen die dargestellten kooperativen Strategien zunächst unökonomisch für den Verantwortlichen und praxisfern für die Betroffenen. Dennoch sollen die kooperativen Strategien als Modellgrundlage dienen, um die Lösung für einen technisch unterstützten Schutzmechanismus personaler Identitäten im Identitätsverwaltungsmodell herleiten zu können. Dafür sollen die von Defektion und Verteilung geprägten Strategien mit dem Konzept der Verhandlung erweitert werden. Dieses knüpft an die Strategiewahl der Kooperation an, die als Grundlage für einen Schutzmechanismus in dem Identitätsverwaltungsmodell weiter untersucht werden soll.

III. Verhandlung im IKT-Recht

1. Einführung

Mit dem Modell der Spieltheorie lassen sich die Wahlmöglichkeiten der Strategien auf defektives und kooperatives Verhalten beschränken, so dass für die Schutzsteigerung der personalen Identität und der Einräumung einer Verhandlungssituation die kooperative Strategieentscheidung im Vordergrund stehen soll. Mit der kooperativen Strategie können Wertschöpfungspotentiale im Sinne eines Kooperationsgewinnes[737] über den Schutz der persönlichen Informationen unter der Annahme, dass ein Konflikt die Herausforderung beider Spieler in gleichem Maße sei,[738] generiert werden. So wird der kooperativen Strategie zugesprochen, dass sie die zivilisatorische Grundlage bilde, obwohl die negative Kooperation etwa durch Korruption ebenfalls denkbar sei.[739] Dabei wird in Kooperationsspielen miteinander verhandelt, um einen Vorteil aus dem Spiel generieren zu können und gleichzeitig soll mit der kooperativen Verhandlung eine Harmonisierung der Interessenlage[740] über den Schutz der persönlichen Informationen herbeigeführt werden können.

Für die Verhandlung mit einer primär kooperativen Strategie bildet das Vertrauen die Grundlage, da erst mit dem Vertrauen in die Strategieentscheidung des Gegenspielers das Strategieverhalten entsprechend auf eine kooperative Strategie angepasst werden könne.[741] Folglich muss der Frage nachgegangen werden, mit welchem Anreizmechanismus die Kooperation gefördert und das Vertrauen gesteigert wird, damit durch das kooperative Verhalten eines Spielers ein für die Zukunft wirkender Schatten gelegt wird.[742] Dies setzt voraus, dass im IKT-Recht das Konzept der Kooperation verankert ist und dieses als Anknüpfungspunkt für ein kooperatives Verhandlungskonzept über die Bilder personaler Identitäten fungieren kann.

---

737 *Eidenmüller*, in: Breidenbach/Henssler (Hrsg.), Mediation für Juristen, 1997, 31 (36).
738 *Shapiro*, Negotiating the nonnegotiable, 2017, S. 128.
739 *Axelrod/Raub*, Die Evolution der Kooperation, 1991, S. 3 f., 18.
740 *Brandimarte/Acquisti*, in: Peitz/Waldfogel (Hrsg.), The Oxford Handbook of the Digital Economy, 2012, S. 565.
741 *Schelling*, The strategy of conflict, 1969, S. 54 f.; *Watzlawick/Beavin/Jackson*, Menschliche Kommunikation, 2016, S. 61 ff.
742 *Axelrod/Raub*, Die Evolution der Kooperation, 1991, S. 112.

2. Förderung der Kooperation

Die Förderung der Kooperation im IKT-Recht erscheint bereits im Zusammenhang mit dem behördlichen Kooperationsgebot gemäß Art. 31 DSGVO. Danach sollen die verantwortliche Stelle und der Auftragsdatenverarbeiter mit der Aufsichtsbehörde „zusammenarbeiten", worin sich ein kooperatives Element in der DSGVO widerspiegelt. Weiter komme in Art. 33 Abs. 4 DSGVO der kommunikative Austausch mit der Aufsichtsbehörde zum Ausdruck, wenn für die Meldung der Verletzung des Schutzes personenbezogener Daten die Informationen schrittweise zur Verfügung gestellt werden dürfen, sofern nicht alle Informationen zur gleichen Zeit bereitgestellt werden können.[743] Ebenso wird im IT-Sicherheitsrecht ein kooperatives Konzept angenommen, wonach zwischen Staat und Wirtschaft eine vertrauensvolle Kooperation als sog. „*shared mission*" hergestellt werden soll.[744] Darin liegen staatliche Regelungsansätze, mit denen rechtliche Konfliktlagen in Anbetracht der schnellen Entwicklungen und Veränderungen in der Informationstechnologie durch ein Verfahren im Rahmen der Selbstregulierung gelöst werden können.[745] Dieses Verfahren ermögliche einen erweiterten Informationsaustausch mit einer höheren Problemlösungskapazität, um eine gesteigerte Akzeptanz und Wirksamkeit von Lösungen erreichen zu können.[746] Insoweit nähme der Staat seine Gewährleistungsverantwortung zur Herbeiführung innovationsoffener Lösungen über die rechtlichen Regelungen wahr, die im Einzelnen ein funktionales Zusammenwirken zur Umsetzung des Kooperationsprinzips fördern und als regulierte Selbstregulierung wirken würde.[747]

Demnach bildet Art. 31 DSGVO einen Anknüpfungspunkt für die Anerkennung der Kooperation in der DSGVO als Ausprägung der regulierten Selbstregulierung im Datenschutzrecht. Folglich lässt sich die Kooperationsförderung als ein bereits im Datenschutzrecht bestehendes Konzept annehmen, welches als wesentlicher Anhaltspunkt für die Implementierung der Identitätsverwaltung herangezogen werden soll. Dafür soll zur Schaf-

743 *Martini*, in: Paal/Pauly/Ernst (Hrsg.), Kommentar, DS-GVO, 2018, Art. 33 DSGVO Rn. 51 f.; *Jandt*, in: Kühling/Buchner (Hrsg.), Kommentar, DS-GVO, BDSG, 2018, Art. 33 DSGVO Rn. 23.

744 *Dürig/Fischer*, DuD 2018, 211 (214)

745 *Spindler/Thorun*, MMR-Beilage 2016, 1 (17).

746 *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts Gesamtwerk, 2012, § 19 Rn. 59.

747 *Ders.*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts Gesamtwerk, 2012, § 19 Rn. 52 f.

fung eines Kooperationsumfeldes die Steigerung der Iterationen dargestellt (a), die *TIT for TAT*-Strategie diskutiert (b) und die Übertragung auf die Bilder personaler Identitäten vorgenommen werden (c).

a) Steigerung der Iterationen

Die Kooperation kann gefördert werden, wenn die Chancen für kooperatives Verhalten gesteigert werden. Dabei bestünde bei unendlichen Spieliterationen (sog. „*Supergame*“) eine hohe Wahrscheinlichkeit, dass die Strategieentscheidung zugunsten der Kooperation ausgehen wird.[748] Gerade unter der vorliegenden Annahme einer Informationsasymmetrie hat die Steigerung der Spieliterationen zur Folge, dass sich bestimmte subjektive Wahrscheinlichkeiten in der Vorstellung des Spielers auf die Strategieentscheidung zur Kooperation auswirken können, weil das Fehlen von Informationen zum Ausgleich der Informationsasymmetrie ignoriert werde und defektives Verhalten des Betroffenen keinen Sinn machen würde.[749] Dabei würde sich die kooperative Strategiewahl wie ein Schatten auf die Zukunft legen, da diese bei dem Gegenspieler ebenfalls eine kooperative Strategieentscheidung in einer späteren Spieliteration auslösen und zu einer *Selbstbindung* zur Kooperation führen könne.[750]

Um eine Reputation über die Anwendung kooperativer Verhandlungsstrategien herbeiführen zu können, fördert eine hohe Anzahl an Spieliterationen das Wirken einer kooperativen Strategieentscheidung auf die folgenden Spieliterationen. Denn sobald ein Spieler die Reputation zu kooperativem Verhalten hat, kann dies bei dem Gegenspieler die Bereitschaft auslösen, seine Strategieentscheidung an dem letzten kooperativen Spielzug zu orientieren und sich damit ebenso kooperativ zu verhalten. Demnach gehe es bei der gezielten Kooperationsförderung darum, eine Spieliteration in mehrere Spieliterationen zu zerlegen oder eine andere Methode zur Iterationssteigerung zu bestimmen.[751]

Insgesamt ist gegen die Annahme der Förderung des Schutzes der persönlichen Informationen durch Kooperation die Strategievariante anzu-

748 *Axelrod/Raub*, Die Evolution der Kooperation, 1991, S. 9; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 177 f.

749 *Rasmusen*, Games and information, 2009, S. 137–140; *Faber/Sedlacek*, DuD 2017, 440 (445).

750 *Axelrod/Raub*, Die Evolution der Kooperation, 1991, S. 113–117; *Faber/Sedlacek*, DuD 2017, 440 (444).

751 *Dies.*, Die Evolution der Kooperation, 1991, S. 119.

führen, die nicht an die letzte Spieliteration anknüpft.[752] Danach bezieht sich die Strategieentscheidung auf eine deutlich frühere Spieliteration, die etwa eine defektive Strategieentscheidung war. Sollte eine frühere negative Reputation vorliegen, könnte diese zu einer Abkehr von der ursprünglichen Kooperation führen, so dass die nächste Spieliteration in defektivem Verhalten liegt. Folglich stellt sich insgesamt die Frage nach einem kooperationsfördernden Strategieverlauf.

b) Kooperationsförderung mit der „*TIT for TAT*"-Strategie

Die Kooperationsförderung zur Verhandlung der Bilder personaler Identitäten kann eine bestimmte Abfolge von defektivem und kooperativem Verhalten voraussetzen. Von *Axelrod* wurde in „*The Evolution of Cooperation*" nachgewiesen, dass die „*TIT for TAT*"-Strategie zu kooperativem Verhalten führt und dafür die beste Strategie darstelle.[753] Der Begriff „*TIT for TAT*" beschreibt ein Verhalten, welches die spiegelbildliche Reaktion zu vorangegangenem Verhalten darstellt, so dass auf Defektion eine defektive Reaktion und auf Kooperation eine kooperative Reaktion folgt. Entscheidend für den Verlauf der Spieliterationen ist, dass die *TIT for TAT*-Strategie mit der Kooperation beginnt und der folgende Spielverlauf durch reziproke Reaktionen auf kooperatives oder defektives Verhalten geprägt ist. Indem *TIT for TAT* mit Kooperation beginnt, wird eine positive Reputation begründet und der Schatten für eine reziprok kooperative Reaktion vergrößert, so dass die Chance für Kooperation in den folgenden Spieliterationen steige.[754] Demgegenüber könne sich bei wiederholter Defektion die Frage nach der Nachsichtigkeit stellen, die auch bei Defektion von einem reziproken Verhalten absieht und gezielt aus einem Optimismus heraus Kooperation einsetzt.[755]

Die Annahme dieser Strategie besteht aus dem Verhalten von zwei Spielern und könne sich ohne den Anreiz einer Autorität realisieren, wenn sich eine Gemeinschaft aus *TIT for TAT* anwendenden Spielern selbst überwacht.[756] Auch gegenüber anderen Strategien wirke die *TIT for TAT*-Strate-

752 *Rasmusen*, Games and information, 2009, S. 110.
753 *Axelrod/Raub*, Die Evolution der Kooperation, 1991, S. 12 f.
754 *Dies.*, Die Evolution der Kooperation, 1991, S. 28, 126; *Rasmusen*, Games and information, 2009, S. 117.
755 *Dies.*, Die Evolution der Kooperation, 1991, S. 32.
756 *Dies.*, Die Evolution der Kooperation, 1991, S. 43, 123 f.

gie in der Gemeinschaft aus *TIT for TAT*-Spielern robust, da *TIT for TAT* in seiner Gesamtleistung eindrucksvoll wiederum *TIT for TAT* fördere und gegenüber defektivem Verhalten eine Sperrwirkung entfalte.[757] Denn nicht *TIT for TAT*-Spieler würden unmittelbar sanktioniert werden, hätten aber gleichzeitig die Chance, schnell die herrschende *TIT for TAT*-Strategie aufgrund der damit verbundenen Belohnung mit kooperativem Verhalten zu verstehen, und sich dem anzupassen.[758] So konnte festgestellt werden, dass in einer Kohorte mit 5 % *TIT for TAT*-Spielern sich diese Strategie ausweite.[759] Gegen dieses Phänomen der *TIT for TAT*-Strategie lasse sich auch nicht die bestehende Informationsasymmetrie anführen, da gerade in Anbetracht bestehender informatorischer Unsicherheiten die subjektiven Vorstellungen der Spieler und die Anknüpfung an den letzten Spielzug eine kooperative Strategieentscheidung begünstigen.[760] Folglich wird für die *TIT for TAT*-Strategie und ihre Wirkungen keine ausgeprägte Rationalität der Spieler nach dem *rational choice*-Ansatz vorausgesetzt. Damit erscheint sie als geeignet, um auf die Verhandlung von Bildern personaler Identitäten übertragen zu werden.

c) Bilder personaler Identitäten als Kooperationsgegenstand

Die *TIT for TAT*-Strategie in Kombination mit der Steigerung der Spieliteration wirkt sich begünstigend auf die kooperative Verhandlung von personalen Identitäten aus und fördert zugleich den Schutz des öffentlichen Gutes der persönlichen Informationen. Dabei geht es um die Verhandlung von dem dargestellten Bild der personalen Identität des Betroffenen gegenüber dem Bild der personalen Identität des Verantwortlichen. Diese Bilder stellen das sichtbare Ergebnis einer generierten personalen Identität infolge einer Datenverarbeitung dar. Unter Einbeziehung des Modells von *Ricœur*[761] handelt es sich um einen dialogischen Prozess, der von einem narrativen Bild der personalen Identität ausgeht und als Agent in den Empfangsbereich des Kommunikationspartners gelangt, damit das Bild der personalen Identität in einer nächsten Iteration verhandelbar wird. Übertragen auf die spieltheoretische Modellierung kann das narrative Bild

757 *Dies.*, Die Evolution der Kooperation, 1991, S. 19, 53.
758 *Dies.*, Die Evolution der Kooperation, 1991, S. 47.
759 *Dies.*, Die Evolution der Kooperation, 1991, S. 118.
760 *Rasmusen*, Games and information, 2009, S. 149, 152.
761 1. Teil, C., II., 2., b).

der personalen Identität beim Gegenspieler eine Defektion oder Kooperation auslösen. Die Defektion könnte aus einer Ablehnung des Bildes der personalen Identität oder in der Erwiderung mit einem verfälschten Bild der personalen Identität etwa als Profil bestehen. Demgegenüber würde die Kooperation aus einer realen Kontrollmöglichkeit des Bildes der personalen Identität bestehen.

Das Phänomen der Evolution des Bildes personaler Identitäten im online-Kontext soll in ein kooperationsförderndes aus mehreren Spieliterationen bestehendes Verhandlungsmodell überführt werden. Dafür bedarf es der Zerlegung des Spiels in weitere Spieliterationen. Mit dieser Zerlegung können die relationalen Querverbindungen und Interdependenzen der Spieler gesteigert[762] und die Diversität der Bilder personaler Identität im Rahmen der Kooperation gefördert werden. Die Zerlegung könnte damit erfolgen, dass das durch den Spieler empfangene Bild der personalen Identität und dem daraus begründeten Profil im kooperativen Sinne transparent gemacht wird, womit das informationelle Machtungleichgewicht modifizierbar wird. Mit dieser Informationsgrundlage würde der Spieler wiederum zwischen Defektion in Gestalt der Ablehnung des Bildes der personalen Identität und Kooperation in Gestalt der Annahme und Modifizierung des Bildes personaler Identitäten entscheiden können. Gleichwohl kann möglicherweise auf die vollständige Transparenz verzichtet werden, solange ein aus mehreren Iterationen bestehendes Verfahren eine stillschweigende Verhandlung, basierend auf den Vorstellungen der Spieler, ermöglicht. Auch damit kann es zu einer Steigerung der Kontrollmöglichkeit über das Bild der personalen Identität kommen und Fokalpunkte über die Bilder der personalen Identitäten erreicht werden. Folglich könnte darin ein Schutzmechanismus zugunsten der persönlichen Informationen liegen, wobei es nicht um den Schutz gegenüber alltäglichen fremden Identitätserwartungen geht, sondern um die Verhandelbarkeit des Bildes der personalen Identität und somit auch den verhandlungsfähigen persönlichen Informationen[763]. Es lässt sich darin eine Umstrukturierung und Neuausrichtung der Verhandlung in eine Verfahrenserweiterung erblicken,[764] die einen ungewissen Verfahrensausgang als Konsens in Gestalt eines Bildes der personalen Identität ermöglicht.

762 *Luhmann*, Legitimation durch Verfahren, 2017, S. 75; *Shapiro*, Negotiating the nonnegotiable, 2017, S. 127.
763 2. Teil, A., II., 1., d).
764 *Luhmann*, Legitimation durch Verfahren, 2017, S. 37–40, 50 f.

Diese Verfahrenserweiterung zu dem Bild der personalen Identitäten ist vergleichbar mit dem elektronischen Zustellungsverfahren, bei dem es um den Konsens über den Zugang eines Dokumentes geht. Denn mit einer amtlichen Abholbestätigung wird das Vertrauen über die Zustellung ausgelöst und gegen nichtkooperative Kommunikationspartner durchgesetzt, § 5a VwZG i.V.m. §§ 5, 17 De-Mail-G.[765] Folglich geht es bei der Übertragung der elektronischen Zustellung auf die Verhandlung der Bilder personaler Identitäten um die „Zustellung" des Bildes der personalen Identität von dem Betroffenen auch gegenüber einem nichtkooperativen Verantwortlichen. Ebenfalls wird ein iteratives Verfahren eingesetzt, mit dem eine Nachricht oder ein Bild der personalen Identität nicht nur in den Empfangsbereich gelangt, sondern auch die Kenntnisnahme fingiert wird.

In der Struktur sieht das De-Mail-G eine rechtssichere Kommunikation vor, die auf eine rechtssichere Verhandlung als „vermittelte Kommunikation"[766] über das Bild der personalen Identität übertragen werden soll. Inhaltlich geht es dabei um die Separierung und Angleichung von Attributen oder Profilen der personalen Identität, die iterativ verhandelt werden (vgl. Abbildung 4) und zu einer dynamischen Konstituierung des Bildes der personalen Identität und zu einer „Entsklavung von den algorithmusbasierten Erzeugnissen"[767] beitragen sollen. Eine derartige iterative und kooperative Verhandlung der Bilder personaler Identitäten stellt ein Verfahren für die Steigerung der Realisierungsmöglichkeiten der informationellen Selbstbestimmung dar und sollte in dem Identitätsverwaltungsmodell einbezogen werden.

765 *Roßnagel*, CR 2011, 23 (29).
766 *Steinmüller*, Information, Modell, Informationssystem, S. 5.
767 *Edwards/Veale*, Duke L. & Tech. Rev. 2017, 18 (84).

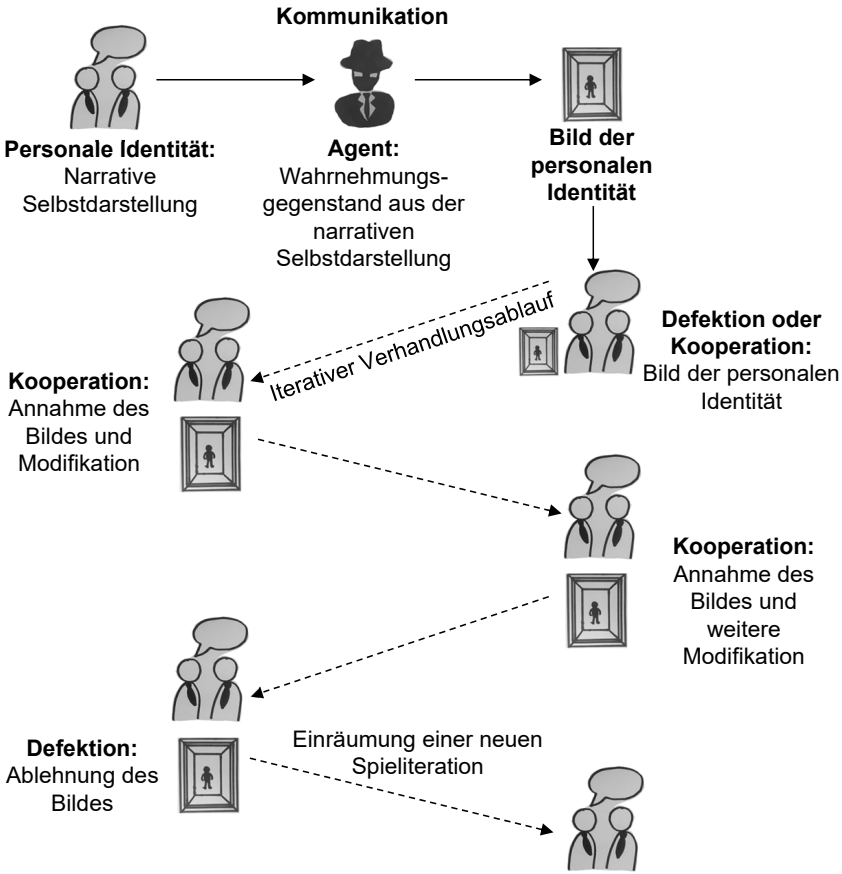

Abbildung 4: Iterative Verhandlung der Bilder personaler Identitäten

3. Bewertung

Die Verhandlung im IKT-Recht dient dem öffentlichen Gut der persönlichen Informationen optimal, wenn die Spieler miteinander kooperieren. Als kooperationsfördernd konnte die Steigerung der Iterationen des Spiels und der Einsatz der *TIT for TAT*-Strategie identifiziert werden. Auch wenn es sich jeweils um ein Spiel zwischen zwei Spielern handelt, hat die *TIT for TAT*-Strategie einen Ausstrahlungseffekt in der Kohorte von Spielern, die eine andere Strategie verfolgen. Gleichwohl ist kooperatives Strategieverhalten fragil, da die Interessen der Spieler über den Schutz des öffentlichen

Gutes der persönlichen Informationen variieren können, so dass es für den überwiegenden Einsatz der kooperativen Strategie der autoritären Gewährleistung mit einem Sanktions- und Anreizmechanismus bedarf.[768] Damit würde die Kooperation als vorzugswürdige Strategie gefördert werden. Ebenso ist eine autoritäre Intervention dahingehend möglich, dass die Macht eingeräumt wird, eine Nachricht in Gestalt eines Bildes der personalen Identität nicht zu empfangen. Denn das kooperative Verhandlungsmodell findet seine Grenzen darin, dass eine personale Identität in ihrem *Ipse*-Anteil nicht mehr verhandelbar ist und das Bild der Identität beibehalten wird. So ist etwa der *Idem*-Anteil einer personalen Identität im Personalausweis- und Meldewesen nicht verhandelbar und das Attribut der strafrechtlichen Schuld nach einer rechtskräftigen Verurteilung ist ebenfalls nicht verhandelbar.

Insoweit fungieren die Rechtsregeln zur Festlegung dieser Bilder der personalen Identität als Fokalpunkte, da mit diesen Rechtsregeln ein stabiler Punkt über die Bilder personaler Identitäten für beide Spieler erreicht wird. Demnach werden mit den Rechtsnormen die Interessen der Spieler über den Schutz der Bilder personaler Identitäten gesteuert und mit ihnen wird ein Interventionsmechanismus bei widerstreitenden Interessen der Spieler geschaffen. Ebenso können als Interventionsmechanismen auf der technischen Gestaltungsebene der „*layered approach*“[769], die Anonymität[770], die Privatheitseinstellungen[771] und ein *Dashboard-System* eingesetzt werden. Mit diesen Interventionsmechanismen erfährt der Betroffene eine Schutzmöglichkeit gegenüber dem Verantwortlichen und der bestehenden Informationsasymmetrie. Weiter könnte eine rechtliche Intervention darin liegen, einen Hinweis in den Informationspflichten über die Auswirkungen der Einwilligung gegenüber dem öffentlichen Gut der persönlichen Informationen aufzunehmen.[772] Damit würde eine Steigerung des Bewusstseins beim Betroffenen über die Risiken der Datenverarbeitung ermöglicht werden.

Insgesamt lässt sich das Konzept der Kooperation gemäß Art. 31 DSGVO als Makroebene des Datenschutzrechts auf die Mikroebene des

768 *Rasmusen*, Games and information, 2009, S. 173–185; *van Aaken*, in: Kirste (Hrsg.), Interdisziplinarität in den Rechtswissenschaften, 2016, 187 (193–196).
769 4. Teil, B., II., 3.
770 4. Teil, B., IV.
771 Diese sind ebenfalls mit Transaktionskosten für den Betroffenen verbunden, so dass ein umfassender Schutz damit zweifelhaft erscheint, vgl. *Hermstrüwer*, JIPITEC 2017, 9 (11) Rn. 9;
772 4. Teil, B., II., 4.

Schutzes der personalen Identität übertragen. Denn auf der Mikroebene würde mit einem kooperativen Verhandlungsverfahren dem *Ipse*-Anteil der personalen Identität entsprochen und ein eigenständiger Schutzmechanismus zur Verhandlung der Bilder personaler Identitäten begründet werden. Darin liegt ein Interventionsmechanismus gegen die Informationsasymmetrie und einen defektiven Strategieverlauf, indem mit der Iteratationssteigerung zugleich die Kooperation gefördert wird. Insoweit stellt sich die Frage nach einem rechtlichen Interventionsmechanismus zur Implementierung der Kooperation über die Bilder personaler Identitäten, so dass sich daraus der mögliche soziotechnische Regelungsbedarf ableiten lässt.

IV. Rechtliche Interventionsmechanismen

1. Einführung

Mit der Annahme konfligierender Interessenlagen bei der spieltheoretischen Modellierung geht es nun bei der rechtlichen Intervention um eine mögliche Förderung der Verhandlung. Für die gezielte Kooperationsförderung soll demnach die zweite Eskalationsstufe des Konfliktes als ein Anknüpfungspunkt herangezogen werden. Dabei geht es darum, das Vorliegen eines Interessenkonfliktes anzuerkennen und eine „*win-lose*"-Lösung zu umgehen. Dies könnte mit einem sanktionsbewehrten Anreiz durch eine Rechtsregel als Interventionsmechanismus erfolgen. Voraussetzung dafür ist eine nähere Analyse der bestehenden Informationsasymmetrie zwischen den Spielern (2.) und die exemplarische Einbeziehung der wettbewerbsrechtlichen Interventionsmechanismen (3.). Schließlich soll die Intervention in den Interessenkonflikt mit einem Verfahren dargestellt werden (4.) und abschließend die Interventionsmechanismen insgesamt bewertet werden (5.).

2. Intervention in die Informationsasymmtrie

Die Intervention in die bestehende Informationsasymmetrie der Spieler verlangt, dass die Wirkungen der Informationsasymmetrie über die beteiligten Spieler hinaus analysiert werden. Dabei könnte sich ein „*Market for Lemons*"[773] über datenverarbeitende Dienste etabliert haben (a), bei dem

773 *Akerlof*, The Quarterly Journal of Economics 1970, 488.

sich in besonderem Maße die Frage nach der Kompensation durch eine erweiterte Transparenz stellt (b).

a) Datenschutzrechtlicher „*Market for Lemons*"

Im IKT-Recht konnte über den Datenzyklus hinaus die Informationsasymmetrie zwischen Verantwortlichem und Betroffenen nachgewiesen werden, die in den Phasen des Datenzyklus jeweils eine rechtliche Kompensation erfährt.[774] Dies führt nicht zu einer gleichen Informationsverteilung und damit zur Aufhebung der Informationsasymmetrie, sondern es liegt vielmehr eine punktuelle kompensatorische Wirkung vor. Dies betrifft zunächst das individuelle Verhalten des Betroffenen etwa mit der Einwilligungserteilung und den Betroffenenrechten. Gleichwohl konnte nachgewiesen werden, dass das Verhalten anderer Betroffener sich auf das individuelle Verhalten auswirkt, wenn sich der Betroffene etwa an dem Mehrheitsverhalten bei der Verwendung sozialer Medien orientiert. In diesen Netzwerkeffekten liegt ein Phänomen, was sich möglicherweise in den Marktmechanismen niederschlägt und sich darüber hinaus auf die datenschutzrechtliche Qualität der Dienste auswirkt.

Entscheidende Ausgangssituation ist dabei die Wahl der technischen und organisatorischen Maßnahmen und die Risikobewertung durch einen defektiv handelnden Verantwortlichen, der die Informationen über einen angebotenen Dienst mit einem geringen Schutzniveau nicht veröffentlicht. Der Betroffene muss demnach auf den öffentlich bekannten Informationsstand über den Verantwortlichen vertrauen und unterliegt einer informatorischen Unsicherheit, was die datenschutzrechtliche Qualität des Dienstes angeht. Gleichwohl ist bei der Datenverarbeitung und der Generierung von Bildern personaler Identitäten ein Verstoß gegen den Stand der Technik oder den Informationspflichten möglich, was sich aber typischerweise erst zu einem späteren Zeitpunkt des Datenzyklus herausstellen wird. Somit können sich Dienste mit verbraucherfreundlichen Informationen, aber mit einem nachteiligen Schutz der persönlichen Informationen im Rahmen des Standes der Technik etablieren. Die zeitliche Verzögerung der Auswirkungen und des Bekanntwerdens von Diensten mit einem unzureichenden Schutzniveau erlaubt es, dass sich diese Dienste mit einem günstigen Preisniveau etablieren. Dieses entspricht dem von *Akerlof* verwendeten Beispiel über den Gebrauchtwagenhandel, in dem ein Markt

774 Vgl. *Zander/Steinbrück/Birnstill*, JIPITEC 2019, 200.

von „bitteren Zitronen“ (Gebrauchtwagen in einem schlechten Zustand) in Gestalt von Diensten mit einem geringen Schutz der persönlichen Informationen entstehen können.[775] Dieser könne sich ebenso auf die Qualität der Datenschutzerklärungen auswirken und die Verwendung klauselartiger Formulierungen begünstigen, was sogar zum Geschäftsmodell der Intermediäre gehören könnte.[776] Weiter lässt sich mit diesem Marktmechanismus feststellen, dass die unehrlichen defektiven Strategien die ehrlichen kooperativen Strategien verdrängen.[777] Zwar ließe sich dem entgegenhalten, dass die „unsichtbare Hand“ des Marktes langfristig für einen Ausgleich sorgen könne, jedoch mangele es bei faktischen Monopolstellungen von Intermediären an echten Wahlmöglichkeiten für den Betroffenen[778] und das Recht auf Datenübertragbarkeit vermag noch keinen angemessenen Ausgleich herstellen.

In Anbetracht der Tatsache, dass bei der Identitätsverwaltung nicht der Gebrauchtwagenhandel, sondern das Primärrechtsgut der persönlichen Informationen als Schutzgegenstand betroffen ist, führt dieser Marktmechanismus zu einem unbefriedigenden Zustand für den Schutz der personalen Identitäten. Folglich sind rechtliche Interventionen in einen datenschutzrechtlichen „*Market for Lemons*“ wünschenswert, da das öffentliche Gut der persönlichen Informationen betroffen ist und im Zusammenhang mit Marktmechanismen steht.

b) Erweiterte Transparenz

Weil für den beschriebenen Marktmechanismus die Informationsasymmetrie ausschlaggebend ist, kann die Intervention in der Wiederherstellung der Informationssymmetrie durch eine Erweiterung der Transparenz erfolgen. Diese könnte in der Ausdehnung der Informationspflichten und der Verbesserung der Informationsdarstellung liegen oder in vertrauensbildenden Maßnahmen etwa durch Garantien und Zertifizierungen gemäß Art. 42, 46 DSGVO. Damit würde die *Selbstbindung* des defektiven oder ko-

775 *Akerlof*, The Quarterly Journal of Economics 1970, 488 (489 f.).
776 *Becker*, JZ 2017, 170 (174); *Di Fabio*, Grundrechtsgeltung in digitalen Systemen, 2016, S. 15, 35–37.
777 *Akerlof*, The Quarterly Journal of Economics 1970, 488 (495).
778 *Becker*, JZ 2017, 170 (174 f.).

operativen Verantwortlichen ausgeweitet werden, welche mit unmittelbaren Sanktionen etwa des Publizitätsschadens verbunden sein könnte.[779]

In spieltheoretischer Hinsicht hat die *informationelle Selbstbindung* in Gestalt der Reputation in wiederholenden Spielen eine stabilisierende und kooperationsfördernde Wirkung, da das Vertrauen für eine ebenfalls kooperationsfördernde Strategieentscheidung geschaffen und die positive Reputation für die Zukunft gesteigert wird.[780] Die positive Reputation könne erweitert werden, wenn über Garantien und Zertifikate hinaus die zur Rechenschaftsdokumentation gemäß Art. 5 Abs. 2 DSGVO gehörenden Risikobewertungsmaterialien etwa als „Beipackzettel"[781] veröffentlicht und eine sog. „Transparenzschnittstelle"[782] für die Verständlichkeit der Wirkmechanismen von Algorithmen eingeräumt werden. Ebenso wird zur Transparenzerweiterung ein „*comply & explain*" Konzept, wie es das Kapitalmarktrecht in § 161 AktG vorsieht, vorgeschlagen.[783] Damit müsse zunächst die Rechtmäßigkeit im Rahmen der freiwilligen Veröffentlichung transparent gemacht werden und diese könnte anschließend einer weiteren Begründungspflicht unterliegen. Dies setzt voraus, dass gerade marktbeherrschende Intermediäre ein Interesse an ihrer Reputation dahingehend haben, dass Einblicke in ihre dokumentierten technischen und organisatorischen Maßnahmen zum Schutz der personalen Identitäten gewährt werden. Jedoch widerspricht diese Variante dem wirtschaftlichen Bedürfnis nach Wahrung der Geschäftsgeheimnisse und dem praktischen Bedürfnis, mit einer positiven Reputation eine hohe Nutzerzahl zu generieren.

Insgesamt könne der Interventionsmechanismus mit einer Transparenzerweiterung im Rahmen der Publizität als „*disclosure*" verstanden werden und sich auf der Makroebene auswirken.[784] Daher erscheint neben der Transparenzerweiterung zwischen Verantwortlichem und Betroffenen die Realisierung einer sog. Strukturtransparenz[785] im Markt über die persönlichen Informationen notwendig. Damit wären wettbewerbsrechtliche Interventionen erforderlich, mit denen eine Entflechtung marktbeherrschen-

779 *Faber/Sedlacek*, DuD 2017, 440 (445); auf die Selbstbindung mit Garantien abstellend, *Akerlof*, The Quarterly Journal of Economics 1970, 488 (499 f.).
780 *Faber/Sedlacek*, DuD 2017, 440 (444 f.).
781 *Bieker/Hansen/Friedewald*, RDV 2016, 188 (196 f.); 4. Teil, B., II., 1.
782 *Gigerenzer/Müller/Wagner*, FAZ vom 22.06.2018, 15.
783 *Klaes*, MMR 2015, 299 (301).
784 *Damler*, Rechtsästhetik, 2016, S. 312 f.
785 *Ders.*, Rechtsästhetik, 2016, S. 307.

der Strukturen erfolgen würde, um zu einer Durchsichtigkeit der Marktstrukturen beizutragen.[786]

3. Intervention durch das Wettbewerbsrecht

Die Intervention in eine von marktbeherrschenden Spielern bestehende Struktur kann mit dem Wettbewerbsrecht erfolgen, damit verfestigte Strukturen im Markt unter der Prämisse eines fairen Wettbewerbs gestört werden. Dazu gehören die kartellrechtliche Intervention wegen des Missbrauchs der marktbeherrschenden Stellung, der Schutz vor unlauterem Wettbewerb und die Intervention durch datenschutzrechtliche Anforderungen im Vergaberecht. Diese Interventionsformen sollen übersichtsartig dargestellt und auf ihre Übertragbarkeit hin zur rechtlichen Förderung eines kooperativen Identitätsverwaltungsmodells untersucht werden.

In struktureller Hinsicht hat das Bundeskartellamt den Missbrauch der marktbeherrschenden Stellung gemäß § 19 Abs. 2 Nr. 4 GWB von *Facebook* in einer Entscheidung am 15.02.2019 festgestellt.[787] Das zur marktbeherrschenden Stellung beitragende Geschäftsmodell des Datensammelns und der Zusammenführung von Datensätzen mit „*Whats App*"-Daten, sowie das Zusammenführen von Datensätzen mit der Funktionsschaltfläche „Gefällt Mir" wurde als missbräuchlich bewertet. Neben den Aktivitäten, die durch die ursprüngliche Einwilligung ausgelöst wurden, würden die Sekundäraktivitäten der Datenzusammenführung von Metadaten ein eigenes Risiko für den Schutz der informationellen Selbstbestimmung bilden. Hervorzuheben an den Ausführungen des Bundeskartellamtes ist, dass keine Kompensation mit den Betroffenenrechten angenommen wurde, so dass darin eine Anerkennung dominierender Marktmechanismen gegenüber den Betroffenenrechten liegt. Vielmehr befand das Bundeskartellamt die Erforderlichkeit einer „Art innere(n) Entflechtung der Daten", weil die Zusammenführung der Daten durch eine faktische Zwangssituation beim Betroffenen ausgelöst werde und der Betroffene keine echte Wahlmöglichkeit bei der Erteilung der Einwilligung habe.

Gleichwohl wurde diese Entscheidung des Bundeskartellamtes im Rahmen des einstweiligen Rechtsschutzes von dem OLG Düsseldorf als rechtswidrig eingeordnet, da insgesamt keine wettbewerbsrechtliche Fehlent-

786 *Ders.*, Rechtsästhetik, 2016, S. 318 f.; *Nissenbaum*, Wash. L. Rev. 2004, 119 (130).
787 *Bundeskartellamt*, Fallbericht vom 15.02.2019, Az.: B6-22/16.

wicklung oder ein Wettbewerbsschaden festzustellen sei.[788] Dabei wurden Unklarheiten in der Entscheidungsbegründung des Bundeskartellamtes hinsichtlich der zusammengeführten Datenarten und des Datenumfangs hervorgehoben, die für die Begründung eines Marktmissbrauchs jedoch Voraussetzung seien. Zudem wurde die Einwilligung der Nutzer als ausreichende Kontrollmöglichkeit über die personenbezogenen Daten angesehen und die fehlende Kausalität zwischen datenschutzrechtlichen Verstößen und Missbrauch der marktbeherrschenden Stellung im Wettbewerb betont. Mit dem Beschluss vom 23. Juni 2020 hat der Bundesgerichtshof die Entscheidung des OLG-Düsseldorf aufgehoben, so dass das Verbot der Zusammenführung von Daten durch das Bundeskartellamt vorläufig durchgesetzt werden darf.[789]

An diesen Entscheidungen werden die Chancen des Kartellrechts deutlich, dass das Marktverhalten und die Marktmacht der Intermediäre begrenzt werden könne, so dass sich kartellrechtliche Maßnahmen auch auf die Reputation der Intermediäre auswirken.[790] Dahingehend wirkt die Entscheidung des Bundeskartellamtes als eine sachgerechte Anerkennung von wirtschaftlichen Wirkmechanismen im Datenschutzrecht. Diese rechtliche Verbindung wurde jedoch mit dem Beschluss des OLG Düsseldorf zunächst deutlich eingeschränkt. Gleichzeitig bleibt abzuwarten, wie in der Hauptsache nach dem Beschluss des Bundesgerichtshofes das OLG-Düsseldorf entscheiden wird.

Jedenfalls kann sich die Aufforderung im OLG-Beschluss zur Differenzierung des Nachweises der Kausalität zwischen marktbeherrschender Stellung und deren Missbrauch durch Intermediäre auf die Hauptsacheentscheidung auswirken. Diese Differenzierung könnte die exogenen Entscheidungsfaktoren[791] bei der Einwilligungserteilung einbeziehen, die kausal sein können für eine langfristige marktbeherrschende Stellung. Weiter könnte sich eine bestehende marktbeherrschende Stellung auf die Zweckänderungsmöglichkeiten im Laufe des Datenzyklus gemäß Art. 6 Abs. 4 DSGVO auswirken und einen Missbrauch dieser begünstigen, indem Datenverarbeitungen erheblich erweitert und verlängert werden. Ebenso können sich der Zugang auf wettbewerbsrelevante Daten und die Gewährleistung der Interoperabilität auf das Entstehen der marktbeherrschenden

788 OLG Düsseldorf, Beschluss v. 26.08.2019, Az.: VI-Kart 1/19 (V).
789 BGH, Beschluss v. 23.06.2020 – KVR 69/19.
790 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 33 f.; *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 77.
791 4. Teil, C., II., 1., c).

Stellung auswirken, wie es in dem Referentenentwurf zu § 19 a GWB geregelt wurde.[792] Demnach lässt sich die Ansicht vertreten, dass mit einer fachübergreifenden Argumentationslinie möglicherweise die Kausalität zwischen Marktbeherrschung und Missbrauch nachweisbar wird.

Ferner kommt als Interventionsmöglichkeit die Abmahnung des Marktverhaltens der Spieler wegen eines Verstoßes gegen die Informationspflichten gemäß Art. 12, 13 DSGVO und des Einwilligungserfordernisses gemäß Art. 6, 7 DSGVO in Betracht. So wurde vereinzelt etwa ein unlauterer Wettbewerb angenommen, wenn die Datenverarbeitung ohne Einwilligungserteilung oder ohne Datenschutzerklärung vorgenommen wurde.[793] Weiter sieht ein Referentenentwurf des Bundesministeriums der Justiz[794] den Aufwendungsersatz für Abmahnungen bei Verstößen gegen die DSGVO und das BDSG gemäß § 13 Abs. 4 UWG-E vor. Gegen einen derartigen Entwurf wird jedoch angeführt, dass bereits abschließende Regelungen für Rechtsbehelfe gegen Datenschutzverstöße gemäß Art. 77 ff. DSGVO bestünden.[795] Entsprechend sieht Art. 80 Abs. 1 DSGVO die Einschaltung eines Verbandes vor und gemäß Art. 58 DSGVO bestehen umfassende Abhilfebefugnisse der Aufsichtsbehörden, die einen ausreichenden Schutzmechanismus begründen. Zudem erscheint die Wirkung einer Abmahnmöglichkeit gegen Datenschutzverstöße auf die bestehenden Marktstrukturen fraglich. Denn eine negative Reputation des Verantwortlichen ist infolge der Abmahnung und der geltendgemachten Rechtsbehelfe gemäß Art. 77 ff. DSGVO ebenso möglich. Demnach würde ein datenschutzrechtliches Abmahnrecht kaum als eigenständiger Interventionsmechanismus gegenüber den Marktstrukturen wirken, sondern in seinen Wirkungen den Rechtsbehelfen aus der DSGVO gleichrangig sein.

Schließlich kommen als wettbewerbsrechtlicher Interventionsmechanismus vergaberechtliche Anforderungen bei der öffentlichen Ausschreibung von IT-Dienstleistungen und IT-Produkten in Betracht. Dabei ist die Einhaltung der Grundsätze des Datenschutzes durch Technik und die Realisierung datenschutzfreundlicher Voreinstellungen ausdrücklich als eine Anforderung bei öffentlichen Ausschreibungen vorgesehen, EWG 78 S. 5. Auch sieht § 128 Abs. 2 S. 3 GWB vor, dass öffentliche Auftraggeber beson-

792 Referentenentwurf, GWB-Digitalisierungsgesetz, S. 9 f.
793 LG Hamburg, Urt. v. 02.03.2017 – Az.: 327 O 148/16; LG Würzburg, Beschluss v. 13.09.2018 – Az.: 11 O 1741/18 UWG.
794 *Bundesministeriums der Justiz und für Verbraucherschutz*, Referentenentwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs.
795 *Köhler*, ZD 2019, 285 f.

dere Ausführungsbedingungen zum „Schutz der Vertraulichkeit von Informationen" verlangen können, was neben den Geschäftsgeheimnissen auch personenbezogene Daten betrifft. Diese Regelung ist auf die „Snowden"-Affäre und dem darauf folgenden „No-Spy"-Erlass von 2014[796] des Bundesinnenministeriums zurückzuführen, wonach eine Zuverlässigkeitserklärung darüber abgegeben werden sollte, dass im Ausland gespeicherte Informationen nicht an ausländische Behörden weitergegeben werden sollen.[797] Darin liegt nicht nur eine rechtliche Verpflichtungserklärung, sondern auch der Bedarf an einer technischen Umsetzung der Vertraulichkeitsanforderungen. Folglich wird im Rahmen der öffentlichen Ausschreibung der Anreiz gesetzt, frühzeitig technische und organisatorische Maßnahmen zur Implementierung der Datensicherung und Datensparsamkeit zu treffen. Diese können bereits in der Entwicklung von Diensten und Produkten einbezogen werden und somit zum Bestandteil der Geschäftsstrategie werden.

Insgesamt wird mit diesen wettbewerbsrechtlichen Interventionsmechanismen in das Marktverhalten korrigierend eingegriffen und ein Anreiz für die Marktteilnehmer geschaffen, die datenschutzrechtlichen Maßgaben umfassend und frühzeitig zu implementieren. Für die Identitätsverwaltung, die sich als datenschutzrechtliches Erfordernis auf der Mikroebene darstellt, wirken sich die wettbewerbsrechtlichen Interventionsmechanismen nur indirekt aus. Diese können zu einem Anreiz für datenschutzfreundliche Produkte und Dienste mit einem „*identity management by design*" führen. Folglich könnte das Reputationsinteresse der Verantwortlichen über ein datenschutzkonformes Marktverhalten zu einem intensiveren Wettbewerb über datenschutzfördernde Dienste führen und die Sensibilität der Nutzer steigern. Gleichwohl wirken sich wettbewerbsrechtliche Interventionen verzögert auf das Verhalten einzelner Spieler aus. Insoweit können die wettbewerbsrechtlichen Interventionsmechanismen über einen längeren Zeitraum den Schutz über das öffentliche Gut der persönlichen Informationen entfalten, wenn wirksame Anreize für die technischen und organisatorischen Maßnahmen und ein kooperatives Identitätsverwaltungsmodell gesetzt werden. Im Rahmen der Technikgestaltung sollte sich das „*identity management by design*" implementieren lassen und in der konkreten Ausgestaltungsform aus mehreren Iterationen bestehen, damit die personale Identität in ihrem *Ipse*-Anteil abgebildet werden kann.

---

796 *Bundesministerium des Innern*, No-Spy-Erlass, 2014.

797 *Fehling*, in: Pünder/Schellenberg (Hrsg.), Vergaberecht, 2019, § 128 GWB Rn. 43; *Gabriel/Bärenbrinker*, VergabeR, 166.

4. Intervention durch Verfahren

Das IKT-Recht ist von einer Verfahrensdimension geprägt, die *ex ante* zur Rechtfertigung in der Risikobewertung und Bestimmung des geeigneten Rechtfertigungsgrundes, auf der Rechtfertigungsebene in dem Einwilligungs*verfahren* selbst und *ex post* zur Rechtfertigung in den Betroffenenrechten erkennbar ist. Weitergehend sind diese Betroffenenrechte als verfahrensmäßige Gewährleistung des Datenschutzes grundrechtlich in Art. 8 Abs. 2 GRC verankert, worin eine staatliche Schutzpflicht auf verfahrensmäßige Grundrechtsgewährleistung gesehen wird.[798] Auch aus dem Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht im Volkszählungsurteil den verfahrensrechtlichen Schutz hervorgehoben, indem gesteigerte organisatorische und verfahrensrechtliche Vorkehrungen für einen wirksamen Schutz verlangt wurden.[799]

Indem die Struktur eines Verfahrens einen übergeordneten Rahmen als Metakommunikation für die Förderung einer Entscheidung ermöglicht, lässt sich das *Verfahren als Intervention* zum Schutz der Bilder personaler Identitäten einsetzen. Denn mit dem Verfahren könne die Entscheidungsfindung in ihrer Richtigkeit kanalisiert und unterstützt werden,[800] so dass darin eine Schutzmöglichkeit gegenüber Verzerrungen der Bilder einer personalen Identität liegt. Gleichzeitig wird mit dem modellierten Verfahren eine Komplexitätsreduktion gewährleistet,[801] mit der sich die potentiell relevanten Daten für das Bild der personalen Identität im Hinblick auf den intendierten Erkenntnisgehalt reduzieren lässt. Entsprechend steht ein Verfahren für das Bild der personalen Identität und schließlich für die Identitätsverwaltung an sich im Gleichlauf zu dem dynamischen Identitätsbegriff in seinem *Ipse*-Anteil. Dieses wurde bereits in einem iterativen Verfahren zur Kooperation über die Bilder personaler Identitäten dargestellt und setzt die Anforderungen an den Begriff der personalen Identität um. Darin liegt eine Verlagerung der Entstehung des Bildes der personalen Identität in ein Verfahren, welches in das Identitätsverwaltungsmodell zu

798 *Knecht*, in: Schwarze/Becker/Hatje u.a. (Hrsg.), EU-Kommentar, 2019, Art. 8 GRC Rn. 10; *DeHert/Gutwirth*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 61 (78).

799 BVerfGE 65, 1 (44, 49).

800 *Luhmann*, Legitimation durch Verfahren, 2017, S. 12 f., 22; *Zippelius*, Das Wesen des Rechts, 2012, S. 117.

801 *Ders.*, Legitimation durch Verfahren, 2017, S. 42–44; *Reisinger*, Rechtsinformatik, 2016, S. 70.

integrieren ist. Damit soll sich der Betrachtungsschwerpunkt hin zu einem prozedural geprägten Identitätsverwaltungsmodell verschieben.

5. Bewertung

Die Interventionsmechanismen zur Förderung des öffentlichen Gutes der persönlichen Informationen dienen der Kompensation des Interessenkonfliktes zwischen Verantwortlichem und Betroffenen. Dabei erscheint eine Intervention mit einer erweiterten Transparenz möglich, die in einer strukturellen Transparenz bestehen könnte. Dieser strukturellen Transparenz dienen die wettbewerbsrechtlichen Interventionsformen, mit denen kartellrechtlich in das Marktverhalten der Verantwortlichen eingegriffen wird, um Anreize für die Realisierung datenschutzrechtlicher und technischer Gestaltungsmechanismen zu schaffen. Damit lässt sich das Verhandlungsungleichgewicht und die bestehende Informationsasymmetrie stören, so dass die bestehende „*win-lose*"-Konstellation zu Lasten des Betroffenen gemindert werden könnte. Zusätzlich würde die Förderung des kooperativen Strategieverhaltens mit einem Verfahren, welches komplexitätsreduzierend bei der Bildung personaler Identitäten eingesetzt wird, für das öffentliche Gut der persönlichen Informationen schonend wirken. Dies würde zugleich dem dynamischen Identitätsbegriff in seinem *Ipse*-Anteil und der Anforderung einer hohen Iterationszahl Rechnung tragen. Ein derartiges prozedurales Identitätsverwaltungsmodell könnte über wettbewerbsrechtliche und datenschutzrechtliche Anreize implementiert werden, damit marktstarke Verantwortliche einem sanktionsbewehrten Anreiz zur Umsetzung von „*identity management by design*"-Maßnahmen unterliegen.

V. Ergebnis

Das spieltheoretische Modell im IKT-Recht ist von einer konfligierenden Interessenlage zwischen dem Verantwortlichen und Betroffenen geprägt. Dabei wirken sich auf die spieltheoretische Modellierung die Informationsasymmetrie und die Interdependenz der rationalen Strategieentscheidung in den sich wiederholenden Spieliterationen aus. Zwischen der defektiven und kooperativen Strategiewahl erweist sich das von Kooperation dominierte Spiel als schonend für das öffentliche Gut der persönlichen Informationen. Wenn es um den Schutz der Bilder personaler Identitäten geht, scheint die kooperative Verhandlung vorzugswürdig und könnte mit

einer Intervention gefördert werden. Dabei erscheint die kooperationsfördernde *TIT for TAT*-Strategie als wirksam und resistent gegenüber störenden gegenläufigen Strategien, so dass die Verhandlung des Bildes der personalen Identität mit der *TIT for TAT*-Strategie ein hohes Schutzniveau über das öffentliche Gut der persönlichen Informationen gewährt und sich als eine sog. „*win-win-win*"-Lösung einordnen lässt. Diese besteht aus dem Gewinn einer gesteigerten Kontrolle des Betroffenen über die Bilder der personalen Identität und dem Gewinn der technischen und organisatorischen Maßnahmen mit einem „*privacy by design*"-Konzept des Verantwortlichen, was sich positiv auf die Reputation im Markt auswirkt. Darüber hinaus würden sich diese kooperativen Strategien des Betroffenen und Verantwortlichen schonend auf das öffentliche Gut der persönlichen Informationen als weiteren Gewinn auswirken, zumal sich das beschriebene Strategieverhalten auf eine Vielzahl von Spielern übertragen lässt und diese sich dann ebenfalls kooperativ verhalten.

Daneben lässt sich die Kooperation mit einer Intervention von außen fördern. Dies kann mit der Erweiterung der Transparenz als Strukturtransparenz, durch Anreize aus dem Wettbewerbsrecht und der Implementierung eines Verfahrens erfolgen. Mit einem Verfahren würde das Bild der personalen Identität dynamisch kontrolliert werden können. Demnach sollte das Verfahren zum Bestandteil des Identitätsverwaltungsmodells werden. Ein solches übergeordnetes Metaverfahren könnte als Anforderung an ein „*identity management by design*"-Konzept gemäß Art. 25 DSGVO implementiert werden.

Insgesamt lässt sich gegen die spieltheoretische Modellierung anführen, dass die Annahme der ausschließlich rationalen Entscheidung als Reduzierung individueller Erwägungen auf ein ökonomisch motiviertes Kalkül fragwürdig sei. Denn auch die Spieltheorie stelle ein theoretisches Modell dar, das nicht mit der Wirklichkeit verwechselt werden dürfe und mit der Annahme, dass Entscheidungen allein auf Auszahlungs- und Sanktionsinteressen zurückzuführen sind, sehr beschränkt sei. Weiter würden sich die in der Spieltheorie gebildeten *Nash*-Gleichgewichte nicht an der Gerechtigkeit orientieren, sondern stellten allein ein berechnetes wertungsfreies Gleichgewicht dar.[802]

802 *Schirrmacher*, Ego, 2013, S. 66, 68; *Rubinstein*, Economic fables, 2012, S. 137. Ebenso führt *Hoffmann-Riem* das Beispiel der Finanzkrise an, welche in ihren ursächlichen wirtschaftlichen Ausprägungen etwa auf dem Immobilienmarkt der Gegenstand eines rationalen Kalküls mit unbeherrschbaren Risikoketten sei und zu einem „Ritt in die Ungewissheit" führe, *Hoffmann-Riem*, in: Augsberg

Gleichwohl soll für die Begründung eines Identitätsverwaltungsmodells die spieltheoretische Modellierung als Grundlage dienen und für die Bestimmung eines „*mechanism by design*“[803] nutzbar gemacht werden. Für ein solches „*mechanism by design*“ könnte eine Differenzierung der Verfahrensschritte erfolgen, indem ein Spielraum für die Reflektionsmöglichkeit durch die Iterationssteigerungen eingeräumt wird und als Grundlage für die Kooperationsförderung dient. Insoweit kommt ein Verfahren als spieltheoretisch begründetes Lösungsmodell mit der Erweiterung um einen Mediationsagenten in Betracht.

C. Mediationsagent als Lösungsmodell

Mit einem übergeordneten Verfahren kann das beschriebene spieltheoretische Modell mit der kooperativen Strategieentscheidung gefördert werden. Dafür kann das Mediationsverfahren die Grundlage für einen sog. „*meta-frame*“[804] bilden, in dem ein Anreiz für eine *TIT for TAT*-Strategie gesetzt wird und für die persönlichen Informationen schonende Spieliterationen erfolgen. Mit den Verfahrensprinzipien der Mediation und dem Mediator als dritten Spieler könnte dieser Anreiz zur Kooperation[805] und Förderung von pluralen Bildern personaler Identitäten gesetzt werden.

Die Mediation wird gemeinhin als ein aus dem angloamerikanischen Rechtskreis stammendes Verfahren eingeordnet, welches zu einem Ausweg aus den langandauernden und kostspieligen Gerichtsverfahren führen sollte und auf den Vortrag von Frank Sander 1978 mit dem Titel „*Varieties of Dispute Processing*“ zurückzuführen ist.[806] Die Adaption der Mediation im Prozessrecht erscheint deswegen strukturell zunächst wesensfremd, weil der Rechtsstreit auf die richterliche Beurteilung der Rechtspositionen

---

(Hrsg.), Ungewissheit als Chance, 2009, 17 (19); von einem prosozialen und kooperativen Menschenbild ausgehend, vgl. *Glöckner*, in: Funke/Schmolke (Hrsg.), Menschenbilder im Recht, 2019, 79 (84 f.).

803 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 226.

804 *Winheller*, ZKM 2018, 116.

805 *Haft*, in: Haft/Schlieffen (Hrsg.), Handbuch Mediation, 2016, § 3 Rn. 15; *Elsenbast*, ZKM 2016, 9 (10 f.).

806 *Ders.*, in: Haft/Schlieffen (Hrsg.), Handbuch Mediation, 2016, § 3 Rn. 13 f. Denn unter der Prämisse „*Justice delayed is justice denied*“ bestünde aus rechtsstaatlichen Gründen der Bedarf nach effektiven alternativen Streitbeilegungsmethoden, *Barnett/Treleaven*, The Computer Journal 2017, 399 f.

ausgerichtet ist und einem Nullsummenspiel gleicht.[807] Demgegenüber zielt die Mediation auf die Einbeziehung der Interessenlagen ab, so dass sie kooperationsfördernd wirken soll. Dies wird über ein Verfahren realisiert, in dem die Autonomie über den Verfahrensverlauf weitgehend an die Parteien zurückgegeben wird und eine Lösung in einem kontrollierten Kommunikationsprozess außerhalb des Rechts gefunden werden soll. Damit könne unter Schaffung eines entsprechenden Kommunikationsrahmens und Beseitigung von Einigungshindernissen eine Einigung im „Schatten des Rechts"[808] erzielt werden. Voraussetzung bleibt dabei, dass die Parteien – vergleichbar zu diplomatischen Beziehungen – ein Interesse an einer nachhaltigen Verhandlung haben.[809] Demnach soll nach einer Einführung in die Mediation im IKT-Recht (I.) die Verhandlung in der Mediation mit den Verfahrensprinzipien ausgeführt werden (II.), um daran anknüpfend einen Mediator als technischen Agenten zu begründen (III.). In diesem verfahrensrechtlichen Rahmen könnte die Verhandlung der Bilder personaler Identitäten erfolgen (IV.) und als Grundlage für ein mediatives Identitätsverwaltungsmodell (V.) fungieren.

I. Mediation im IKT-Recht

Die Mediation als Ausprägung der alternativen Streitbeilegungsmethoden wird im IKT-Recht benannt und ist darüber hinaus immanent in den Rechtsnormen des IKT-Rechts erkennbar. Gemäß § 124 TKG kann die Bundesnetzagentur den Parteien zur Beilegung telekommunikationsrechtlicher Streitigkeiten ein Mediationsverfahren vorschlagen und gemäß § 47a Abs. 1 TKG kann auf Antrag ein Schlichtungsverfahren eingeleitet werden. Weiter sieht Art. 12 Abs. 4 f) eIDAS-VO vor, dass der Interoperabilitätsrahmen für die Identifizierungen auch Regeln zur Streitbeilegung enthalten soll. Im Datenschutzrecht enthält Art. 31 DSGVO das Kooperationsgebot zwischen dem Verantwortlichen und der Aufsichtsbehörde und erlaubt einen sukzessiven Informationsaustausch. Indem die Aufsichtsbehörden einerseits über investigative Kompetenzen gemäß Art. 58 DSGVO verfügen, andererseits aber auch eine gestaltende Rolle bei datenschutzrechtlichen

807 *Ders.*, in: Haft/Schlieffen (Hrsg.), Handbuch Mediation, 2016, § 3 Rn. 18 f.

808 Das Konzept des „*Bargaining in the Shadow of the Law*" wurde von *Mnookin/Kornhauser* für emotionalisierte Scheidungskonflikte mit einer Hinwendung zur Mediation begründet, *Mnookin/Kornhauser*, Yale L. J. 1978, 950.

809 *Elsenbast*, ZKM 2016, 9.

Aufklärungs- und Beratungsmaßnahmen gemäß Art. 57 Abs. 1 DSGVO haben, wird ihnen eine mediierende Kompetenz zugesprochen.[810] Demnach ist das Konzept der alternativen Streitbeilegung mit dem Mediationsverfahren für den Konfliktfall dem IKT-Recht nicht fremd und kann als rechtliche Verankerung für ein zu begründendes Modell zum Schutz der Bilder personaler Identitäten eingesetzt werden. Entsprechend wurde von *Nissenbaum* ein Verfahren zum Ausgleich der bestehenden Asymmetrie zum Schutz der *kontextuellen Integrität* vorgeschlagen.[811]

II. Verhandlung mit Mediation

Mit der Mediation erfährt die Kommunikation der Parteien in der Verhandlung einen spezifischen Rahmen, der kooperationsfördernd wirken soll. Dabei sind für die Verhandlungsförderung das Mediationsverfahren (1.) und der Ausgleich ungleicher Verhandlungspositionen durch den Mediator richtungsweisend (2.) und sollen abschließend bewertet werden (3.).

1. Mediationsverfahren

Die konkrete Ausgestaltung der Verhandlung mit Mediation unterliegt der Parteienautonomie und dem Streitgegenstand, so dass nicht von einer einzigen Ausprägung des Mediationsverfahrens auszugehen ist, sondern ein ganzes Spektrum an Verfahrensarten der Mediation zuzuordnen ist. Die Darstellung der Verfahrensprinzipien nach dem Mediationsgesetz soll jedoch die Grundlage bilden (a), um anschließend die Aufgaben des Mediators herauszuarbeiten (b).

a) Verfahrensprinzipien, § 1 MedG

Die Verfahrensprinzipien der Mediation richten sich nach § 1 Abs. 1 MedG[812] und sehen ein vertrauliches und strukturiertes Verfahren vor, in

810 *Jóri*, IDPL 2015, 133.
811 *Nissenbaum*, Wash. L. Rev. 2004, 119 (130).
812 Das Mediationsgesetz ist auf die Richtlinie 2008/52/EG vom 21. Mai 2008 über bestimmte Aspekte der Mediation in Zivil- und Handelssachen (Mediationsrichtlinie) zurückzuführen.

dem eine freiwillige, eigenverantwortliche und einvernehmliche Konfliktlösung herbeigeführt wird. Diese wird durch einen unabhängigen und neutralen ohne Entscheidungsbefugnis ausgestatteten Mediator gefördert, § 1 Abs. 2 MedG. Mit diesen Rahmenkriterien sind die Grundlagen für die Verfahrensstruktur gelegt und sollen im Folgenden nach den Schlüsselkriterien des Mediationsverfahrens dargestellt werden. Zu Beginn steht das Motiv der Parteien, ein vertrauliches Mediationsverfahren durchzuführen (aa). Dem folgt das Erfordernis der Freiwilligkeit (bb), in einem von der Neutralität des Mediators (cc) und von der Eigenverantwortlichkeit der Parteien geprägten Verfahren (dd).

aa) Vertraulichkeit, §§ 1 Abs. 1, 4 MedG

Die Mediation ist ein vertrauliches Verfahren gemäß § 1 Abs. 1 MedG. Mit der Vertraulichkeit soll die Erweiterung des Verfahrensgegenstandes von den (Rechts-)Positionen hin zu den Interessenlagen erleichtert werden, damit eine Einigung über die Rechtspositionen hinaus ermöglicht wird. Dieser Verfahrensgrundsatz erstreckt sich auf den Mediator und den anderen in der Mediation eingebunden Personen, so dass eine grundsätzliche Verschwiegenheit gilt. Es besteht jedoch die Ausnahme, dass Tatsachen aus Gründen des *ordre public* und für die wirksame Vollstreckung offenzulegen sind, § 4 Abs. 1 Nr. 1, 2 MedG. Insgesamt soll mit der Vertraulichkeit des Verfahrens ein Anreiz für die Bereitschaft zur Offenlegung der hinter den Positionen liegenden Interessen geschaffen werden.

bb) Freiwilligkeit, §§ 1 Abs. 1, 2 Abs. 2 MedG

Das Mediationsverfahren verlangt die freiwillige Teilnahme der Parteien am Verfahren, was eine Ausprägung des privatautonomen Charakters der Mediation ist. Mit dem Erfordernis der Freiwilligkeit wird ein tatsächliches Interesse an der Lösungsfindung vorausgesetzt, so dass die angenommene Chance für ein erfolgreiches Mediationsverfahren mit einer Einigung die Voraussetzung der Freiwilligkeit erfüllt. Gleichwohl wird mit der Freiwilligkeit ebenso die Möglichkeit umfasst, jederzeit das Mediationsverfahren sanktionsfrei beenden zu können, § 2 Abs. 5 S. 1 MedG.[813] Dem

813 *Greger*, in: Greger/Unberath/Steffek (Hrsg.), Recht der alternativen Konfliktlösung, 2016, § 1 Rn. 30–32.

steht gegenüber, dass die gesetzliche oder richterliche Anordnung zur Durchführung eines Mediationsverfahrens der Freiwilligkeit grundsätzlich widersprechen könnte, was aber im Einzelnen umstritten ist.[814] Dabei wird einerseits auf die freiwillige Entscheidung zum Mediationsverfahren und andererseits auf die inhaltliche Gestaltung des Einigungsinhaltes in der Mediation abgestellt. Nach einer Entscheidung des EuGHs[815] wurde auf die freiwillige inhaltliche Ausgestaltung der Einigung im Mediationsverfahren abgestellt, so dass kein Verstoß gegen das Freiwilligkeitserfordernis bei einer Anordnung zur Mediationsteilnahme besteht, wie es sich auch aus Art. 5 Abs. 2 der Mediationsrichtlinie[816] ergibt. Schließlich ist zur Sicherstellung der Freiwilligkeit gemäß § 2 Abs. 2 MedG vorgesehen, dass der Mediator sich über die freiwillige Teilnahme der Parteien an der Mediation vergewissert.

cc) Neutralität, §§ 1 Abs. 2, 2 Abs. 3, 3 Abs. 1 MedG

Das Mediationsverfahren ist geprägt von der Neutralität des Mediators gegenüber den Parteien und von seiner Verpflichtung, im gleichen Maße die Kommunikation der Parteien zu fördern, §§ 2 Abs. 3 S. 1–2, 1 Abs. 1 MedG. Bei Vorliegen der Unabhängigkeit und Neutralität des Mediators beeinträchtigenden Umständen, wären diese gemäß § 3 Abs. 1 MedG offenzulegen. Dieses Schutzkonzept dient dem Postulat der *Allparteilichkeit* des Mediators, sich gegenüber beiden Parteien inhaltlich gleichermaßen zu verpflichten und beide Parteien in die Kommunikation einzubinden, sog. *Gleichbehandlungsgebot*.[817] Darin kommt der Verfahrensrahmen zur eigenverantwortlichen Lösungsfindung zum Ausdruck, der mit spezifischen Methoden etwa der Durchführung von Einzelgesprächen und sogar Lösungsideen des Mediators ausgestaltet werden kann.[818]

814 *Ders.*, in: Greger/Unberath/Steffek (Hrsg.), Recht der alternativen Konfliktlösung, 2016, § 1 Rn. 33.
815 EuGH, Urt. v. 14.06.2017, C-75/16, Rn. 49.
816 Richtlinie 2008/52/EG vom 21. Mai 2008 über bestimmte Aspekte der Mediation in Zivil- und Handelssachen (Mediationsrichtlinie).
817 *Greger*, in: Greger/Unberath/Steffek (Hrsg.), Recht der alternativen Konfliktlösung, 2016, § 2 Rn. 140, 151 f.; daraus ableitend das *Differenzierungsgebot*, vgl. *Gasser*, Kausalität und Zurechnung von Information als Rechtsproblem, 2002, S. 235.
818 *Eidenmüller*, ZKM 2013, 4.

dd) Eigenverantwortlichkeit, §§ 1 Abs. 1, 2 Abs. 5 MedG

Die Eigenverantwortlichkeit der Parteien in dem Mediationsverfahren ist eines der tragenden Grundsätze der Mediation. Die Parteien sollen in dem Mediationsverfahren eigenverantwortlich eine Lösung finden, was die Alternative zum Gerichtsverfahren ausmacht. Der Mediator schafft den Verhandlungsrahmen für die Kooperation, mit dem die Parteien über die Positionen hinaus ihre Interessen für eine nachhaltige Einigung austauschen können. Dabei ist der Mediator lösungsabstinent und schafft einen Rahmen, in dem die Parteien eine eigenverantwortliche Lösung finden können, § 1 Abs. 1 MedG. Dies setzt voraus, dass die Parteien im Vorfeld ihre beste und schlechteste Verhandlungsalternative[819] für die Entscheidung der mitzuteilenden Interessenlage aussondiert haben. Die Eigenverantwortlichkeit ist gemäß § 2 Abs. 5 MedG für die Mediation konstituierend und kann dazu führen, dass der Mediator das Mediationsverfahren beendet, wenn die eigenverantwortliche Kommunikation in der Mediation aus der Sicht des Mediators fehlt. Insgesamt wird damit von den Parteien eine Eigenverantwortlichkeit und Aufrichtigkeit abverlangt, die erst mit einem neutralen und sanktionsfreien Verfahrensrahmen möglich ist.[820]

b) Aufgaben des Mediators, § 2 MedG

Der Mediator wird von den Parteien ausgewählt und ist für die Gewährleistung der Verfahrensprinzipien und den Rahmen der Verhandlung verantwortlich, § 2 MedG. Dabei ist der Mediator den Parteien gleichermaßen verpflichtet und ermöglicht eine eigenverantwortliche Einigung. Es gehört zu den Kernkompetenzen des Mediators, sich solcher Methoden zu bedienen, die den Kommunikations- und Kooperationsprozess fördern.[821] Etwa mit der sog. „*shuttle-Diplomatie*" kann eine Brückenkommunikation durch den Mediator gefördert werden, die zugleich eine Ausprägung des *Gleichbehandlungsgebotes* darstellt.[822] Damit wird die Kommunikation verändert und die Interessen können offengelegt werden, so dass sich aus den Nach-

819 *Barnett/Treleaven*, The Computer Journal 2017, 399 (406).
820 *Rasmusen*, Games and information, 2009, S. 33.
821 *Greger*, in: Greger/Unberath/Steffek (Hrsg.), Recht der alternativen Konfliktlösung, 2016, § 2 Rn. 147, 253 f.; *Eidenmüller*, in: Breidenbach/Henssler (Hrsg.), Mediation für Juristen, 1997, 31 S. 52 f.
822 *Ders.*, in: Greger/Unberath/Steffek (Hrsg.), Recht der alternativen Konfliktlösung, 2016, § 2 Rn. 162.

richten ein anderer Erkenntnisgehalt ableiten lässt und eine „Rekonzeptualisierung des Konfliktes" möglich wird.[823] An dem bereits erwähnten Orangenbeispiel[824] kann die Methodik des Mediators dazu führen, dass das Interesse an der Orangenschale auf der einen Seite und das Interesse an dem Orangensaft auf der anderen Seite den ursprünglichen Konflikt um die eine Orange in eine „*win-win*"-Lösung überführt. Damit kann der Mediator zur Einigung von Teilkonflikten in dem Mediationsverfahren beitragen, die in eine Gesamtlösung münden und aus spieltheoretischer Perspektive den Fokalpunkt als gemeinsames Gleichgewicht begründen. Mit der Erweiterung auf den Konfliktgegenstand des öffentlichen Gutes der persönlichen Informationen ginge es um die Herbeiführung einer die persönlichen Informationen schonenden „*win-win-win*"-Lösung für den Betroffenen und Verantwortlichen mit Hilfe der Mediation.

2. Ausgleich der ungleichen Verhandlungsmacht

Zur Verhandlung mit der Mediation bei einer gleichen Verteilung der Verhandlungsmacht passt das Verfahren, wohingegen die Einsetzbarkeit der Mediation bei einer ungleich verteilten Verhandlungsmacht zu hinterfragen ist. Die Verfahrensprinzipien der Mediation können zu Lasten der schwächeren Verhandlungspartei wirken, wenn diese etwa über begrenzte Ressourcen für den Einigungsspielraum verfügt, unter Kostendruck steht, über weniger Verhandlungserfahrung verfügt oder eine deutliche Informationsasymmetrie besteht. So könnte die Vertraulichkeit und Freiwilligkeit des Verfahrens genutzt werden, um die Interessenlage der gegnerischen Partei für eine anschließend defektive Spielentscheidung in Erfahrung zu bringen. Indem die Verhandlung über die Bilder personaler Identitäten und den Schutz des öffentlichen Gutes der persönlichen Informationen erfolgt, können die Informationsasymmetrien in einer Verhandlung zu einer Gefährdung der Schutzinteressen führen.

Innerhalb eines Mediationsverfahrens kann eine bestehende Informationsasymmetrie mit den Verfahrensprinzipien zunächst keinen Ausgleich erfahren, jedoch können „*Schwächerenschutzinstrumente*"[825] eingesetzt werden. Diese können darin liegen, dass der Mediator im Rahmen seiner Verpflichtung zur Allparteilichkeit das bestehende Machtungleichgewicht an-

823 *Eidenmüller*, ZKM 2013, 4 (8); *Glasl*, Konfliktmanagement, 2020, S. 322.
824 5. Teil, B., II., 1.
825 *Wendenburg*, Der Schutz der schwächeren Partei in der Mediation, 2013, S. 234.

erkennt[826] und anschließend die schwächere Partei in ihrer Selbstbestimmung möglicherweise als Verbraucherschutzmaßnahme fördert.[827] Denn der Mediator unterliegt der Neutralitätspflicht, was die allparteiliche Förderung der Parteiinteressen umfasst. Sollten die Parteiinteressen aufgrund des Machtungleichgewichts nicht mehr zum Gegenstand der Mediation werden können, würde dies den Verfahrensgrundsätzen widersprechen und ein Grund zur vorzeitigen Beendigung der Mediation sein.[828] Ungeachtet dessen kommt als Schwächeschutzinstrument ebenso die Anordnung der Mediation in Betracht. Diese würde dazu dienen, dass die Parteien überhaupt erst miteinander verhandeln, ohne jedoch dabei den Anspruch eines vollständigen Ausgleiches der Informationsasymmetrie zu verfolgen. Der Ausgleich von Informationsasymmetrien in der Mediation lässt sich zudem über die Methoden des Mediators lösen. Insgesamt kommen für die Verhandlung zwischen Verantwortlichem und Betroffenen die Anordnung zur Mediation und die Implementierung spezifischer Methoden in Frage. Darin liegen Schwächeschutzinstrumente, die in der Identitätsverwaltung eingesetzt werden könnten, um die bestehende Informationsasymmetrie auszugleichen.

3. Bewertung

Die Verhandlung mit der Mediation unterliegt Verfahrensprinzipien, die kooperationsfördernd wirken und bei der Verhandlung über die Bilder personaler Identitäten dem Schutz des öffentlichen Gutes der persönlichen Informationen dienen. Die Neutralitätspflichten des Mediators und das *Gleichbehandlungsgebot* in dem Verfahren fungieren als kompensatorisches Gegengewicht gegenüber den potentiell diskriminierend ausgestalteten Profilen und Bildern personaler Identitäten. Weiter deckt sich der Grundsatz der Freiwilligkeit für die inhaltliche Verhandlung des Bildes der personalen Identität in ihrem *Ipse*-Anteil mit der freiheitlichen informationellen Selbstbestimmung. Gleichwohl kann die Freiwilligkeit beim Einsatz des Mediationsverfahrens eine Einschränkung erfahren, wenn die Durchführung der Mediation angeordnet wird. Eine solche Anordnung gegenüber dem Verantwortlichen könnte zunächst ermöglichen, dass die Parteien miteinander in Verhandlung treten. Entscheidend ist dabei die Bewahrung

826 *Ders.*, Der Schutz der schwächeren Partei in der Mediation, 2013, S. 259.
827 *Ders.*, Der Schutz der schwächeren Partei in der Mediation, 2013, S. 262–271.
828 *Ders.*, Der Schutz der schwächeren Partei in der Mediation, 2013, S. 273.

der Freiwilligkeit der Parteien über den Verhandlungsinhalt und die grundsätzliche Neutralität des Mediators, damit das Mediationsverfahren in seinem Rahmen genutzt wird, um die Interessen für spezifische Bilder personaler Identitäten einbeziehen zu können. Damit würde eine eigenverantwortliche Einigung über die Bilder personaler Identitäten in ihrer dynamischen *Ipse*-Dimension erfolgen, ohne dass es bei den statisch erstellten Bildern der Identitäten durch den Verantwortlichen bleibt. Der Betroffene würde auf diese Weise seine informationelle Selbstbestimmung in einem *Konzept des Selbstdatenschutzes* unter den Bedingungen der Verhandlung ausüben können.

Schließlich kann gegenüber der bestehenden Informationsasymmetrie die Identitätsverwaltung selbst als Schwächeschutzinstrument eingesetzt werden, wenn diese als „*mechanism by design*" Gleichgewichte zwischen den jeweiligen Bildern personaler Identitäten und eine Pluralität von Bildern personaler Identitäten ermöglicht.

III. Mediator als technischer Agent

Die Verhandlung mit Mediation kann ebenso auf der technischen Ebene durchgeführt werden. Für die Identitätsverwaltung kommt der Einsatz eines technischen Mediators als Schwächeschutzinstrument in Betracht, der dem Schutz des öffentlichen Gutes der persönlichen Informationen dient. Dafür sollen die Eigenschaften eines technischen Mediators (1.) und die Zwecke eines technischen Mediators (2.) bestimmt werden. Weiter soll die Begründung eines technischen Mediationsagenten erfolgen (3.).

1. Eigenschaften eines technischen Mediators

Für die Steigerung der Kooperation über die Bilder personaler Identitäten kann ein technischer Mediator als Schwächeschutzinstrument eingesetzt werden. Es geht dabei um die Steigerung der Iterationszahl bei der Erstellung des Bildes der personalen Identität durch den Verantwortlichen. Die Bestimmung der Eigenschaften eines technischen Mediators soll sich nach einem hypothetischen Mediator richten, da dieser den Verfahrensrahmen für differenzierte Spieliterationen zur Kooperationsförderung setzen würde. Demnach muss ein technischer Mediator neutral und lösungsabstinent sein, indem er keinen eigenen Beitrag zu der Konstruktion von Bildern personaler Identitäten leistet. Aus der Perspektive der Informatik ginge es

möglicherweise um einen Informationskanal, der über einen technischen Vermittler als Umsetzer verfügt, wie man es bei den Banken als Intermediäre von Transaktionen mit dem Einsatz von Transaktionsnummern kennt.[829] Danach wird der Eingabewert infolge der Authentifizierung mit der TAN in einen Ausgabewert umgewandelt und der Vorgang erfolgt mit einem neutralen technischen Vermittler unter den vorgegebenen Maßgaben. Dieser technische Vermittler würde einen Beitrag zur Informationsveränderung und Komplexitätsreduktion leisten, um neue Erkenntnismöglichkeiten generieren zu können.[830] Dies entspräche der Aufgabe eines Mediators als „*Agent of (a new) reality*"[831], mit dem eine Neuverhandlung („*renegotiate*")[832] der Erkenntnismöglichkeiten erfolgt. In einem Informationskanal mit einer vermittelten Informationsveränderung besteht die Chance, dass vorangegangene Erkenntnismöglichkeiten im Datenzyklus intransparent und vergessen werden. Dabei wäre ein kommunikativer Austausch durch den Mediator nicht zwingend erforderlich, vielmehr können die Verfahrensiterationen Signalwirkung haben und einen stillschweigenden kooperationsfördernden Beitrag leisten.[833]

Die grundsätzliche Vertraulichkeit der Mediation steht dabei im Gleichlauf zur Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 f) DSGVO, da der technische Mediator einen Schutzmechanismus für die Bilder personaler Identitäten verkörpern würde. Ebenso wäre die Freiwilligkeit der Mediation gewährleistet, selbst wenn der technische Mediator obligatorisch implementiert werden würde. Indem die Verhandlung der Bilder personaler Identitäten auf der inhaltlichen Ebene unter der Maßgabe der Freiwilligkeit erfolgen würde, könnte der technische Mediator obligatorisch eingesetzt werden. Zudem könnte mit einem technischen Mediator dem Betroffenen eine erweiterte Zugangskontrolle über die Informationen zu den Bildern personaler Identität ermöglicht werden.

---

829 *Steinmüller*, Information, Modell, Informationssystem, S. 2; *Froomkin*, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, S. 30.

830 *Ders.*, Information, Modell, Informationssystem, S. 61–63; *Haft*, Einführung in die Rechtsinformatik, 1977, S. 100–102.

831 *Kracht*, in: Haft/Schlieffen (Hrsg.), Handbuch Mediation, 2016, § 13 Rn. 95, 97.

832 *Jay*, Data protection law and practice, 2012, Rn. 6.39.

833 *Schelling*, The strategy of conflict, 1969, S. 64 f.

2. Zwecke eines technischen Mediators

a) Zweck der Risikominimierung

Mit dem technischen Mediator lässt sich das Risiko für den Schutz der persönlichen Informationen minimieren, da dieser als ein Assistenzsystem für den Betroffenen zum Schutz der *kontextuellen Integrität* personaler Identitäten fungieren könnte. Die Notwendigkeit eines Assistenzsystems wird von *Spina* dahingehend vorgeschlagen, dass der verhältnismäßige Ausgleich individueller Interessen eines unterstützenden Systems bedarf.[834] Damit ginge es um die Transparenz und die Beherrschbarkeit des Risikos mit einer gesonderten Zugangskontrolle zu den Bildern personaler Identitäten und ihrer Verhandelbarkeit über den technischen Mediator. Entscheidend dabei ist es, dass mit einem technischen Assistenzsystem bei dem Betroffenen keine gesteigerte Kontrollmöglichkeit für den Schutz personaler Identität suggeriert wird, damit die Wirkungen des Kontroll-Paradoxons nicht greifen. Vielmehr gilt es, dass aus der Perspektive des Betroffenen mit einem technischen Mediator die Iterationen erweitert werden und das Risiko für die persönlichen Informationen minimiert wird.

b) Zweck der Rechtsdurchsetzung

Mit dem technischen Mediator könnte die Wirksamkeit IKT-rechtlicher Vorgaben gesteigert werden. Das legitimatorische Defizit im Datenzyklus personaler Identitäten könnte über die *iterative Kontrolle* durch die Verhandlungsmöglichkeit der Bilder personaler Identitäten im Datenzyklus kontextspezifisch wiederhergestellt werden. Damit wird auf die Wirksamkeit des Rechts hingewirkt, wenn mit einem Verfahren der Zugang zu einem rechtsdurchsetzenden Mechanismus geschaffen wird. Dieser Mechanismus könnte über den technischen Mediator erfolgen und würde einen Beitrag zur Kontrolle über den Zugang zu den Bildern personaler Identitäten leisten, so dass damit die Immunisierung gegenüber dem legitimatorischen Defizit im Datenzyklus gesteigert würde. Somit lässt sich mit dem technischen Mediator, bestehend aus einem alternativen Streitbeilegungsmechanismus, eine Steigerung der Verfahrensgerechtigkeit und ein Ausgleich der Informationsasymmetrie für die Parteien herbeiführen.

---

834 *Spina*, EJRR 2014, 248 (252).

3. Technischer Mediationsagent

Der technische Mediatonsagent hätte die Eigenschaften eines Mediators und würde der Risikominimierung und Rechtsdurchsetzung für eine iterative Verhandlung der Bilder personaler Identitäten dienen. Dieser Agent wäre den jeweiligen Prinzipalen des Betroffenen und des Verantwortlichen zuzuordnen und sein Einsatz wäre kontrollierbar, wobei die inhaltliche Ausgestaltung der Bilder personaler Identitäten Verhandlungsgegenstand sein müsste. Es würde sich um einen *aktiven Agenten* handeln,[835] der inhaltlich auf die Informationen verändernd einwirken und damit ein „neues" Bild der personalen Identität schaffen würde, welches einer Bestätigung oder Ablehnung von den Prinzipalen des Verantwortlichen und Betroffenen bedürfte. Insofern bestünde ein technischer Mediationsagent aus einem *strukturierten Entscheidungsverfahren*[836] und ihm käme eine gestalterische und dynamische Funktion im Datenzyklus der personalen Identität in ihrem *Ipse*-Anteil zu. Dieses strukturierte Entscheidungsverfahren könnte der Formalisierung mit den Verfahrensprinzipien nach dem Mediationsgesetz unterliegen und als *Instruktion* für die Verhandlung der Bilder personaler Identitäten dienen. Mit dem Transfer in einen Algorithmus, der als ein intelligenter Agent eingesetzt wird, könnten die Verfahrensregeln automatisiert werden. Dieser intelligente Agent müsste eine kooperative Funktionalität aufweisen und eine Wissensbasis voraussetzen, mit der algorithmusbasiert neue Sachzusammenhänge unter Wahrung der *Instruktionen* als Lösungen hergestellt werden.[837] Diese Lösungen könnten in einem Abgleich der widerstreitenden Bilder personaler Identitäten münden und der dynamischen *Ipse*-Dimension der personalen Identität gerecht werden.

Die technische Einrichtung eines Verfahrensrahmens für den Mediationsagenten könnte sich auch nach der EU-Verordnung über die online-Beilegung verbraucherrechtlicher Streitigkeiten[838] und dem Gesetz über die alternative Streitbeilegung in Verbrauchersachen (Verbraucherstreitbeilegungsgesetz-VSBG) richten. Mit diesen Regelungen werden die rechtlichen Grundlagen für alternative Streitbeilegungsmethoden im online-Kontext festgelegt, bei denen die Parteien zusammengeführt werden, um einen Einigungsprozess durchführen zu können. Der technische Mecha-

835 3. Teil, D.
836 3. Teil, B., I.
837 Angelehnt an *Müller-Henstenberg/Kirn*, MMR 2014, 307 (309).
838 Verordnung (EU) Nr. 524/2013 vom 21. Mai 2013 über die Online-Beilegung verbraucherrechtlicher Streitigkeiten.

nismus wird dabei die Informationssammlung und die Beilegungsmethode mit einem mehrstufigen Kommunikationsprozess[839] umfassen müssen und kann teil- oder vollautomatisiert ausgestaltet sein.[840] Der Kommunikationsprozess wäre in Phasen zu begrenzen, damit diese als koordinierender Faktor für eine Einigung wirken.[841]

Insoweit lässt sich in einem technischen Mediationsagenten auch die Ausprägung einer „Daten(rechts)verkehrsordnung"[842] erblicken, mit der ein technisch unterstütztes Verfahren zur Koordination der Bilder personaler Identität bestünde. Die geregelte Ordnung für die online-Beilegung von Streitigkeiten ließe sich auf einen für die Bilder personaler Identitäten eingesetzten technischen Mediationsagenten übertragen, so dass dieser auf der Mikroebene über ein online-Streitbeilegungsverfahren verfügt. Weiter müsste dieser Agent die Interoperabilität zwischen den Informationsströmen der Bilder personaler Identitäten erlauben, damit die kontextbezogene Verhandlung und die gleichzeitige Trennung der kontextbezogenen Bilder zur Wahrung der *kontextuellen Integrität*[843] ermöglicht werden. Für die Funktionalität des interoperablen Agenten könnte das Konzept des maschinenlesbaren elektronischen Formats gemäß Art. 12 Abs. 7 S. 2 DSGVO angewendet und auf die elektronischen Bilder personaler Identitäten übertragen werden.

---

839 *Barnett/Treleaven*, The Computer Journal 2017, 399 (405); www. *smartsettle.com/about-us/process/* (zuletzt aufgerufen 20.06.2020) Hier werden sechs Phasen für die Streitbelegung beschrieben. In der vierten Phase ist ein Lösungsvorschlag durch Software vorgesehen, auf den sich die Parteien einigen können. Von *Pretschner/Walter* wird ein produktbezogener mehrstufiger Kommunikationsprozess zur Verhandlung der „*Policies*" vorgeschlagen, der automatisiert erstens das Angebot von Produkten, zweitens die Mitteilung des Verbrauchers über das ihn interessierende Produkt, drittens das konkrete Angebot des Unternehmers und viertens die Wahl durch den Verbraucher vorsieht, *Pretschner/Walter*, IEEE 2008, 1135. Ebenso könnte die Blackbox-Pflicht gemäß §§ 63a, 63b StVG für einen technischen Mediationsagenten mögliche Anhaltspunkte bieten, da gemäß § 63a Abs. 4 StVG eine sechsmonatige Löschroutine vorgesehen ist und Deckungsgleich mit dem Löschbedarf von Bildern personaler Identitäten herangezogen werden kann.

840 *Dies.*, The Computer Journal 2017, 399 (402–404). Dabei ist in dem Konzept des „*Discovery*"- Verfahrens gerade zu berücksichtigen, dass die jeweiligen Verbindungen der Fakten genutzt werden können für ein technisiertes „*E-Discovery*"-Verfahren, *Kaulartz*, DSRI 2017, 599 (605).

841 *Schelling*, The strategy of conflict, 1969, S. 60.

842 *Lewinski*, Die Matrix des Datenschutzes, 2014, S. 51.

843 4. Teil, A., II.

4. Zusammenfassung

Der Mediator für die Bilder personaler Identitäten lässt sich als technischer Agent ausgestalten, um mit einer gesteigerten Verfahrensgerechtigkeit den Rahmen für die Kompensation legitimatorischer Defizite und die Immunisierung im Datenzyklus zu gewährleisten. Dabei sind die Verfahrensprinzipien aus der Mediation in einen technischen Agenten zu überführen, der auf der Mikroebene im iterativen Verfahren, welches mit der Online-Streitbeilegung vergleichbar wäre, wirken könnte. Für den Schutz des öffentlichen Gutes der persönlichen Informationen könnte damit ein gesteigerter Zugang zu den Bildern personaler Identitäten geschaffen werden, der Gegenstand kooperativer Verhandlungen wäre und risikomindernd wirken würde. Damit einher ginge eine Erweiterung der Kontrollmöglichkeiten, ohne dabei das Kontroll-Paradoxon auszulösen, da die Kontrolle sich auf den Zugang zu den Bildern der personalen Identitäten und ihrer Verhandlungsfähigkeit zu beschränken hätte. Gleichzeitig wäre der technische Mediationsagent obligatorisch für die Bilder personaler Identitäten einzusetzen, was keinen Verstoß gegen den Grundsatz der Freiwilligkeit des Mediationsverfahrens bedeutet, da die inhaltliche Ausgestaltung des Verfahrens weiterhin der Freiwilligkeit unterliegen würde. Schließlich könnte der technische Mediationsagent mit einer fragmentarischen Rechtssubjektivität ausgestattet werden, die aus künstlicher Intelligenz bestehen würde und dem Prinzipalen zurechenbar wäre. Somit könnte ein technischer Mediationsagent als ein *aktiver Agent* den Zugang zu den Bildern personaler Identitäten und die Verhandlungsfähigkeit dieser gewährleisten.

IV. Verhandelte Identität im Schatten des Rechts

Für die Verhandlung der Bilder personaler Identitäten wurde ein technischer Mediationsagent erarbeitet, der als alternative Streitbeilegungsmethode im „Schatten des Rechts" zum Einsatz käme. Das schattenwerfende IKT-Recht umfasst die Informationspflichten über die Datenverarbeitung, die datenschutzkonforme Technikgestaltung gemäß Art. 25 DSGVO für ein Konzept des „*identity management by design*", die Rechtfertigungsgründe nach Art. 6 DSGVO mit dem verbundenen Legitimationsdefizit und das Auskunftsrecht gemäß Art. 15 DSGVO als Zugangsrecht zu den Bildern personaler Identitäten. Denn diese rechtlichen Maßgaben richten sich an die Datenverarbeitung und die damit verbundenen Rechtspositionen, wohingegen die Interessen am Schutz der persönlichen Informationen

sich im Schatten des Rechts befinden und über einen möglichen technischen Mediationsagenten einbezogen werden könnten. Daneben ergibt sich mit diesem Konzept eine direkte Wirkung auf die Bilder personaler Identitäten. Das Konzept lässt sich dafür einsetzen, Bilder personaler Identitäten mit Vergangenheitsbezug zu aktualisieren.

Indem die Neuverhandlung des Bildes der personalen Identität mit dem Effekt des „*Reframings*", bestehend aus einer anderen sprachlichen „Verpackung" des Bildes der personalen Identität, erfolgen kann, können *Priming*-Effekte nutzbar gemacht werden. Dabei sollte die Aufmerksamkeitsausrichtung mit anderen Referenzpunkten versehen werden,[844] damit eine Neuinterpretation und ein neuer Erkenntniswert des Bildes personaler Identität ermöglicht wird. Entscheidendes Kriterium bei diesen Maßgaben wäre es, dass sie im Schatten des bestehenden IKT-Rechts realisiert werden müssten, da eine direkte rechtliche Regelung zur Einrichtung eines technischen Mediationsagenten dem Abstraktionsgrad des Rechts widersprechen würde. Dabei kommt die Implementierung eines technischen Mediationsagenten als „*identity management by design*"-Konzept und auch als Verhaltensregel zur fairen und transparenten Verarbeitung gemäß Art. 40 Abs. 2 a) DSGVO in Betracht. Demnach können Verbände solche Verhaltensregeln ausarbeiten, die von den Verantwortlichen im Rahmen der regulierten Selbstregulierung zur Implementierung und Anwendung eines technischen Mediationsagenten angewendet werden. Diese Einordnung der „Mediation als regulierte Selbstregulierung"[845] erlaubt die Einbeziehung des technischen Mediationsagenten als eine Form der kooperativen Umsetzung IKT-rechtlicher Vorgaben. Ein derartiges Konzept der regulierten Selbstregulierung mit Verhaltensregeln gemäß Art. 40 DSGVO ließe sich als freiwilliges Engagement innerhalb der „*Corporate Social Responsibility*"[846] einordnen und hätte den Vorteil, dass die Anwendung der Verhaltensregeln in Gestalt des technischen Mediationsagenten in inhaltlicher Hinsicht über eine hohe Flexibilität[847] verfügen würde. Damit würde aus dem IKT-Recht ein „*identity management by design*"-Konzept das bestehende Recht ergänzen und die Verhaltensregeln gemäß Art. 40 DSGVO den Schutz der personalen Identität erweitern. Daneben erscheinen ein viel-

844 4. Teil, C., II., 1, b), bb); *Winheller*, ZKM 2018, 116 (117–119).

845 *Appel*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts Gesamtwerk, 2012, § 32 Rn. 106; über die Stärkung gegenüber Machtungleichgewichten mit dem Selbstdatenschutz, vgl. *Talidou*, Regulierte Selbstregulierung im Bereich des Datenschutzes, 2005, S. 26 f., 30.

846 *Spindler/Thorun*, MMR-Beilage 2016, 1 (13, 23).

847 *Dies.*, MMR-Beilage 2016, 1 (9).

schichtiger Anreizmechanismus zur Implementierung technischer Mediationsagenten und ein entsprechender Verhaltenskodex im IKT-Recht und im Wettbewerbsrecht wünschenswert.

V. Mediative Identitätsverwaltung

Die mediative Identitätsverwaltung ist geprägt von der Verhandlung personaler Identitäten und dem Schutz dieser im Sinne einer *kontextuellen Integrität*. Die Implementierung einer mediativen Identitätsverwaltung verlangt die Einbeziehung derjenigen rechtlichen Mechanismen, die zu dem unzureichenden Schutzgefüge personaler Identitäten geführt haben. Entsprechend kann mit Rechtsnormen ein Anreizmechanismus geschaffen werden, der sich ebenfalls ökonomisch auswirkt. Dies kann in einer Konkretisierung der Vorgabe des „*privacy by design*" liegen, wonach der Verantwortliche ein „*identity management by design*" in Gestalt eines technischen Mediationsagenten zu implementieren hätte. Auf der Ebene des Betroffenen wären Anreize erforderlich, um eine risikobewusste Entscheidung bei der Nutzung eines technischen Mediationsagenten zu fördern. Unter diesen Maßgaben würde eine mediative Identitätsverwaltung umgesetzt werden können. Dabei würde ein solches Konzept mit inhaltlichen und technischen Methoden unter Einbeziehung von Visualisierungstechniken[848] realisiert werden, wie es mit einem *Dashboard-System* möglich wäre.

Auf der rechtlichen Ebene kann die Grundlage für ein *verhaltensänderndes Anreizsystem* geschaffen werden, wie es etwa für die Implementierung der Mediation mit § 253 Abs. 3 Nr. 1 ZPO erfolgt ist, wonach in der Klageschrift eine Angabe darüber erfolgen soll, ob vor Klageerhebung ein Mediationsversuch oder ein anderes Verfahren der außergerichtlichen Konfliktbeilegung unternommen wurde. Mit dieser Vorschrift wird der Regelungszweck verfolgt, ein Begründungserfordernis zur Bewusstseinsförderung über das Bestehen von Alternativen zum Gerichtsverfahren herbeizuführen und kann insoweit als eine verhaltensfördernde Regelung mit einer konkreten Verhaltensauswirkung auf die Parteien eingeordnet werden.[849] Demnach könnte für die Implementierung eines technischen Mediationsagenten *de lege ferenda* eine Regelung erfolgen, die von dem Verantwortlichen die Einbeziehung eines technischen Mediationsagenten für die Kontrolle der Bilder personaler Identitäten im Datenzyklus verlangt. Ebenso

848 *Winheller*, ZKM 2018, 175.
849 *Eidenmüller*, JZ 2011, 814 (819).

wäre *de lege ferenda* denkbar, dass dem Verantwortlichen eine Begründungspflicht auferlegt würde, wenn bei umfangreichen Datenverarbeitungen kein Identitätsverwaltungskonzept vorgesehen ist, mit dem die Bilder personaler Identitäten dem Betroffenen zugänglich gemacht werden und ihm eine Verhandlungsmöglichkeit eingeräumt wird.

Die konkrete Maßnahme zur Implementierung eines technischen Mediationsagenten als „*identity management by design*" ließe sich unter den technischen und organisatorischen Maßnahmen bei der Umsetzung des Standes der Technik gemäß Art. 25 DSGVO einordnen. Ebenso kann der Datenverarbeitungsgrundsatz der Verarbeitung nach Treu und Glauben gemäß Art. 5 Abs. 1 a) DSGVO als rechtliche Grundlage für einen der *datenschutzrechtlichen Verfahrensgerechtigkeit* dienenden „*mechanism by design*" fungieren. Jeder dieser potentiellen Anreizmechanismen könnte zu einer mediativen Identitätsverwaltung und insgesamt zur Verwirklichung des öffentlichen Gutes der persönlichen Informationen beitragen, was einer Erosion datenschutzrechtlicher Vorgaben entgegenwirken würde. Insofern kann eine mediative Identitätsverwaltung das Gegengewicht zu der marktbeherrschenden Stellung von Intermediären darstellen, da in ihr ein „*opacity tool*" liegen könnte. Dieses würde der Iterationssteigerung dienen und damit als Schutzmechanismus für die Pluralität der Bilder personaler Identitäten fungieren.

Gegen die *mediative Identitätsverwaltung* ließe sich anführen, dass sie als ein paternalistisches Konzept und als eine Erweiterung des Datenverarbeitungsvorgangs ebenso *Angriffsgegenstand* werden könnte. Demnach würde sich das Risiko für die Rechte und Freiheiten natürlicher Personen steigern, wenn die Bilder personaler Identitäten durch einen Angriff für einen Dritten einsehbar wären. Weiter könne in diesem Konzept ein „Techno-Humanismus"[850] gesehen werden, der einerseits den menschlichen Willen als zentral ansieht, andererseits aber diesen mit technischer Steuerung und Lenkung verdrängt, so dass jede empfundene Kontrollmöglichkeit einer Scheinkontrolle gleichkomme. Auch führten technische Verfahren zur Formalisierung von Menschenrechten meist zu einer Erosion dieser.[851] Dem lässt sich entgegenhalten, dass das Phänomen von personalen Identitäten im online-Kontext ubiquitär und unumkehrbar ist, so dass die Lösung der damit verbundenen Risiken ebenso durch einen technischen Mechanismus erfolgen müsste. Folglich lässt sich ein Lösungsmechanismus

850 *Harari*, Homo Deus, 2017, S. 195.

851 *DeHert/Gutwirth*, in: Claes/Gutwirth/Duff (Hrsg.), Privacy and the criminal law, 2006, 61 (85).

anführen, der den Geschäftsmodellen von Intermediären gegenübergestellt wird. Da diese Geschäftsmodelle möglicherweise von spieltheoretischen Überlegungen zur maximalen Gewinnerzielung geprägt sind, sollte ein spieltheoretisch begründetes Schutzmodell über die personale Identität als Lösungsmechanismus herangezogen werden. Denn in Anbetracht der ökonomischen Prägung von Geschäftsmodellen erscheint eine Beschränkung des Schutzmechanismus auf das IKT-Recht mit den Betroffenenrechten unbefriedigend. Vielmehr wird ebenso die spieltheoretische Fundierung eines Lösungsmechanismus notwendig, um eine effektive Wirksamkeit und Durchsetzung des IKT-Rechts herbeiführen zu können.

Dieser Lösungsmechanismus könnte mit einer im „Schatten des Rechts" liegenden mediativen Identitätsverwaltung realisiert werden, die den Zugang, die Verhandlung der Bilder personaler Identitäten und die dynamische Identitätsbildung technisch unterstützt. Dazu kann der Einsatz rechtlicher Interventionsmechanismen in Gestalt einer Begründungspflicht dahingehend gehören, dass grundsätzlich ein mediatives Identitätsverwaltungskonzept bei einem bestimmten Datenverarbeitungsumfang vorgesehen ist. Dieses sollte ein „*identity management by design*"-Konzept im Rahmen des Standes der Technik gemäß Art. 25 DSGVO vorsehen. Ebenfalls kommt eine Implementierung des technischen Mediationsagenten als Verhaltensregel gemäß Art. 40 DSGVO in Betracht und könnte zum Gegenstand der Beschreibung eines Dienstes oder Produktes werden, so dass diese das Verhalten der Marktteilnehmer beeinflussen könnte.

VI. Zwischenergebnis

Das Mediationsverfahren ist im IKT-Recht verwurzelt, so dass sich aus den Verfahrensprinzipien wesentliche Vorgaben für die Verhandlung der Bilder personaler Identitäten ergeben. Diese würden durch einen technischen Mediationsagent umgesetzt werden, der als „*opacity tool*" ein Gegengewicht zu marktbeherrschenden Intermediären darstellen könnte. Denn mit einem technischen Mediationsagenten wird eine Iterationssteigerung herbeigeführt, die den dynamischen *Ipse*-Anteil personaler Identitäten gewährleistet. Die Implementierung eines technischen Mediationsagenten sollte im „Schatten des Rechts" erfolgen, indem ein „*identity management by design*"-Konzept einen technischen Mediator umfasst und ein *verhaltensänderndes Anreizsystem* über eine mit § 253 Abs. 3 Nr. 1 ZPO vergleichbare Regelung einbezogen wird. Damit könnte *de lege ferenda* der Verantwortliche ein Schutzregime einführen, was eine risikobewusste Entscheidung des

Betroffenen und die iterative Verhandlung der Bilder personaler Identitäten in Gestalt eines „*Reframings*" ermöglicht. Dies würde die Verfahrensgerechtigkeit steigern und dem Schutz des öffentlichen Gutes der persönlichen Informationen dienen.

D. Ergebnis: Mediationsagent zur Identitätsverwaltung

Die personale Identität unterliegt dem grundrechtlichen Schutz der informationellen Selbstbestimmung und ist zugleich vom Schutzgut der persönlichen Informationen umfasst. Der Schutz persönlicher Informationen ist eine Voraussetzung für demokratische Strukturen und ist als öffentliches Gut der Gegenstand spieltheoretischer Verhandlungen.[852] Dabei würde man die informationelle Selbstbestimmung grundsätzlich nicht in ein ökonomisches Modell überführen wollen, jedoch ist das Verhalten des Verantwortlichen und des Betroffenen als Spieler von Informationen und Auszahlungen beeinflusst, so dass eine spieltheoretische Modellierung des IKT-Rechts der Verdeutlichung von Strukturen dienen kann. Dafür wurde das IKT-Recht in den Strategieentscheidungen des Verantwortlichen und des Betroffenen *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung modelliert. Es konnte aufgezeigt werden, dass dieses als Nullsummenspiel über die Verteilung des öffentlichen Gutes der persönlichen Informationen mit defektiven und kooperativen Handlungen gespielt wird, ohne die Interessenlagen der Akteure in dem Spiel einzubeziehen.[853]

Demgegenüber wird das öffentliche Gut der persönlichen Informationen gewahrt, wenn das Strategieverhalten von Kooperation geprägt ist. Folglich stellt sich die Frage nach der Evolution der Kooperation, welche mit der *TIT for TAT*-Strategie erreicht werden kann. Mit der bestehenden Informationsasymmetrie und dem Verhandlungsungleichgewicht zwischen dem Verantwortlichen und den Betroffenen wurde das Erfordernis einer Intervention durch Verfahren nachgewiesen. Sobald Intermediäre mit marktbeherrschender Stellung in dem Spiel involviert sind, kommen wettbewerbsrechtliche Interventionen hinzu. Diese können aufgrund eines Missbrauchs der marktbeherrschenden Stellung, des unlauteren Wettbewerbs und im Rahmen der Ausschreibungsanforderungen zum „Schutz

852 5. Teil, A.
853 5. Teil, B., II.

der Vertraulichkeit von Informationen“ von Diensten und Produkten erfolgen.[854]

Für die Identitätsverwaltung konnte die Intervention mit dem kooperationsfördernden Mediationsverfahren herausgearbeitet werden, welches als Metakommunikation die Verhandlung der Bilder personaler Identitäten ermöglicht und als technischer Mediationsagent mit künstlicher Intelligenz ausgestattet werden könnte.[855] Dabei würde es sich um ein Konzept des „*mechanism by design*“ zum Schutz des öffentlichen Gutes der persönlichen Informationen handeln, welches in einem Gesamtkonzept der mediativen Identitätsverwaltung stünde. Dieses umfasst die Verhandlung der Bilder personaler Identitäten unter den *Instruktionen* des technischen Mediationsagenten und ein Anreizsystem zur Kompensation des Legitimationsdefizits im IKT-Recht. Das Anreizsystem könnte im „Schatten des Rechts“ in Gestalt von datenschutzrechtlichen Technikanforderungen und Verhaltensregeln umgesetzt werden. Weiter kommt *de lege ferenda* eine Verfahrensregel in Betracht, die dem Verantwortlichen eine Begründungspflicht darüber auferlegt, welche Identitätsverwaltungsmaßnahmen getroffen werden.[856] Ebenso wäre es denkbar, das öffentliche Gut der persönlichen Informationen in die Auflistung der Schutzgüter gemäß § 1 Abs. 1 ProdHG im Hinblick auf ein Recht auf datenerhebungsfreie Produkte aufzunehmen.[857] Damit würde dem Hersteller bereits zu einem frühen Stadium der Produktentwicklung eine umfassende Pflicht zur Implementierung von Schutzmaßnahmen auferlegt werden, die sich dann auf den gesamten Datenzyklus einer personalen Identität und ihren Schutz auswirken kann.

854 5. Teil, B., VI., 3.
855 5. Teil, C., I.–III.
856 5. Teil, C., V.
857 4. Teil, B., VI.

6.Teil: Modell der Identitätsverwaltung

Für die Begründung des Modells der Identitätsverwaltung sollen aus den bestehenden Analysen die maßgeblichen Voraussetzungen herausgearbeitet werden. Diese stehen den bisherigen Konzepten der Identitätsverwaltung als Berechtigungsverwaltung entgegen und legen einen Paradigmenwechsel zum dynamischen Identitätsbegriff nahe. Daher sollen nach einer Einführung (A.) die Modellvoraussetzungen der Identitätsverwaltung konkretisiert werden (B.) und in ein Konzept der verhandelten personalen Identität mit einem dezentralen Zugang überführt werden (C.).

A. Einführung

Für die Identitätsverwaltung wurden die Grundlagen herausgearbeitet und die Anforderungen aus dem IKT-Recht benannt. Weiter wurde eine spieltheoretische Modellierung vorgenommen, damit die ökonomischen Wirkungen gegenüber den persönlichen Informationen in dem Lösungskonzept ebenfalls berücksichtigt werden. Dies führte zu der Begründung des technischen Mediationsagenten, der *de lege ferenda* Gegenstand einer Regelung werden oder aber im „Schatten des Rechts" wirken könnte. Insoweit wurden rechtliche und ökonomische Modellierungen für ein Identitätsverwaltungsmodell vorgenommen, die nunmehr in eine systematische Perspektive in Gestalt einer technischen Infrastruktur eingeordnet werden. Danach konnten in den Grundlagen des 2. Teils dieser Arbeit die grundrechtlichen Anforderungen an den Begriff der personalen Identität festgelegt und im 3. Teil die Anforderungen an die Identitätsverwaltung beschrieben werden. Diese Anforderungen sollten, auch wenn sie ideell sein mögen, in eine technische Infrastruktur überführt werden. Die technische Infrastruktur sollte die rechtlichen und ökonomischen Perspektiven einbeziehen und im Zusammenhang mit den Realweltphänomenen der Selbstbestimmung und Selbstdarstellung der natürlichen Person im offline-Kontext stehen. Daher sollen aus den erarbeiteten rechtlichen und ökonomischen Perspektiven übergeordnete systematische Voraussetzungen der Identitätsverwaltung im online-Kontext beschrieben werden.

B. Modellvoraussetzungen der Identitätsverwaltung

Mit der bisherigen Einordnung der Identitätsverwaltung sind die Paradigmen einer statischen und dauerhaften Dimension der personalen Identität in ihren *Idem*-Anteilen verbunden, die im IKT-Kontext über ein *Berechtigungskonzept* verwaltet werden können. Aus den herausgearbeiteten IKT-rechtlichen Phänomenen ergibt sich jedoch eine Erweiterung der personalen Identität auf den Datenzyklus in seinen dynamischen und temporären Dimensionen des Begriffs der Identität in ihrem *Ipse*-Anteil. Unter Einbeziehung der ökonomischen Auswirkungen IKT-rechtlicher Phänomene erscheint eine Schwerpunktverschiebung auf den relationalen und kommunikativen Gehalt der Identität maßgeblich, so dass die Identitätsverwaltung eine Erweiterung verlangt. Dazu gehört, dass die bisherige Perspektive einer Berechtigungsverwaltung einem Perspektivwechsel unterzogen wird und auf eine kommunikationsbezogene, dynamische und temporäre Dimension der personalen Identität abzustellen ist. Dieser Perspektivwechsel[858] soll im Folgenden anhand der herausgearbeiteten Modellvoraussetzungen aufgeführt werden, und als Zuspitzung der Ergebnisse aus den rechtlichen und ökonomischen Analysen fungieren. Für ein Identitätsverwaltungsmodell wurden die Voraussetzungen herausgearbeitet, wonach die personale Identität zugänglich sein muss (I.), verhandelbar sein soll (II.) und dezentral auszugestalten ist (III.).

I. Paradigmenwechsel zum Identitätszugang

Die Ausprägungen der personalen Identität wurzeln bereits in der Legaldefinition zu den personenbezogenen Daten gemäß Art. 4 Nr. 1 DSGVO und in den Regelungen zu den Profilen und besonderen Kategorien personenbezogener Daten, aus denen sich jeweils ein eigenständiger kontextbezogener Erkenntnisgehalt generieren lässt. Gleichwohl gehört zu den Kriterien der Identitätsverwaltung die Kontrolle über die personalen Identitäten, die mit dem Zugang realisiert wird. In Anbetracht der Kontextbezogenheit und des Kommunikationszusammenhangs von personalen Identitäten können diese nur in relativer Hinsicht der Kontrolle unterliegen, so dass für eine ausgeprägte Steuerung und Kontrolle der Zugang Voraussetzung ist.[859] Zwar unterliegt auch die Generierung der Attribute von personalen

858 *Kuhn*, Die Struktur wissenschaftlicher Revolutionen, 2003, S. 137–155.
859 3. Teil, C., II., 2.

Identitäten zu Beginn des Datenzyklus der absoluten Kontrolle, jedoch verlagert sich die Kontrolle auf die Transparenz gemäß Art. 12 DSGVO und das Auskunftsrecht als Zugangsrecht gemäß Art. 15 DSGVO.[860] Ebenso spricht der Erlaubnisvorbehalt der Identitätsverwaltung für einen Kontrollschwerpunkt bei der Einwilligung, obwohl diese faktisch an Schutzwirkung gegenüber der informationellen Selbstbestimmung des Betroffenen einbüßt.[861] Entscheidend ist der Zugang zu den personenbezogenen Daten als Kontrollgegenstand gegenüber der scheinbaren Kontrolle durch die rechtfertigende Einwilligung, wie sie in dem Konzept „myneData"[862] beschrieben wird.

Es ergibt sich daraus der Bedarf nach einer verlagerten Betrachtung auf die Rechte nach der Rechtfertigung, die mit dem Zugang zu den kontextspezifischen personalen Identitäten über ein bereits beschriebenes *Dashboard-System* erfolgen kann. Dabei wird die Ausübung der informationellen Selbstbestimmung mit einem iterativen Zugangskonzept gefördert, das den Anknüpfungspunkt für die kontextbezogene Bündelung des Zugangs zu den personalen Identitäten mit einer spezifischen Vertrauens- und Sicherheitsstufe bilden kann, sog. (online) „*Identity Ecosystem*".[863] Voraussetzung dafür wäre, dass innerhalb des Kontextes der jeweiligen Vertrauens- und Sicherheitsstufe, wie sie gemäß Art. 8 Abs. 2 eIDAS-VO abgebildet ist,[864] die Interoperabilität über die personalen Identitäten hergestellt wird. Daher wäre eine gesicherte Plattform innerhalb der Vertrauens- und Sicherheitsstufe mit einem hohen Schutzniveau für personale Identitäten denkbar, welches als plattformbasiertes „*Identity Ecosystem*" fungieren würde. In diesem stünde zunehmend die Entscheidung der natürlichen Person im Vordergrund, inwieweit in den jeweiligen Vertrauens- und Sicherheitsstufen die personalen Identitäten verwaltet werden.

Darin liegt eine Verlagerung der Informationsmacht vom Verantwortlichen auf den Betroffenen, so dass bei dem Identitätszugang von einem nutzerzentrierten Ansatz auszugehen ist. Gleichzeitig steht der nutzerzentrierte Ansatz in Relation zu dem Verantwortlichen, so dass die Zugangsgewährung aufgrund der widerstreitenden Interessenlagen zum Gegenstand der Verhandlung werden sollte. Dafür wäre es denkbar, den Zugang

860 4. Teil, B., II., D., I.
861 4. Teil, C.
862 In „myneData" ist ein Datencockpit mit der Kontrollmöglichkeit über die Einwilligung vorgesehen, *Matzutt/Müllmann/Zeissig u.a.*, in: Eibl/Geadke (Hrsg.), INFORMATIK 2017, 1073 (1081).
863 2. Teil, A., III.
864 2. Teil, B., II., 2., b).

auch vertraglich durch Einräumung von Rechten und Pflichten zu regeln, damit die Verhandlungspositionen aneinander angeglichen werden können. Gleichzeitig bleibt für die Gewährleistung des Zugangs zu personalen Identitäten aus wettbewerbsrechtlichen Gründen eine staatliche Intervention nicht ausgeschlossen. Dabei geht es darum, dem Betroffenen eine effektive Verhandlungsmöglichkeit über den *Ipse*-Anteil der personalen Identität im Rahmen des Selbstdatenschutzes einzuräumen.

Um eine Abkehr von einem Zugang zu den personenbezogenen Daten und eine Hinwendung zu einem Identitätszugang vornehmen zu können, bedarf es durch den Verantwortlichen einer Bereitstellung der personenbezogenen Daten in einer die personale Identität darstellenden Form. Damit läge eine Maßnahme zum Ausgleich der Informationsasymmetrie und erweiterten Transparenz zugunsten des Betroffenen vor. Denn mit dem Identitätszugang wird die kontextbezogene personale Identität zunächst erkennbar und kann anschließend Gegenstand der individuellen Risikobewertung und Entscheidung über die Geltendmachung von Rechten werden. Ebenso könnte in einer Bereitstellung der Datensätze als personale Identität bereits ein Teil der Begründung und Erklärung der automatisierten Datenverarbeitung im Rahmen der Informationspflichten gemäß Art. 13 Abs. 2 f) DSGVO liegen, die Bestandteil eines „*identity management by design*"-Konzeptes werden könnten.

II. Paradigmenwechsel zur verhandlungsfähigen Identität

Von der Zugangs- und Berechtigungsverwaltung aus der informationstechnischen Perspektive abgesehen, geht es bei den personalen Identitäten um die kommunikative Ausprägung. Diese stellt sich infolge des dialogischen Prozesses zwischen *Idem*- und *Ipse*-Anteil der personalen Identität als ein narratives Selbstbild dar, welches wiederum zum Gegenstand der Kommunikation wird und von dem Empfänger als Gegenbild wahrgenommen wird. Infolgedessen kann sich der kommunikative Ablauf wiederholen und sich die Relation zwischen Selbstbild und Gegenbild einer Verhandlung über die personale Identität gleichen. Demnach bedarf es der Schwerpunktverlagerung von der personalen Identität hin zu den im Rahmen der Kommunikation verhandelten Bildern personaler Identitäten. Diese Bilder der personalen Identität sind das nach außen erkennbare Ergebnis, welches innerhalb der Kommunikation in Erscheinung tritt.

Nach dem bestehenden IKT-Recht erfolgt die Vergabe von Identitäten durch staatliche oder private Institutionen (1.) und kann zur Wahrung der

informationellen Selbstbestimmung in ein kompensatorisches Konzept der verhandelten personalen Identität mit einem Mediationsagenten münden (2.).

1. Identitätsvergabe durch Institutionen

a) Öffentlich-rechtliche Identitätsvergabe

Die öffentlich-rechtliche Identitätsvergabe über das Namensrecht, Pass-, Personalausweisgesetz oder Meldewesen begründet einen öffentlichen Glauben an die Identität der natürlichen Person, so dass diese Identitätsvergabe die höchste Vertrauens- und Sicherheitsstufe bildet und der „Identitätsvergewisserung“[865] dient. Mit dieser staatlichen Identitätsvergabe wird der statische *Idem*-Anteil der personalen Identität umfasst, der nicht verhandelbar ist und sich nur unter den engen Voraussetzungen etwa des Namensrechts oder Transsexuellenrechts ändern lässt.[866] Ebenso wird mit der staatlich erteilten Identität ein Vertrauensmaß geschaffen, welches im elektronischen Rechtsverkehr etwa für Bürgerdienste über den elektronischen Identitätsnachweis gemäß § 18 PAuswG zur Identifizierung und Erteilung von Berechtigungen[867] eingesetzt werden kann. Mit niedrigerem Vertrauensniveau kann die Identitätsvergabe bei der einfachen elektronischen Signatur erfolgen und damit einem anderen Vertrauens- und Sicherheitsniveau unterliegen, EWG 48. Insofern fungiert die identitätsvergebende Institution als akkreditierte *Trusted Third Party* für die innereuropäische Interoperabilität behördlicher Identifizierungen, was die Anerkennung der Zertifikate in den Mitgliedstaaten voraussetzt, Art. 25 Abs. 3 eIDAS-VO. Damit ist für den Zertifikatnutzer der Zugang zu einem innereuropäischen Identifizierungssystem geschaffen, welches zur europaweiten behördlichen Identifizierungsmöglichkeit und Rationalisierung dokumentengeprägter Prozesse beiträgt.[868] Voraussetzung dafür ist eine personale Teilidentität, bestehend aus den Personenidentifizierungsdaten gemäß Art. 3 Nr. 3 eIDAS-VO, mit denen die eindeutige Repräsentation der natür-

865 *Eichenhofer/Gusy*, in: Hornung/Engemann (Hrsg.), Der digitale Bürger und seine Identität, 2016, 65 (67); über das „informationelle Vertrauen“ in der Identitätsverwaltung, vgl. *Warnecke*, Identitätsmanagement und Datenschutz, 2019, S. 59–63.

866 2. Teil, A., II., 1., a).

867 *Hornung/Möller*, Passgesetz, Personalausweisgesetz, 2011, § 18 PAuswG Rn. 8.

868 *Sosna*, CR 2014, 825 (828).

lichen Person möglich wird. Dieses innereuropäische Identifizierungssystem kann um autorisierte privatrechtliche Institutionen erweitert werden, wie es die eIDAS-VO in EWG 13, 17 S. 1 vorsieht. Dies könnte langfristig ein Gegengewicht zu der verbreiteten Identifizierungsmöglichkeit von Intermediären bilden, die ebenfalls identitätsstiftend wirken können und das staatliche Identitätsstiftungsmonopol ignorieren würden.[869] Insofern ist mit der eIDAS-VO für eine grenzüberschreitende Identitätsvergabe eine Stärkung der staatlichen Identitätsstiftung anzunehmen, die sich auf den privatrechtlichen Kontext ausweiten lässt und als ein Beitrag zur Steigerung des Identitätsschutzes in Europa eingeordnet werden kann.

b) Privatrechtliche Identitätsvergabe

Mit der privatrechtlichen Identitätsvergabe durch Intermediäre werden die Funktionen des dienstbezogenen und kontextübergreifenden Identitätszugangs, wie es *Facebook* und *Google* mit *Single Sign-On*-Lösungen ermöglichen, umfasst. Die gebündelte Funktionalität eines kontextübergreifenden Identitätszugangs sieht ebenfalls eine *Trusted Third Party* vor, bei der die personalen Identitäten hinterlegt sind. Als Intermediäre für den privatrechtlichen Kontext kommen ebenso staatlich zugeordnete Institutionen in Betracht, wie die Bundesdruckerei oder die Bundesrechtsanwaltskammer, die kontextspezfische personale Teilidentitäten in Gestalt des Personalausweises mit einer Personalausweisnummer und den Zugang zum elektronischen Anwaltspostfach vergeben können. Diese können über die bloße Identitätsvergabe hinaus mit zertifizierten personalen *Idem*-Teilidentitäten ausgestattet werden, so dass die Einsatzfähigkeit in Kontexten mit einem gesteigerten Vertrauens- und Sicherheitsniveau gewährleistet wird.

Denn die privatrechtliche Identitätsvergabe durch Intermediäre wirft die Frage nach der Umsetzung IT-sicherheitsrechtlicher Standards auf, gerade wenn die Niederlassung außerhalb des Regelungsregimes der Europäischen Union liegt. Insofern sollte die Wahl der Intermediäre zur privatrechtlichen Identitätsvergabe in Verbindung mit dem herrschenden Regelungsregime stehen, so dass die Entscheidung über die Nutzung eines Intermediärs zugleich eine Entscheidung über das maßgebliche rechtliche Schutzregime ist. Damit obliegt der natürlichen Person die Verantwortung, den geeigneten Intermediär zu wählen, der über die spezifischen Plattformen für das jeweilige Vertrauens- und Sicherheitsniveau verfügt

869 *Hornung/Engemann* (Hrsg.), Der digitale Bürger und seine Identität, 2016, S. 16.

und als „*Identity Ecosystem*“ dem Regelungsregime der europäischen Datenschutzgrundverordnung unterliegt.

2. Identitätsvergabe durch den Mediationsagenten

a) Mediationsagent als Software

Die Identitätsvergabe unter der Prämisse einer verhandelten personalen Identität setzt die Offenlegung der personalen *Ipse*-Identität durch den Verantwortlichen voraus, die mit dem Selbstbild der personalen Identität des Betroffenen verhandelt werden sollte. Ein dafür eingesetzter technischer Mediationsagent könnte eine weitere Identität vergeben, die der Verhandlung unterliegt und das Ergebnis eines Aushandlungsprozesses unter spezifischen *Instruktionen* darstellt. Diese verhandelte Identität würde dem Kalkül des Mediationsagenten sowie den Eingabewerten des Verantwortlichen und des Betroffenen über die personale Identität unterliegen. Dabei würde das Kalkül des Mediationsagenten aus den Eigenschaften eines Mediators bestehen, das neutrale und diskriminierungsfreie *Instruktionen* für die Bilder personaler Identitäten ermöglicht. Darüber hinaus kommen inhaltliche Verstärkungs- und Schwächungsmechanismen über Attribute in Betracht, die kontextbedingt hinsichtlich der generierbaren Erkenntnismöglichkeiten gesteuert werden müssten. Damit könnten unerwünschte Wissensgenerierungen, wie sie etwa in § 81g Abs. 2 S. 2 StPO über die Beschränkung der Erkenntnisse aus der DNA geregelt werden, vermieden werden.

Der Mediationsagent würde als Softwareprogramm eingesetzt werden können, welches mit eigener Intelligenz ausgestattet wäre und *Instruktionen* für die Generierung der Bilder personaler Identität enthielte und vollziehen könnte.[870] Dieses müsste als Finalprogramm ausgestaltet sein, bei dem das Entscheidungsergebnis offen ist und das Programm auf der Einbeziehung von Informationen basiert.[871] Insofern würde mit dem Vollzug der Regeln eines Mediationsagenten durch Software gleichzeitig eine Steuerung des Verhaltens ausgelöst werden können, so dass einem technischen Mediationsagenten aus Software eine institutionelle Dimension[872] zukommen würde, sog. „*Code as law*“. In Anbetracht der möglichen recht-

870 5. Teil, C., III.–IV.
871 *Reisinger*, Rechtsinformatik, 2016, S. 99 f.
872 *Orwat/Raabe/Buchmann u.a.*, Informatik Spektrum 2010, 626 (628).

lichen Verankerung eines technischen Mediationsagenten im MedG könnte der Mediationsagent als Legitimationsquelle gegenüber der bisherigen einseitigen Identitätsvergabe fungieren und das Legitimations- und Kontrolldefizit auf der Ebene der Rechtfertigung kompensieren.

b) Mediationsagent als „*Smart Contract*"

Für den Einsatz eines technischen Mediationsagenten könnte die Generierung einer verhandelten Identität mit einem *Smart Contract* erfolgen. Indem *Smart Contracts* eine Streitbeilegungsklausel über einen „*online dispute resolution*"-Mechanismus enthalten können,[873] erscheint eine Verbindung zum technischen Mediationsagenten naheliegend. Dabei könnte das Mikroverfahren eines technischen Mediationsagenten möglicherweise mit einem *Smart Contract* ausgeführt werden.

Grundsätzlich ist dabei die Bezeichnung des *Smart Contracts* missverständlich, denn es handelt sich im Rechtssinne gerade nicht um einen Vertrag, sondern um die automatisierte Durchführung und Durchsetzung eines vorher verhandelten Vertrages.[874] Dies setzt voraus, dass der Vertragsinhalt technisch übersetzt werden kann, was gerade bei der Übersetzung der allgemeinen Geschäftsbedingungen in ein Softwareprogamm[875] naheliegend erscheint und aus der IKT-rechtlichen Perspektive der Übersetzung von Datenschutzerklärungen entsprechen kann. Damit könne die Realisierung der Datenschutzerklärung in der Datenverarbeitung mit der automatisierten Durchführung „garantiert"[876] werden. Dieser Mechanismus des *Smart Contract* könnte etwa durch die Einwilligung ausgelöst werden und zum Vollzug der kontextspezifischen Datenverarbeitungsvorgaben führen.

Gleichwohl erscheint die Verhandlung der personalen Identität mit einem *Smart Contract* fernliegend, da mit diesem die Durchführung von Regeln unter der Prämisse erfolgt, dass es keine inhaltlichen Unbestimmtheiten über die konkrete Darstellung des Bildes personaler Identitäten geben darf. Demnach ist die Funktionalität eines *Smart Contract* für den technischen Mediationsagenten zur Verhandlung von Bildern personaler Identitäten fernliegend und steht dem Erfordernis der Ergebnisoffenheit in der

873 *Kaulartz*, DSRI 2017, 599 (605).
874 *Kaulartz/Heckmann*, CR 2016, 618.
875 *Dies.*, CR 2016, 618 (622); *Wright/Filippi*, Decentralized blockchain technology and the rise of lex cryptographia, 2015, S. 24–26.
876 *Dies.*, CR 2016, 618 (620); *Kaulartz*, DSRI 2017, 599 (601).

Mediation entgegen. Allerdings könnte ein *Smart Contract* für eine automatisierte Verweisung zu einem technischen Mediationsagenten in einem bestimmten Zeitpunkt im Datenzyklus eingesetzt werden, wie es bei der automatischen Verweisung zu einem Streitbeilegungsverfahren mit einem *Smart Contract* möglich ist.

3. Zusammenfassung

Nach den IKT-rechtlichen Vorgaben erfolgt die Identitätsvergabe öffentlich-rechtlich und privatrechtlich. Die öffentlich-rechtliche Identitätsvergabe kann aufgrund ihrer Funktionalität der Identitätsvergewisserung und des öffentlichen Glaubens im Rechtsverkehr nicht verhandelbar sein. Demgegenüber sind die vergebenen personalen Identitäten durch die privatrechtlichen Institutionen faktisch ebenfalls nicht verhandelbar, wenngleich das Interesse an der Identitätsvergewisserung bei Intermediären aufgrund des Vorrangs der Datenverarbeitungen geringer ausgeprägt sein dürfte. Indem der institutionellen Identitätsvergabe keine Identitätsvergabe durch den Betroffenen – mit Ausnahme der Einwilligung – gegenübergestellt wird, bedarf es für einen Ausgleich der Interessenlagen zwischen dem Verantwortlichen und Betroffenen der Identitätsvergabe durch einen technischen Mediationsagenten. Dieser könnte mit Software gestaltet werden, die die formalisierten Verfahrensprinzipien der Mediation enthalten würde und in inhaltlicher Hinsicht ergebnisoffen ausgestaltet wäre. Dabei müsste der technische Mediationsagent über *Instruktionen* verfügen, die eine neutrale und diskriminierungsfreie Generierung der Bilder personaler Identitäten ermöglicht. Für eine Schwerpunktverlagerung von der bloßen Identitätsvergabe hin zu einer verhandelten Identität könnte ein softwarebasierter technischer Mediationsagent für die Identitätsverwaltung im privatrechtlichen Kontext als Institution wirken.

III. Paradigmenwechsel zur dezentralen Identitätsverwaltung

Der dynamische Identitätsbegriff und das Konzept einer kontextspezifischen Identitätsverwaltung verlangen eine dezentrale Identitätsverwaltung, die es ermöglicht, zwischen verhandelbaren und nicht verhandelbaren personalen Identitäten zu differenzieren. Da es jeweils um die Darstellung des Bildes einer personalen Identität geht, führt eine *kontextspezifische Identitätsverwaltung* zu einer pluralisierten Verteilung der personalen Teilidenti-

täten, die der jeweiligen Verwaltung bedürfen. Demnach erscheint aus der Gesamtbetrachtung, die dezentrale Ausgestaltung der Identitätsverwaltung dem *Idem*- und den *Ipse*-Anteilen der personalen Identität in einem Datenzyklus gerecht zu werden. Auch kann damit der Lebenszyklus spiegelbildlich in dem Datenzyklus der personalen Identität abgebildet werden. Dies würde bei einem zentralisierten Konzept, das aus *einer* „digitalen Identität" besteht, kaum mit dem grundrechtlichen und fachübergreifenden Identitätsbegriff vereinbar sein, weil darin das differenzierte Vertrauens- und Sicherheitsniveau nicht aufgehen würde. Vielmehr liegt darin eine Zentrierung und Beschränkung auf den Namen als *Idem*-Anteil der personalen Identität, was dem hier vertretenen Identitätsbegriff nicht entspricht.

Für ein dezentrales Identitätsverwaltungsmodell spricht weiter, dass bereits im Volkszählungsurteil die Dezentralisierung von Datenspeicherungen als verfassungsrechtliches Gebot vorgetragen wurde.[877] Denn bei einem Angriff auf die Datenspeichersysteme würde das Risiko für die Datensicherheit deutlich geringer ausfallen, als wenn ein Angriff gegenüber einer *Trusted Third Party* mit sämtlichen Datensätzen einer personalen Identität erfolgt. Ferner ermöglicht die dezentrale Identitätsverwaltung die *iterative Kontrolle* personaler Teilidentitäten in ihrem *Ipse*-Anteil in systemischer Hinsicht, da die natürliche Person die Kontrolle im Laufe des Datenzyklus für den jeweiligen Kontext ausüben und das Bild der personalen Identität gestalten könnte. Mit einem dezentralen Identitätsverwaltungsmodell könnte die natürliche Person durch kontextspezifische Transparenz und damit verbundene Kontrollmöglichkeiten gestärkt werden. Für eine nähere Analyse des dezentralen Identitätsverwaltungsmodells sollen im Einzelnen das treuhänderische Konzept (1.) und die Blockchain (2.) als mögliche Lösungsmechanismen untersucht werden.

1. Treuhänderische Identitätsverwaltung

Die treuhänderische Identitätsverwaltung lässt sich zwischen einer zentralen *Trusted Third Party* und einem dezentralen System einordnen. Denn das Treuhandkonzept würde die Verwahrung der personenbezogenen Daten vorsehen, ohne ein wirtschaftliches Interesse zu verfolgen. So wird als Datentreuhand von *Kühling/Sackmann* eine Pseudonymisierungsinstanz vorgeschlagen, die als Stellvertreter der Verbraucher eingesetzt werde und die Verwaltung des Personenbezugs der Daten mit dem damit verbunde-

877 BVerfGE 65, 1 (19).

nen Risiko der Identifizierbarkeit ermögliche.[878] Die Neutralität und Unabhängigkeit des Datentreuhänders wäre dabei entscheidend, um mit dem Treuhänder keine weitere Risikoquelle über den Schutz der informationellen Selbstbestimmung zu schaffen. Weiter wird eine treuhänderische Lösung auch von *Hermstrüwer* vorgeschlagen, wonach neben der Rechtfertigung zwischen dem Verantwortlichen und Betroffenen eine Treuhandabrede darüber geschlossen werden könnte, dass die personenbezogenen Daten gewinnbringend eingesetzt werden sollen und eine entsprechende Auszahlung an den Betroffenen zu erfolgen hätte.[879] Ferner schlägt die Kommission Wettbewerbsrecht 4.0 für die betroffenen Personen einen selbstgewählten Datentreuhänder vor, mit dem die Bereitstellung der personenbezogenen Daten organisiert werden kann.[880] Ebenso wird als Treuhand ein „*Digital Clearinghouse*" von dem europäischen Datenschutzbeauftragten (EDPS) angeführt, mit dem Verbraucher- und Wettbewerbsfragen vereinigt und der natürlichen Person zur Rechtsdurchsetzung verholfen werden soll.[881] Schließlich wird von *Drexl* eine Agentenstruktur vorgebracht, die den Verbraucher mit dem Verantwortlichen bei umfangreichen und dynamischen Datensätzen zusammenbringen soll und so der Zugang zu den Datensätzen mit den Privatheitseinstellungen durch den Betroffenen kontrolliert werden könne.[882]

Auch wenn in einer treuhänderischen Konstruktion eine Alternative zur *Trusted Third Party* liegen kann, besteht dennoch eine strukturelle Parallele zu dieser. Denn bei einem Angriff auf die IT-Sicherheit der Treuhand kann der Schaden für die informationelle Selbstbestimmung erheblich sein, so dass die treuhänderische Konstruktion in Nischenbereichen naheliegender erscheint.[883] Weiter setzt eine treuhänderische Konstruktion voraus, dass der Betroffene den Zugang und die Einstellungen kontrollieren kann, womit das Risiko des Kontroll-Paradoxons seine Wirkung entfaltet und die vermeintliche Kontrolle über den kontextbezogenen Zugang zu einer bereitwilligen Offenlegung personenbezogener Daten führt.

Insgesamt würde es sich bei der treuhänderischen Konstruktion ebenfalls um einen Mediator auf der Makroebene handeln, der unabhängig und neutral zwischen dem Verantwortlichen und dem Betroffenen einge-

878 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 17.
879 *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, S. 139 f.
880 *Kommission für Wettbewerbsrecht 4.0*, Bericht, S. 43 f.
881 www.edps.europa.eu/data-protection/our-work/subjects/big-data-digital-clearinghouse_de (zuletzt aufgerufen 20.06.2020).
882 *Drexl*, JIPITEC 2017, 257 (275) Rn. 88; *Bernau*, FAS vom 10.02.2019, 23.
883 *Kühling/Sackmann*, Rechte an Daten, 20. November 2018, S. 18.

setzt wird. Insoweit kann das *Dashboard-System* zum Bestandteil einer treuhänderischen Konstruktion werden, damit der Zugang zu den personalen Identitäten und die Transparenz über die kontextspezifischen Bilder der Teilidentitäten gewährt werden. Dabei müsste ein Gleichgewicht zwischen einer absoluten Kontrolle in Gestalt des Zugangs und dem Kontroll-Paradoxon hergestellt werden. Ein solches *Dashboard-System* könnte den Zugang, die Bilder personaler Identitäten und den technischen Mediator umfassen, der von dem Verantwortlichen oder einem Dritten eingesetzt werden könnte. Dabei sollte der Dritte keine wirtschaftlichen Eigeninteressen verfolgen. Ebenfalls ließe sich an eine Zertifizierung eines solchen *Dashboard-Systems* mit einem technischen Mediator gemäß Art. 42 DSGVO denken, was sich auf eine positive Reputation und damit auf das Marktverhalten des Betroffenen und des Verantwortlichen auswirken könnte. Schließlich kommt die Anknüpfung an einen bestimmten Schwellenwert über den Datenverarbeitungsumfang in Betracht, der dazu verpflichten könnte, ein *Dashboard-System* einzuführen.

2. Identitätsverwaltung in der Blockchain

Für die dezentrale Identitätsverwaltung lässt sich die Blockchain einsetzen. Die Blockchain ist eine Ausprägung der „*Distributed Ledger Technologie*" und löst einen zentralen Intermediär ab, indem eine koordinierte und dezentrale Speicherung der Datensätze erfolgt. Es handelt sich dabei um eine Technologie, die aus einer Kombination von „*Peer-to-Peer-network*" und Kryptographie besteht. Daher wird der Blockchain aus ökonomischer Perspektive ein institutioneller Charakter zugeschrieben,[884] der für den Anwendungsbereich der Identitätsverwaltung maßgeblich sein könnte. Denn die Blockchain ermöglicht eine interoperable, dezentrale Datenverarbeitung und stellt gleichzeitig die Authentizitität über die Datensätze sicher, weshalb sie als Technologie für die Identitätsverwaltung in Frage kommt. Demnach soll die Funktionsweise der Blockchain (a) aufgezeigt und ihr Einsatz bei der Identitätsverwaltung (b) diskutiert werden.

884 *Davidson/Filippi/Potts*, Journal of Institutional Economics 2018, 639.

a) Funktionsweise der Blockchain[885]

Die Blockchain besteht aus „*Nodes*“[886], in denen die Eingabe des Wertes durch ein Individuum vorgenommen wird. Dieser Eingabewert wird in einem Datenblock („*Block*“) dezentral repliziert und synchronisiert, was zur allgemeinen Transparenz des Datensatzes in den jeweiligen „*Nodes*“ führt. Gleichzeitig erscheint der Datensatz als umgerechneter Hashwert, dem verschlüsselten Datensatz, der mit einem Zeitstempel versehen ist, womit sich der Hashwert in eine zeitliche Reihenfolge gegenüber anderen Hashwerten setzen lässt. Diese in einer festen Reihenfolge miteinander verbundenen Datenblöcke bilden eine Kette, sog. „*chain*“, die nur erweitert werden kann und damit irreversibel ist.[887] Die Entstehung der Kette verlangt das „*hashing*“ und „*rehashing*“, welches den „*Proof of Work*“ darstellt und eine hohe Rechenleistung verlangt.[888] Demgegenüber kann die kostenintensive hohe Rechenleistung mit einer Technologie ohne den „*Proof of Work*“ reduziert werden, indem der Vorgang des „*hashing*“ und „*rehashing*“ auf den „*Proof of Stake*“ beschränkt wird, ohne dass die vorangegangenen Eingabewerte in die Rechenoperation einbezogen werden, so dass der Rechenleistungsaufwand geringer wird.[889] Insgesamt wird mit der Blockchain die allgemeine Transparenz, verteilt auf die „*Nodes*“, gewährleistet und mit der Bildung des Hashwertes ein Schutzmechanismus gegen

885 Vgl. *Steinbrück*, in: Schweighofer/Kummer/Saarenpää (Hrsg.), Tagungsband, IRIS 2019, 2019, 283.

886 *Wattenhofer*, The science of the blockchain, 2017, S. 5, Definition: „We call a single actor in the system node“; historisch ging es darum, das byzantinische Problem zu lösen, wonach ein *Node* sich inkorrekt verhält etwa mit der Sendung eines korrumpierten Datensatzes. Wenn in einem Netzwerk durch ein Quorum aller Nodes ein Gleichlauf hergestellt wird, würde dieses byzantinische *Node* überstimmt werden können, was mit dem Paxos-Algorithmus ermöglicht wird.

887 *Peck*, IEEE Spectrum 54 (2017), 26.

888 *Ders.*, IEEE Spectrum 54 (2017), 26 (27, 32 f.); *Wattenhofer*, The science of the blockchain, 2017, S. 83. Hinsichtlich der hohen Rechenleistung und des Energieverbrauches werden daher Alternativen diskutiert, etwa „*Hashgraph*“.

889 Ein System ohne den Proof of Work bildet „*Hashgraph*“; *Luu/Teutsch/Kulkarni u.a.*, in: Ray/Li/Kruegel (Hrsg.), CCS'15, 2015, 706 (706–708): Mit dem sog. „*Verifier Dillema*“ kann die hohe Rechenleistung in Frage gestellt werden. Denn nach der bisherigen Konstellation müssen die Miner eine Transaktion verifizieren, jedoch kann diese Verifizierung ausbleiben und der Rechenaufwand wird geringer.

die Manipulation des Datensatzes geschaffen, wodurch ein Vertrauensanker gebildet wird.[890]

Die Blockchain wird in eine öffentliche und private Blockchain differenziert. Die Unterscheidung richtet sich danach, ob der Zugang zu der Blockchain für einen beschränkten Nutzerkreis besteht und einer Erlaubnis bedarf oder der Zugang für jeden eröffnet wird. Für die kontextbezogene Identitätsverwaltung erscheint eine private Blockchain mit einem beschränkten Nutzerkreis als eine potentielle technische Lösung zur Realisierung eines „*privacy by design*"-Konzeptes[891]. Indem die Blockchain auf die Sicherstellung der allgemeinen Transparenz und der Irreversibilität von Datensätzen abstellt, könnte sie für die Kontexte einer statischen personalen Identität dann eingesetzt werden, wenn der Bedarf nach dem öffentlichen Glauben besteht, wie es etwa bei Grundbucheintragungen der Fall ist. Gleichzeitig ermöglicht die Blockchain die wiederkehrende Erneuerung von Erkenntniswerten mit dem jeweiligen „*Update*" das Hashwertes, wobei die redundante Speicherung der Hashwerte erwünscht sein müsste.

b) Personale Identität in der Blockchain

Sobald die Identitätsverwaltung in der Blockchain erfolgt, bedarf es der Bestimmung eines Datensatzes, der in einen Hashwert umgewandelt werden soll. Dabei kommen die Speicherung einer personalen Identität, die Speicherung spezifischer Attribute, die Speicherung der Einwilligung oder die Speicherung eines Zugangsrechts in der Blockchain in Betracht.

Es wird für eine Identitätsverwaltung unter Einbeziehung der elektronischen Identifizierung nach der eIDAS-VO die Speicherung von Identitätsattributen („*Identifier*") mit der Einwilligung im Hashwert vorgeschlagen.[892] Diese sollte mit einer elektronischen Signatur als Hashwert verschlüsselt werden, was über die ISÆN-App erfolgen könnte. Nach dem ISÆN-Konzept wird mit dem Hashwert, in dem die Einwilligung gespeichert ist, eine gezielte Authentifikation für den privaten Sektor möglich,

---

890 *Peck*, IEEE Spectrum 54 (2017), 26 (28). Danach wird zunächst auf Bitcoin Bezug genommen mit einem Ausblick auf weitere Anwendungen etwa den Kontext *Social Media.*

891 *Bechtolf/Vogt*, ZD 2018, 66 (71).

892 *Smart Data Begleitforschung*, Sicheres Identitätsmanagement im Internet, 2017, S. 37; demgegenüber setzt das estländische e-Residency Programm die Blockchain Technologie für die Authentifizierung und Verifikation ein, vgl. *Sullivan*, CLSR 2018, 723 (727).

wobei der Hashwert aufgrund der Verschlüsselung als anonymes Datum eingeordnet wird.[893] Dagegen lässt sich einwenden, dass mit der Verschlüsselung durch den Hashwert zwar die Identifizierbarkeit deutlich erschwert wird, aber im Sinne des objektiviert-relativen Ansatzes die Identifizierbarkeit einer natürlichen Person nicht ausgeschlossen ist.[894] Dies gilt besonders, weil der „*Public Key*" für die Verschlüsselung als personenbezogene Daten zu qualifizieren ist. Um einen angemessenen Schutz für die informationelle Selbstbestimmung zu gewährleisten, wird der Annahme von anonymen Daten in der Blockchain nicht gefolgt. Sobald diese als anonyme Daten eingeordnet werden, würden die Grundsätze der Datenverarbeitung nach der DSGVO nicht mehr gelten, obwohl das Risiko der Identifizierbarkeit etwa aus den Metadaten bei der Verwendung der Blockchain besteht und der Personenbezug hergestellt werden kann.[895]

Die personenbezogenen Daten können auch in der „*off-chain*" gespeichert werden, womit der Hashwert in jedem Fall als anonym einzustufen wäre und die datenschutzrechtlichen Anforderungen für die Blockchain nicht gelten würden.[896] Demnach ist für einen datenschutzkonformen Einsatz der Blockchain diese als Dienst im Sinne eines „*Blockchain as a Service*" (BaaS) denkbar, so dass die Funktionsweise der Blockchain außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen könnte.[897]

Darüber hinaus würde die Speicherung der Identitätsattribute mit der Einwilligung in der Blockchain datenschutzrechtlich fragwürdig sein, da in einem dezentralen Speicherungssystem die Datenminimierung und das Recht auf Vergessenwerden umzusetzen wären. Für die Wahrung des Grundsatzes der Datenminimierung könnte zwar argumentiert werden, dass die DSGVO auf zentrale Strukturen ausgerichtet sei und eine angepasste Auslegung auf dezentrale Strukturen verlangt, so dass die Verschlüsselung im Hashwert eine ausreichende Umsetzung der Datenminimierung darstelle, Art. 5 Abs. 1 c), 4, Nr. 5 DSGVO. Jedoch erscheint diese Ausle-

893 *Smart Data Begleitforschung*, Sicheres Identitätsmanagement im Internet, 2017, S. 34.

894 *Finck*, EDPL 2018, 17 (25).

895 *Dies.*, EDPL 2018, 17 (22). Eine Ausnahme wird dann gesehen, wenn der Hashwert sich über eine sog. Einwegfunktion bilden lässt. Für diesen Fall könne der Hashwert als anonymes Datum eingeordnet werden; als Metadaten kommen die Verkehrs- und Standortdaten, die eine eigene personale Teilidentität bilden können, in Betracht.

896 *Dies.*, EDPL 2018, 17 (22).

897 *Dies.*, EDPL 2018, 17 (27 f.); *Kulhari*, Building-blocks of a data protection revolution, 2018, S. 22.

gung der Datenminimierung zu weitgehend und es steht vielmehr eine Anpassung der DSGVO an dezentrale Technologien im Raum. Hinsichtlich des Rechts auf Vergessenwerden würde sich die Umsetzung gemäß Art. 17 Abs. 2 DSGVO auf die „Berücksichtigung der verfügbaren Technologie" beschränken und steht gemäß § 35 Abs. 1 BDSG unter dem Verhältnismäßigkeitsvorbehalt, so dass für die rechtskonforme Umsetzung das Löschen des Datensatzes nicht zwingend erforderlich ist. Folglich könnte nach der Geltendmachung des Rechts auf Vergessenwerden der Block um einen weiteren Block mit dem Inhalt erweitert werden, dass die Blockchain bis zu einem bestimmten Zeitpunkt „falsch" sei. Zwar wird damit ein eigener neuer Erkenntnisgehalt begründet, aber zumindest könnte auf diesem Weg der Neubeginn einer personalen Teilidentität ermöglicht werden. Ebenso könnte das Recht auf Berichtigung gemäß Art. 16 DSGVO durch Hinzufügung einer weiteren „*chain*" realisiert werden, so dass auch hier eine der Blockchain angepasste Lösung denkbar wäre.[898]

Insgesamt lässt sich diesen Lösungsmöglichkeiten entgegenhalten, dass die Realisierung der Identitätsverwaltung in der Blockchain mit erheblichen rechtlichen Risiken verbunden ist. Weiter konterkariert sich die Zielrichtung der Blockchain, einen hohen öffentlichen Glauben und Transparenz zu schaffen, mit dem Ziel der Identitätsverwaltung, unter Wahrung der Datenminimierung und Sicherstellung eines dynamischen Identitätsbegriffs umgesetzt zu werden. Demnach erscheint die Verbindung zwischen Identitätsverwaltung und Blockchain nach den bekannten technischen Lösungsmöglichkeiten als Konstruktion, ohne derzeit ein rechtskonformes Konzept der Blockchain als „*privacy by design*"-Lösung abbilden zu können.

Für die Blockchain spricht jedoch, dass mit ihr die Kontrolle über die Datensätze in den Hashwerten und eine grenzüberschreitende, dezentrale und interoperable Datenverarbeitung ermöglicht wird. Gleichwohl ist sie als Technologie für die privatheitsschützende Identitätsverwaltung bislang mit der DSGVO schwerlich in Einklang zu bringen, jedoch nicht vollständig abzulehnen. Etwa kommt eine private Blockchain in einem Unternehmen in Betracht, das über ein eigenständiges und separiertes Schutzregime verfügt. Weiter kommen für die spezifischen Anforderungen der Identitätsverwaltung technische Anpassungen bei der Gestaltung der Blockchain in Frage, mit denen sich die datenschutzkonforme Umsetzung vornehmen

898 *Dies.*, EDPL 2018, 17 (29 f.); ebenso den Modizierungsbedarf des Rechts auf Vergessenwerdens anerkennend, vgl., *Kulhari*, Building-blocks of a data protection revolution, 2018, S. 42–45, 52.

lässt. Ebenso ist die Anpassung der DSGVO auf dezentrale Technologien und dezentrale verantwortliche Stellen denkbar.

3. Zusammenfassung

Die Identitätsverwaltung über ein Treuhandsystem kann eine Alternative zu der Identitätsverwaltung mit einer zentralen *Trusted Third Party* darstellen, wenn die Treuhand neutral und ohne wirtschaftliche Interessen zum Einsatz käme. Denn die treuhänderische Konstruktion birgt die Chance, dass die umfangreiche Datenverarbeitung zur Auszahlung eines Geldbetrages führen und die Transparenz über die Bilder personaler Teilidentitäten hergestellt werden könnte. Insoweit wäre ein *Dashboard-System* ein Konzept, mit dem eine treuhänderische Identitätsverwaltung erfolgen könnte. Gleichwohl bündelt ein treuhänderisches Konzept ebenfalls die personalen Teilidentitäten, so dass bei einem Angriff auf die IT-Sicherheit der Treuhand ebenso ein erhebliches Risiko für den Schutz der informationellen Selbstbestimmung besteht. Demnach bedarf es der Verlagerung des Betrachtungsschwerpunktes auf eine dezentrale Identitätsverwaltung.

In technologischer Hinsicht kommt dafür die Blockchain in Betracht, dahingehend, dass mit ihr die personalen Teilidentitäten dezentral gespeichert und kontrolliert werden können. Gleichwohl konnte bei einer Identitätsverwaltung mit der Blockchain nachgewiesen werden, dass erhebliche Rechtsunsicherheiten über die Eröffnung des datenschutzrechtlichen Anwendungsbereiches und der Umsetzung der Betroffenenrechte bestehen. Daher sind technische Konzepte, in denen die Blockchain zwar eingesetzt wird, aber die Identitätsattribute und personalen Teilidentitäten in der „*off-chain*“ gespeichert werden, bislang vorzugswürdig. Weiter erscheint technologieunabhängig die Transparenz über die bestehenden Bilder personaler Identitäten notwendig, wobei die Datenverarbeitungen entsprechend zum Datenzyklus personaler Identitäten dezentral erfolgen sollten. Damit kann den kontextbezogenen IT-sicherheitsrechtlichen Anforderungen entsprochen und das gestufte Vertrauens- und Sicherheitsniveau gemäß Art. 8 Abs. 2 eIDAS-VO über die jeweiligen Teilidentitäten realisiert werden.

IV. Zwischenergebnis

Ein Modell für die Identitätsverwaltung setzt voraus, dass die Kontrolle über die personalen Identitäten mit dem Zugang zu den Identitäten sichergestellt wird. Folglich bedarf es eines Zugangskonzeptes zu den personalen Identitäten und der Verhandlungsfähigkeit von Bildern personaler Teilidentitäten in den jeweiligen Kontexten, was über ein *Dashboard-System* erfolgen sollte. Ein derartiger Identitätszugang lässt sich aus dem Transparenzgebot gemäß Art. 12 DSGVO und dem Auskunftsrecht als Zugangsrecht gemäß Art. 15 DSGVO ableiten. Eine bislang ungeregelte Voraussetzung ist, dass mit dem Zugang die Transparenz über die personale Identität durch den Verantwortlichen hergestellt werden müsste. Dafür könnte von einer Treuhand das *Dashboard-System* zur Verfügung gestellt werden, mit dem die Transparenz zu der personalen Teilidentität hergestellt wird. Dieses *Dashboard-System* würde in struktureller Hinsicht einem Mediator entsprechen, der die personale Identität in ihrer statischen *Idem*- und dynamischen *Ipse*-Dimension unterteilt und mit dem Zugang zu den personalen Identitäten die Verhandlung der Bilder personaler Identitäten ermöglicht.

Die Verhandlung würde auf der Mikroebene mit dem technischen Mediator erfolgen, der aus Software besteht und über *Instruktionen* für die ergebnisoffene Verhandlung der Bilder personaler Identitäten verfügt. Dabei würden die *Instruktionen* aus den formalisierten Verfahrensprinzipien der Mediation bestehen, damit die Generierung der Bilder personaler Identität unter rechtlichen Schutzvorgaben und nicht willkürlich erfolgt. Dies ermöglicht eine kontextbezogene Pluralität der Bilder personaler Identitäten, was zugleich der *iterativen* Identitätsverwaltung im Rahmen des Lebenszyklus dienen würde.

Insgesamt bedarf es auf der Makroebene eines dezentralen Identitätsverwaltungskonzeptes, bei dem die treuhänderische Lösung eines *Dashboard-Systems* als vorzugswürdig herausgearbeitet wurde. Daneben erscheint die Blockchain als dezentrale Technologie für die Identitätsverwaltung ebenso naheliegend, würde aber nach derzeitiger Rechtslage entweder als private Blockchain oder in der „*off-chain*" in Betracht kommen. Die dezentrale Identitätsverwaltung verlangt, dass kontextspezifische Vertrauens- und Sicherheitsanforderungen etwa nach den *drei Stufen* gemäß Art. 8 Abs. 2 eIDAS-VO umgesetzt werden, damit die *kontextuelle Integrität* der personalen Identität in ihren *Idem*- und *Ipse*-Anteilen gewährleistet wird.

C. Ergebnis: Dezentraler Zugang zur verhandelten Identität

Ein Modell der Identitätsverwaltung soll die *kontextuelle Integrität* der personalen Identität gewährleisten. Der Komplexität des realen Individuums wird in einem IKT-System entsprochen, wenn neben dem statischen *Idem*-Anteil der personalen Identität der dynamische *Ipse*-Anteil ebenso kontrollierbar wird. Voraussetzung dafür ist der Perspektivwechsel weg von einem statischen Berechtigungskonzept hin zum Zugang zur personalen Identität und zu der Verhandlungsfähigkeit der Bilder personaler Identitäten. Somit bedarf es der *iterativen Kontrollmöglichkeit* in einem Identitätsverwaltungsmodell, welches den absoluten Zugang der personalen Identität und die relative Verhandlungsfähigkeit der Bilder personaler Identitäten ermöglicht. Die Modellvoraussetzung der Iteration wurde auf der Miko- und Makroebene der mediativen Identitätsverwaltung nachvollzogen.[899]

Auf der Mikroebene bedarf es eines technischen Mediationsagenten, der die Verhandlungsfähigkeit der Bilder personaler Identitäten gewährleistet und über *Instruktionen* für die Generierung der Bilder personaler Identitäten verfügt. Diese sollten als Software ausgestaltet werden und aus den Verfahrensgrundsätzen der Mediation bestehen, damit ergebnisoffene und diskriminierungsfreie Bilder personaler Identitäten generiert werden können. Dazu gehört, dass die Erkenntnismöglichkeiten über die Bilder personaler Identitäten von den *Instruktionen* abhängen, indem allein die rechtlich zulässigen Bilder personaler Identitäten generiert werden sollen. Darin liegt eine Verschiebung des Blickwinkels auf den Schutz des dynamischen *Ipse*-Anteils einer personalen Identität, der zum Gegenstand der relativen Kontrolle des Betroffenen und Voraussetzung für das Identitätsverwaltungsmodell wird.[900]

Auf der Makroebene bedarf es der Gewährleistung eines kontextbezogenen Vertrauens- und Sicherheitsniveaus, welches dezentral und treuhänderisch mit einem *Dashboard-System* ausgestaltet sein sollte. Dieses dient dem Zugang zu den personalen Identitäten als absolute Kontrolle und der damit verbundenen Verhandlungsfähigkeit der Bilder personaler Identitäten als relative Kontrolle. Daneben kommt die dezentrale Identitätsverwaltung über die Blockchain in Betracht, die jedoch mit der derzeitigen Rechtslage der DSGVO schwerlich in Einklang zu bringen ist. Vielmehr kommt die Blockchain als Lösung in Betracht, wenn die personalen Identitäten in der „*off-chain*" gespeichert werden. Weiter verlangt der *Ipse*-Anteil einer perso-

899 6. Teil, B., I., II., 1.
900 6. Teil, B., II., 2.

nalen Identität, dass die technische Lösung eine dynamische Anwendung erlaubt. Diese lässt sich mit der Blockchain und den statischen Hashwerten kaum realisieren. Ebenso wird mit einem *Smart Contract* allein ein statisches Ergebnis generiert, was keine adäquate Lösung für die Identitätsverwaltung bilden würde. Somit kommt ein Intermediär in Frage, der die kontextbezogene Identitätsverwaltung mit spezifischen Plattformen für das jeweilige Vertrauens- und Sicherheitsniveau ermöglicht und damit ein „*Identity Ecosystem*" begründet. Folglich würde dem Individuum mit der iterativen Identitätsverwaltung über den Datenzyklus hinweg eine Kontrollmöglichkeit im Rahmen des Selbstdatenschutzes eingeräumt werden.[901]

901 6. Teil, B., III.

7.Teil: Gesamtergebnis

Es wurde ein Identitätsverwaltungsmodell begründet, welches die personale Identität im online-Kontext im Gleichlauf zum offline-Kontext schützen soll. Dafür wurde die Identitätsverwaltung in IKT-Systemen zunächst stipulativ als die Kontrolle einer natürlichen Person über die Begründung und Annahme von personalen Teilidentitäten definiert. Dies führte zu der Differenzierung zwischen einem statischen *Idem*-Anteil und einem dynamischen *Ipse*-Anteil der personalen Identität,[902] die gleichermaßen in das Identitätsverwaltungsmodell einbezogen wurden. Der Schutz dieser Anteile der personalen Identität unterliegt nach dieser Untersuchung der abwehrrechtlichen Dimension des Kombinationsgrundrechts gemäß Art. 7, 8 GRC, was die informationelle Selbstbestimmung der natürlichen Person über die Verwendung der personenbezogenen Daten umfasst.[903] Ebenso wurde das Konzept der Kontrolle über personale Identitäten aus dem allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG abgeleitet, wenn die innere Dimension der Persönlichkeitsentwicklung und die äußere Dimension der Selbstdarstellung auch in ihrem Gewährleistungsgehalt geschützt werden. Dabei wurde die kommunikative Dimension des allgemeinen Persönlichkeitsrechts herausgearbeitet, was sich in dem Recht auf informationelle Selbstbestimmung konkretisiert und den Schutz der Informationen und Erkenntnismöglichkeiten über eine personale Identität umfasst. Weiter lässt sich der datenbasierte Lebenszyklus einer personalen Identität mit dem *Recht auf Neubeginn* zeitlich beschränken, was seine einfachrechtliche Ausprägung im Recht auf Vergessenwerden gemäß Art. 17 DSGVO findet und die grundrechtliche Anforderung der Kontrolle über personale Teilidentitäten verdeutlicht.[904] Darin kommen die zeitgebundene und kontextspezifische Dynamik der personalen Identität in ihren *Idem*- und *Ipse*-Anteilen zum Ausdruck, die vom grundrechtlichen Schutz umfasst sind.

Weiter wurden auf dieser Basis die Anforderungen an die Identitätsverwaltung konkretisiert, indem einfachrechtliche Typologien als Grundlage für die Modellbildung herangezogen wurden. Dazu gehörten zunächst das

902 1. Teil, C., II., 2.
903 2. Teil, A., I.
904 2. Teil, A., II., 1.

Namensrecht und im elektronischen Rechtsverkehr die Signatur, die jeweils an den *Idem*-Anteil der personalen Identität anknüpfen. Demgegenüber konnte der dynamische *Ipse*-Anteil personaler Identitäten im elektronischen Rechtsverkehr mit der vertraulichen und sicheren Kommunikation über das De-Mail-G abgebildet werden.[905] Diese Ausprägungen der personalen Identität bedürfen in einem Identitätsverwaltungsmodell der Kontrolle, die in eine absolute Kontrolle über den Zugang zur personalen Identität und in eine relative Kontrolle über das Bild der personalen Identität differenziert wurde.[906] Insoweit kommt es bei dem Identitätsverwaltungsmodell darauf an, dass eine Kontrollierbarkeit über die Erkennntnisse zu einer personalen Identität geschaffen wird.[907] Diese Anforderungen an ein Identitätsverwaltungsmodell wurden auf das IKT-Recht übertragen.

Demnach sollte die soziotechnische Kontrollierbarkeit der personalen Identitäten mit ihren *Idem*- und *Ipse*-Anteilen über den Datenzyklus hinweg im IKT-Recht nachvollzogen werden. Dafür wurde die Identitätsverwaltung im Datenschutzrecht chronologisch *ex ante* zur Rechtfertigung, der Rechtfertigung und *ex post* zur Rechtfertigung abgeleitet. Es konnte nachgewiesen werden, dass für die Kontrolle durch den Betroffenen zunächst die Informationspflichten maßgeblich sind und der Bedarf nach Transparenz über die Risiken der Datenverarbeitung besteht.[908] Weiter dient die rechtfertigende Einwilligung ebenfalls der Kontrolle von personalen Identitäten, so dass die Einwilligungsentscheidung einer differenzierten Analyse unterlag und in Anbetracht der hohen Einwilligungsbereitschaft („*digital unconscious*“) auf verhaltensökonomische Verzerrungsfaktoren untersucht wurde.[909] Dabei wurde ein legitimatorisches Defizit über die Rechtfertigungswirkung der Einwilligung und der Rechtfertigung ohne aktive Handlung bei der Begründung personaler Identitäten festgestellt, welches zu einem Kompensationsbedarf mit den Betroffenenrechten führt.[910] Da jedoch die Betroffenenrechte nicht immer umfassend wahrgenommen werden, konnte eine umfassende Kompensation schwerlich angenommen werden.[911]

Ferner konnten in online-Kontexten die personalen Teilidentitäten, basierend auf den Bestands-, Nutzer-, Standort- und Verkehrsdaten, aufzei-

905 3. Teil, A., I., II.
906 3. Teil, C.
907 3. Teil, B., D.
908 4. Teil, B., II.
909 4. Teil, B., II.
910 4. Teil, C., II., III.
911 4. Teil, D.

gen, dass sie einen eigenständigen Erkenntnisgehalt über die personale Identität ermöglichen.[912] Für die Kontrolle dieser personalen Teilidentitäten wurde der Bedarf nach einem Identitätszugang im Rahmen der Informationspflichten und des Auskunftsrechts gemäß Art. 12, 15 DSGVO und der damit verbundenen Gewährleistung der *kontextuellen Integrität* von personalen Teilidentitäten abgeleitet. Ein Gesamtüberblick sollte dabei mit einem *Dashboard-System* geschaffen werden, denn darin liegt die Grundlage für ein Konzept des *„identity management by design"*[913].

Bei einem Ausgleich des Legitimationsdefizits gegenüber der informationellen Selbstbestimmung stellt sich die Frage nach einem kompensatorischen Mechanismus über die Betroffenenrechte hinaus. Dafür konnte mit der spieltheoretischen Modellierung eine weitere Perspektive eingeführt werden, mit der die datenschutzrechtliche Konstellation im Hinblick auf das Strategieverhalten der Spieler des Verantwortlichen und des Betroffenen untersucht wurde. Nach dieser spieltheoretischen Modellierung richtet sich das Strategieverhalten nach den bestehenden Informationsständen und den erzielbaren Auszahlungswerten. Wenn dabei das öffentliche Gut der persönlichen Informationen als „Verhandlungsmasse" im Zentrum des Strategieverhaltens steht, bedarf es zum Schutz des öffentlichen Gutes der persönlichen Informationen eines möglichst schonenden Strategieverhaltens.[914] Dieses liegt in der kooperationsfördernden *TIT for TAT*-Strategie, die mit den Verfahrensprinzipien der Mediation begünstigt wird und das Potential zu einer dominierenden Strategie hat. Mit dem Mediationsverfahren wird dieser Rahmen geschaffen, in dem die Bilder personaler Identitäten unter den *Instruktionen* der Verfahrensprinzipien im „Schatten des Rechts" verhandelbar werden.[915] Denn es konnte ein Konflikt zwischen dem Verantwortlichen und Betroffenen über den Schutz der persönlichen Informationen nachgewiesen werden, der einer Intervention bedarf. Diese Intervention wurde im Wettbewerbsrecht, welches Anreize für datenschutzkonforme Produkte und Dienste schaffen kann, und in einem Verfahren[916], welches mit einem technischen Mediationsagenten als Metakommunikation konkretisiert wurde,[917] aufgezeigt. Folglich wird in einem Identitätsverwaltungsmodell die Notwendigkeit einer mediativen Identi-

912 4. Teil, E.
913 4. Teil, B., VI.
914 5. Teil, A.
915 5. Teil, B., III.
916 5. Teil, B., IV.
917 5. Teil, C., III.

tätsverwaltung aufgezeigt, um die Verhandlung der Bilder personaler Identitäten in ihrem *Ipse*-Anteil zu ermöglichen.[918] Dabei geht es um die Intervention und um ein Gegengewicht zur Datenverarbeitung und Profilerstellung von Intermediären mit marktbeherrschender Stellung.

Insgesamt konnte gezeigt werden, dass die mediative Identitätsverwaltung dem Schutz des öffentlichen Gutes der persönlichen Informationen dient und ein technischer Mediationsagent als Interventionsmechanismus fungieren kann. Daneben konnte für die Gewährleistung des Modells der Identitätsverwaltung ein Paradigmenwechsel auf drei Ebenen abgeleitet werden, der aus dem Zugang zu den personalen Identitäten, der verhandlungsfähigen personalen Identität und einer dezentralen kontextbezogenen Identitätsverwaltung besteht.[919] Dafür soll etwa mit einem *Dashboard-System* die Transparenz über die kontextspezifischen personalen Teilidentitäten begründet und die Verwaltung dieser zur Gewährleistung der *kontextuellen Integrität* ermöglicht werden. Folglich stellt sich die Frage nach der Implementierung der Identitätsverwaltung auf der Mikro- und Makroebene, so dass der soziotechnische Regelungsbedarf (A.) und der prinzipienbasierte Ansatz (B.) mit einem abschließenden Ausblick (C.) dargestellt werden sollen.

A. Soziotechnischer Regelungsbedarf

Die grundrechtssichernde Implementierung eines technischen Mediationsagenten und einer Struktur für die mediative Identitätsverwaltung könnte einen regulatorischen Eingriff verlangen, bei dem der Anknüpfungspunkt zu bestimmen ist. Zum einen geht es auf der Mikroebene um die Implementierung eines „*mechanism by design*" in Gestalt des technischen Mediationsagenten und zum anderen geht es auf der Makroebene um einen Anreizmechanismus für Maßnahmen zum Ausgleich der Informationsasymmetrien gerade gegenüber Intermediären mit marktbeherrschender Stellung. Jeweils kann ein staatlicher regulatorischer Eingriff dazu dienen, die Technologieentwicklung, Gesamtstrukturen und schließlich das Verhalten des Einzelnen zu beeinflussen. Demgegenüber ist in ökonomischer Hinsicht ein „*Nudging*"-System denkbar, welches bei der Umsetzung rechtlicher Anforderungen durch den Verantwortlichen für den Selbstdatenschutz des Betroffenen unterstützend wirkt, ohne dabei freiheitsbeschrän-

---

918 5. Teil, C., IV., V.
919 6. Teil.

kende Wirkung zu entfalten. Als „*Nudges*" sind Konzepte denkbar, die neben einer vereinfachten bildlichen Darstellung der Risiken auch Warnungen über die Folgen der Einwilligungen enthalten können. Diese würden als (paternalistische) Anreize für eine risikobewusste Entscheidung wirken und sich als wenig invasiver Mechanismus günstig auf den Schutz des öffentlichen Gutes der persönlichen Informationen auswirken.

Ferner kommt *de lege ferenda* die Erweiterung der Schutzgüter im Produkthaftungsrecht gemäß § 1 Abs. 1 ProdHG auf den Schutz der persönlichen Informationen und damit der informationellen Selbstbestimmung in Betracht, womit die Hersteller gehalten wären, die Fehlerfreiheit bei der Entwicklung datenschutzkonformer Produkte zu gewährleisten. Dies würde sich wiederum auf den Wettbewerb mit datenschutzkonformen Produkten auswirken und die öffentliche Reputation, „*privacy by design*"-Produkte im Markt anzubieten, eine positive Marktdynamik für den „*Market for Lemons*"[920] und den Schutz personaler Identitäten im online-Kontext fördern. Gleichwohl würde es sich dabei um eine Marktentwicklung handeln, die den „*Market for Lemons*" nicht vollständig verdrängt, da Informationsasymmetrien nicht aufgelöst werden können. Insofern besteht der Bedarf an wettbewerbsrechtlichen Interventionsmechanismen gegenüber Intermediären mit marktbeherrschender Stellung fort, da der Markt allein, wie sich an dem *Cambridge Analytika*- und *Facebook*-Skandel zeigte,[921] kaum datenschutzkonforme Produkte hervorbringt.

Mit der rechtfertigenden Einwilligung als maßgebliche Kontrollhandlung über personale Identitäten geht ein soziotechnischer Regelungsbedarf einher, um verhaltensökonomische Verzerrungen und langfristige Erkenntnismöglichkeiten aus dem Datenzyklus kompensieren zu können. Dafür kommen erweiterte Transparenzpflichten gemäß Art. 13 DSGVO in Betracht, die etwa auf die verhaltensökonomischen Verzerrungen hinweisen würden, so dass eine Ergänzung dieser Norm in Frage kommt. Ebenso ist ein mit dem AGB-Recht vergleichbares Schutzregime denkbar, was zwischen Datenverarbeitungen im B2C-, B2B- und C2C-Verhältnis differenziert und eine *contra proferentem*-Regel für Zweifelsfälle vorsieht.[922] Daneben wäre die Einbeziehung der Risikobewertung durch den Verantwortlichen *de lege ferenda* als ausdrückliche Informationspflicht wünschenswert, damit eine risikobewusste Entscheidung von dem Betroffenen vorgenom-

920 4. Teil, B., IV., 2., a).
921 www.faz.net/aktuell/wirtschaft/diginomics/fragen-und-antworten-zu-facebook-und-cambridge-analytica-15505321.html (zuletzt aufgerufen 20.06.2020).
922 4. Teil, C., II., 2.

men werden kann. Dies lässt sich aus den Informationspflichten gemäß Art. 13 DSGVO und dem EWG 39 S. 5 ableiten, wonach Betroffene über die Risiken der Datenverarbeitung informiert und aufgeklärt werden sollen. Dafür müssten die maßgeblichen Risikokriterien, die im Rahmen der semi-quantitativen Risikobewertungsmethode bestimmt wurden, transparent gemacht werden.[923]

Weiter könnte eine spezifische Rechtsregel mit dem Inhalt, dass neben „*privacy by design*" ein „*identity management by design*" mit umfassenden Transparenzanforderungen eingesetzt werden müsste, verfolgt werden.[924] Es würde sich um eine konkretisierende Regelung des Art. 25 DSGVO handeln, die für eine effektive Wirkung über eine Soll-Vorschrift hinaus als Muss-Vorschrift ausgestaltet werden sollte. Diese könnte auch in dem EWG 78 S. 2 abgebildet werden. Darin käme die „techniksteuernde Funktion des Rechts"[925] zum Ausdruck und die Reputation über den Einsatz eines „*identity management by design*"-Konzeptes würde sich positiv auf die Wettbewerbsfähigkeit des Verantwortlichen auswirken können.

Ebenso kommt *de lege ferenda* eine Begründungspflicht in Frage, sollte der Verantwortliche bei umfangreichen Datenverarbeitungen kein Identitätsverwaltungskonzept vorsehen. Diese könnte vergleichbar mit der Begründungsanforderung aus § 253 Abs. 3 Nr. 1 ZPO ausgestaltet sein, wonach Angaben in einer Klageschrift über den Versuch einer Mediation oder außergerichtlichen Streitbeilegung vorzunehmen sind.[926] Darin würde ein einfachrechtlicher Anreiz liegen, der den Verantwortlichen dazu veranlasst, sich mit der Einbeziehung der Identitätsverwaltung ernsthaft auseinanderzusetzen und der Verantwortliche begründen müsste, warum ein Identitätsverwaltungskonzept nicht umgesetzt wurde.

B. Prinzipienbasierter Ansatz

Neben einer einfachrechtlichen Regelung zur Implementierung der Identitätsverwaltung könnte ebenso ein prinzipienbasierter Ansatz gewählt werden. Gegenüber den Rechtsnormen ermöglicht das Prinzip die Verfolgung eines generellen Regelungsziels und einen hohen Abstraktionsgrad.[927] Das

923 4. Teil, B., II., 2.
924 4. Teil, B., VI.
925 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 182.
926 5. Teil, C., V.
927 *Zippelius*, Das Wesen des Rechts, 2012, S. 84.

Prinzip ist somit ein Gegengewicht zu einem Regelungsüberschuss, der seit dem Volkszählungsurteil dem Datenschutzrecht teilweise zugeschrieben wird.[928] Insoweit könnte die Einführung eines Prinzips dem Schutz der personalen Identitäten und der Identitätsverwaltung im online-Kontext dienen.

Zwar ist der prinzipienbasierte Ansatz von der angloamerikanischen Rechtskultur geprägt und wurde im Zusammenhang mit dem IT-Recht von *Easterbrook* in dem Aufsatz „*Cyberspace and the Law of the Horse*" zugespitzt.[929] Danach sollten nämlich generelle Prinzipien für das IT-Recht bestimmt werden, damit kontextspezifische detaillierte Rechtsregeln (etwa das „Pferderecht") für das damals neue IT-Recht unnötig werden. Entsprechend zeigen die Grundsätze der Datenverarbeitung in Art. 5 DSGVO die Wirksamkeit eines prinzipienorientierten Ansatzes, da diese Grundsätze sich auf das gesamte Datenschutzrecht erstrecken und kontextspezifisch umgesetzt werden müssen. Folglich wird die Innovationsoffenheit gewährleistet und kontextspezifische Detailregeln werden verdrängt. Weiter könne mit Prinzipien flexibler auf zeitlich bedingte neue Entwicklungen reagiert werden, womit zugleich eine Technologieoffenheit gewährleistet wäre.[930]

Das Regelungsziel, den Selbstdatenschutz mit der mediativen Identitätsverwaltung zu fördern, lässt sich auf prinzipieller Ebene abbilden. Indem die Kontrollmöglichkeiten des Betroffenen im IKT-Recht nachgewiesen wurden, erscheint eine hohe Abstraktion zum Schutz der personalen Identität folgerichtig. Gleichwohl bedarf es einer Erweiterung auf der technischen Gestaltungsebene, die den Zugang zu den personalen Identitäten und die Verhandlung der Bilder personaler Identitäten etwa mit einem *Dashboard-System* ermöglicht. Damit wird dem politischen und wirtschaftlichen Bestreben, die *digitale Souveränität* zu stärken, gefolgt und ein effektiver Schutzmechanismus zum eigenverantwortlichen Selbstdatenschutz begründet.

Erweiternd lässt sich die Identitätsverwaltung hinsichtlich der statischen *Idem*- und dynamischen *Ipse*-Anteile als Gegenstand der staatlichen Daseinsvorsorge einordnen, die bereits von *Schallbruch* für die elektronische Identifizierung angenommen wird.[931] Damit müsste dem Betroffenen

928 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 226.
929 *Easterbrook*, U. Chi. Legal F. 1996, 207.
930 *Zippelius*, Das Wesen des Rechts, 2012, S. 107.
931 *Schallbruch*, Schwacher Staat im Netz, 2018, S. 234; ebenso *Hornung*, in: Roßnagel (Hrsg.), Wolken über dem Rechtsstaat?, 2015, 189 (206).

über den Datenzyklus hinweg prinzipiell eine dynamische Identitätsverwaltung ermöglicht werden, die ein umfassenderes, digitales Handeln gewährleisten würde. Dies würde den Schutz der informationellen Selbstbestimmung im offline-Kontext auf den online-Kontext spiegelbildlich übertragen. Folglich würde sich die staatliche Gewährleistungsverantwortung zur Grundrechtsausübung auf den online-Kontext mit einer dynamischen Identitätsverwaltungsmöglichkeit erstrecken.

Insgesamt könnte es sich um ein im IKT-Recht geltendes „*Prinzip der verhandlungsfähigen personalen Identität*" für den online-Kontext handeln, dem ein dynamisches und iteratives Schutzkonzept für personale Identitäten immanent ist. Dieses sollte mit den Anforderungen einer dezentralen Identitätsverwaltung erweitert werden und ebenso den Zugang zur personalen Identität ermöglichen. Weiter müsste die Verhandlungsfähigkeit der personalen Identität rechtlich und technisch gewährleistet werden. Dieses Prinzip würde dem Konzept der „regulierte(n) Selbstregulierung im Schatten des Rechts"[932] dienen, wenngleich die Effektivität eines solchen Prinzips von seiner tatsächlichen Anwendung abhängig sein würde. Damit besteht ebenso der Bedarf an der Sicherstellung einer effektiven Rechtsanwendung, die mit einem verhaltensökonomischen Anreizmechanismus umgesetzt werden sollte.

C. Ausblick

Die Identitätsverwaltung würde für eine Implementierung zunächst einen politischen Willen voraussetzen, damit eine rechtliche Regulierung folgen kann. Diese sollte nicht als Detailregelung ausgestaltet sein, sondern es würde ebenso wirksam ein Prinzip mit entsprechenden Anreizmechanismen eingeführt werden können. Weiter wäre ein solches Prinzip dazu geeignet, eine technische Gestaltungsprämisse auf der Hardware- und Software-Ebene für den online-Kontext zu schaffen. Hierbei kommt die Implementierung einer dezentralen und interoperablen Identitätsverwaltungsarchitektur in Betracht, mit der die Überführung personaler Teilidentitäten in verschiedene Kontexte ermöglicht wird. Gleichzeitig könnte die Implementierung auf der Softwareebene mit der Einrichtung eines technischen Mediationsagenten, der die Verfahrensprinzipien der Mediation umsetzt, erfolgen. Damit würde für eine Identitätsverwaltungsarchitektur die wesentliche Implementierungsebene zur effektiven Anwendung eines „*Prin-*

932 *Spiecker gen. Döhmann*, K&R 2017, 4 (6).

zips der verhandlungsfähigen personalen Identität" für den online-Kontext realisiert werden können.

Weiter würde mit der Implementierung einer Identitätsverwaltungsarchitektur eine Steigerung des Informationszugangs des Betroffenen zu den personalen Identitäten erfolgen und der Verantwortliche wäre dazu gehalten, diesen Zugang zu ermöglichen. Darin würde nicht nur eine Schutzsteigerung für das öffentliche Gut der persönlichen Informationen liegen, sondern auch die Pluralität personaler Identitäten für den online-Kontext im freiheitlich demokratischen Sinne gefördert werden. Folglich ließe sich sogar vertreten, dass es zur staatlichen Gewährleistungsverantwortung gehöre, die Pluralität der personalen Identitäten auch im online-Kontext sicherzustellen. Demnach lässt sich nicht nur die elektronische Identifizierung als Bestandteil der staatlichen Daseinvorsorge einordnen, sondern auch das *Prinzip der verhandlungsfähigen personalen Identität*.

Mit der Europäisierung des Datenschutzrechts erscheint hierbei jedoch eine nationale Regulierung wenig zielführend, so dass eine Erweiterung der Datenverarbeitungsgrundsätze gemäß Art. 5 DSGVO in Frage kommt. Damit würde ein Gegengewicht zu den Intermediären mit marktbeherrschender Stellung geschaffen werden, welches jedoch mit einem wirksamen Anreizmechanismus ergänzt werden müsste. Zudem wurzelt die prinzipielle Förderung einer dynamischen Identitätsverwaltung im online-Kontext in den grundrechtlichen und einfachrechtlichen Schutzvorgaben, weshalb ein Prinzip für den online-Kontext eine konsequente Erweiterung des bestehenden Schutzregimes bedeuten würde. Insofern ist für die Implementierung der Identitätsverwaltung zunächst der europäische Gesetzgeber gefragt und zugleich erscheint nach den hier gewonnenen Ergebnissen die Einbeziehung verhaltensökonomischer Erkenntnisse für wirksame Anreizmechanismen und für den Selbstdatenschutz wünschenswert.

Literaturverzeichnis

Aamodt, Agnar/Nygård, Mads, Different roles and mutual dependencies of data, information, and knowledge — An AI perspective on their integration, Data & Knowledge Engineering 16 (1995), S. 191–222.

Acquisti, Alessandro, Privacy in electronic commerce and the economics of immediate gratification – Proceedings of the 5th ACM conference on Electronic commerce, ACM 2004, S. 21–29.

—, Nudging Privacy: The Behavioral Economics of Personal Information, IEEE Security & Privacy Magazine 2009, S. 72–75.

Akerlof, George A., The market for "lemons": Quality Uncertainty and the Market Mechanism, The Quarterly Journal of Economics 1970, S. 488–500.

Albers, Marion, Informationelle Selbstbestimmung, Baden-Baden 2005, (Habil. Berlin 2002).

Appel, Ivo, § 32 Privatverfahren, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts Gesamtwerk, 2. Auflage, München 2012.

Art. 29 Data Protection Working Party, WP 185, Stellungnahme zu Geolokalisierungsdiensten von intelligenten mobilen Endgeräten, 16. Mai 2011.

—, WP 217, Opinion 6/2014 on the notion of legitimate interest of the data controller, 9. April 2014.

—, WP 242, Guidelines on the right to data portability, 5. April 2017.

—, WP 260, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 11. April 2018.

Axelrod, Robert M./Raub, Werner, Die Evolution der Kooperation, München 1991.

Barnett, Jeremy/Treleaven, Philip, Algorithmic Dispute Resolution—The Automation of Professional Dispute Resolution Using AI and Blockchain Technologies, The Computer Journal 2017, S. 399–408.

Bartels, Karsten/Backer, Merlin, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 2018, S. 214–219.

Bechtolf, Hans/Vogt, Niklas, Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, S. 66–71.

Becker, Maximilian, Ein Recht auf datenerhebungsfreie Produkte, JZ 2017, S. 170–182.

Bender, Jens, Technische Aspekte grenzüberschreitender Interoperabilität, in: Hornung, Gerrit/Engemann, Christoph (Hrsg.), Der digitale Bürger und seine Identität, Baden-Baden 2016, S. 187–210.

Ben-Shahar, Omri, The Myth of the 'Opportunity to Read' in Contract Law, ERCL 2009, S. 1–28.

Ben-Shahar, Omri/Strahilevitz, Lior Jacob, Contracting over Privacy: Introduction, The Journal of Legal Studies 2016, S1–S11.

Bergfelder, Martin, Der Beweis im elektronischen Rechtsverkehr, Hamburg 2006, (Diss. Freiburg i. Br. 2006).

Bergt, Matthias, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, S. 365–371.

Bernau, Patrick, Der Wert der Daten, FAS vom 10.2.2019, S. 23.

Bernsdorff, Norbert/Borowsky, Martin, Die Charta der Grundrechte der Europäischen Union – Handreichungen und Sitzungsprotokolle, Baden-Baden 2002.

Besemer, Christoph, Mediation – Vermittlung in Konflikten, 12. Auflage, Königsfeld 2007.

Beyerer, Jürgen/Müller-Quade, Jörn/Reussner, Ralf, Karlsruher Thesen zur Digitalen Souveränität Eruopas, DuD 2018, S. 277–280.

Bidgoli, Hossein, Handbook of information security, Hoboken, N.J./Chichester 2006.

Bieker, Felix/Bremert, Benjamin/Hansen, Marit, Die Risikobeurteilung nach der DSGVO, DuD 2018, S. 492–496.

Bieker, Felix/Hansen, Marit/Friedewald, Michael, Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2016, S. 188–197.

Birnstill, Pascal/Beyerer, Jürgen, Building Blocks for Identity Management and Protection for Smart Environments and Interactive Assistance Systems, in: ACM-PETRA 2018, S. 292–296.

Black, R. Brian, Legislating US data privacy in the context of national identification numbers: models from South Africa and the United Kingdom, Cornell Int'l LJ 34 (2001), S. 397–454.

Böckenförde, Thomas, Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, S. 925–939.

Boehme-Neßler, Volker, Rating von Menschen, K&R 2016, S. 637–644.

Brandimarte, Laura/Acquisti, Alessandro, The Economics of Privacy, in: Peitz, Martin/Waldfogel, Joel (Hrsg.), The Oxford Handbook of the Digital Economy, Oxford 2012.

Brandimarte, Laura/Acquisti, Alessandro/Loewenstein, George, Misplaced Confidences: Privacy and the Control Paradox, Social Psychological and Personality Science 4 (2013), S. 340–347.

Bräutigam, Peter/Rücker, Daniel, E-Commerce – Rechtshandbuch, München 2016.

Brecht, Corinna/Steinbrück, Anne/Wagner, Manuela, Der Arbeitnehmer 4.0? Automatisierte Arbeitgeberentscheidungen durch Sensorik am smarten Arbeitsplatz, PinG 2018, S. 10–15.

Breuer, Rüdiger, Direkte und indirekte Rezeption technischer Regeln durch die Rechtsordnung, AöR 101 (1976), S. 46–88.

Britz, Gabriele, Freie Entfaltung durch Selbstdarstellung – Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG, Tübingen 2007.

—, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, S. 1–11.

Brockhaus Enzyklopädie – in 30 Bänden, 21. Auflage, Leipzig, Mannheim 2006.

Buchmann, Erik, Wie kann man Privatheit messen?, DuD 2015, S. 510–514.

Budras, Corinna, Es gibt ein Leben nach dem Smartphone, FAS vom 14.10.2018, S. 21.

Bundeskartellamt, Fallbericht vom 15.2.2019, Az.: B6-22/16 – Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung, abrufbar unter: www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=4 (zuletzt aufgerufen am 20.6.2020).

Bundesministerium des Innern, No-Spy-Erlass, 2014, abrufbar unter: www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2014/no-spy-erlass.pdf (zuletzt aufgerufen am 20.6.2020).

Bundesministeriums der Justiz und für Verbraucherschutz, Referentenentwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs, abrufbar unter: www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_fairerWettbewerb.pdf?__blob=publicationFile&v=1 (zuletzt aufgerufen am 20.6.2020).

Bundesministerium für Wirtschaft und Energie, Referentenentwurf eines zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz), Januar 2020, abrufbar unter: www.bmwi.de/Redaktion/DE/Downloads/G/gwb-digitalisierungsgesetz-referentenentwurf.html (zuletzt aufgerufen am 20.6.2020)

Bundesministerium für Wirtschaft und Energie, Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft, Bericht der Kommission für Wettbewerbsrecht 4.0, September 2019, abrufbar unter: www.bmwi.de/Redaktion/DE/Pressemitteilungen/2019/20190909-expertenkommission-wettbewerbsrecht-40-uebergibt-abschlussbericht-an-minister-altmaier.html (zuletzt aufgerufen am 20.6.2020)

Carroll, Lewis, Alice im Wunderland, Hamburg 1993.

Cohen, Julie E., Irrational privacy, JTHTL 2012, S. 242–249.

Damler, Daniel, Rechtsästhetik – Sinnliche Analogien im juristischen Denken, Berlin 2016, (Habil. Tübingen 2016).

Davidson, Sinclair/Filippi, Primavera de/*Potts, Jason*, Blockchains and the economic institutions of capitalism, Journal of Institutional Economics 2018, S. 639–658.

DeHert, Paul/Gutwirth, Serge, Privacy, data protection and law enforcement: Opacity of the individual and transparency of power, in: Claes, Erik/Gutwirth, Serge/Duff, Anthony (Hrsg.), Privacy and the criminal law, Antwerpen 2006, S. 61–104.

Di Fabio, Udo, Grundrechtsgeltung in digitalen Systemen – Selbstbestimmung und Wettbewerb im Netz, München 2016.

Drackert, Stefan, Die Risiken der Verarbeitung personenbezogener Daten – Eine Untersuchung zu den Grundlagen des Datenschutzrechts, Berlin 2014, (Diss. Freiburg i. Br. 2014).

Dreier, Thomas, Bild und Recht – Versuch einer programmatischen Grundlegung, Baden-Baden 2019.

Drexl, Josef, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, JIPITEC 2017, S. 257–292.

DSK, Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DS-GVO 22.2.2019.

Dürig, Markus/Fischer, Matthias, Cybersicherheit in Kritischen Infrastrukturen, DuD 2018, S. 211–213.

Easterbrook, Frank H., Cyberspace and the Law of the Horse, U. Chi. Legal F. 1996, S. 207–216.

Eckhardt, Jens, Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?, CR 2016, S. 786–790.

Edwards, Lilian/Veale, Michael, Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for, Duke L. & Tech. Rev. 2017, S. 18–84.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO – Datenschutz-Grundverordnung: Kommentar, 2. Auflage, München/Wien 2018.

Eichenhofer, Johannes/Gusy, Christoph, Digitale Identifizierung, in: Hornung, Gerrit/Engemann, Christoph (Hrsg.), Der digitale Bürger und seine Identität, Baden-Baden 2016, S. 65–84.

Eidenmüller, Horst, Ökonomische und spieltheoretische Grundlagen von Verhandlung/Mediation, in: Breidenbach, Stephan/Henssler, Martin (Hrsg.), Mediation für Juristen – Konfliktbehandlung ohne gerichtliche Entscheidung, Köln 1997, S. 31–55.

—, Liberaler Paternalismus, JZ 2011, S. 814–821.

—, Wege aus der Sackgasse: Wie lassen sich Blockaden in Mediations- und Güteverfahren lösen?, ZKM 2013, S. 4–9.

Eifert, Martin, § 19 Regulierungsstrategien, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts Gesamtwerk, 2. Auflage, München 2012.

Elsenbast, Wolfgang, Zum Verhältnis von Spieltheorie und Mediation, ZKM 2016, S. 9–12.

Engels, Barbara/Grundwald, Mara, Das Privacy Paradox: Digitalisierung versus Privatsphäre, No. 57.2017, abrufbar unter: www.iwkoeln.de/fileadmin/publikationen/2017/356747/IW-Kurzbericht_2017-57_Privacy_Paradox.pdf (zuletzt aufgerufen am 20.6.2020).

Erikson, Erik H., Identität und Lebenszyklus – Drei Aufsätze, 27. Auflage, Berlin 2015.

European Data Protection Supervisor, EDPS, Opinion 8/2016 on coherent enforcement of fundamental right in the age of big data, abrufbar unter: www.edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf (zuletzt aufgerufen am 20.6.2020).

Faber, Eberhard von/*Sedlacek, Walter*, Spieltheorie im Dienst der IT-Sicherheit im Internet-der-Dinge, DuD 2017, S. 440–447.

Finck, Michèle, Blockchains and data protection in the european union, EDPL 2018, S. 17–35.

Forum Privatheit, White Paper – Selbstdatenschutz, 2014, abrufbar unter: www.forum-privatheit.de/wp-content/uploads/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf (zuletzt aufgerufen am 20.6.2020).

Froomkin, A. Michael, Building Privacy into the Infrastructure: Towards a New Identity Management Architecture, 2016, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2740719 (zuletzt aufgerufen am 20.6.2020).

Gabriel, Marc/Bärenbrinker, Verena, Der „No Spy" – Erlass des Bundesinnenministeriums: Resümee nach 1,5 Jahren Anwendung und Ausblick für die weitere Praxis, VergabeR, S. 166–173.

Gasser, Urs, Kausalität und Zurechnung von Information als Rechtsproblem, München 2002, (Diss. St. Gallen 2001).

Gellert, Raphael, Understanding the notion of risk in the General Data protection Regulation, CLSR 2018, S. 279–288.

Gersdorf, Hubertus, Telekommunikationsrechtliche Einordnung von OTT-Diensten am Beispiel von Gmail, K&R 2016, S. 91–101.

Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2017.

Gigerenzer, Gerd/Müller, Klaus-Robert/Wagner, Gert, Wie man Licht in die Blackbox wirft, FAZ vom 22.6.2018, S. 15.

Glasl, Friedrich, Konfliktmanagement – Ein Handbuch für Führungskräfte, Beraterinnen und Berater, 12. Auflage, Bern u.a. 2020.

Glöckner, Andreas, Der Mensch im Spannungsfeld zwischen (begrenzter) Rationalität, Eigeninteresse und Kooperation, in: Funke, Andreas/Schmolke, Klaus Ulrich (Hrsg.), Menschenbilder im Recht, 2019, S. 79–92.

Gola, Peter/Eichler, Carolyn/Franck, Lorenz/Klug, Christoph/Lepperhoff, Niels (Hrsg.), Datenschutz-Grundverordnung – VO (EU) 2016/679: Kommentar, 2. Auflage, München 2018.

Gonscherowski/Hansen, Marit/Rost, Martin, Resilienz – eine neue Anforderung aus der DS-GVO, DuD 2018, S. 442–446.

González Fuster, Gloria, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Cham, Heidelberg 2014, (Diss. Brüssel 2013).

Gössl, Susanne, Abstammung und Geschlecht, ZRP 2018, S. 174–177.

Graf von Westphalen, Friedrich, Datenvertragsrecht – disruptive Technik – disruptives Recht, IWRZ 2018, S. 9–21.

Grafenstein, Max von, Die Auswirkungen des Zweckbindungsprinzips auf Innovationsprozesse in Startups, DSRI 2016, S. 233–246.

Greger, Reinhard/Unberath, Hannes/Steffek, Felix (Hrsg.), Recht der alternativen Konfliktlösung – Mediationsgesetz, Verbraucherstreitbeilegungsgesetz: Kommentar, 2. Auflage, München 2016.

Grimm, Dieter, Der Datenschutz vor einer Neuorientierung, JZ 2013, S. 585–592.

—, Notwendigkeit und Bedingungen interdisziplinärer Forschung in der Rechtswissenschaft, in: Kirste, Stephan (Hrsg.), Interdisziplinarität in den Rechtswissenschaften – Ein interdisziplinärer und internationaler Dialog, Berlin 2016, S. 21–34.

Haft, Fritjof, Einführung in die Rechtsinformatik, Freiburg 1977.

—, § 3 Verhandlung und Mediation, in: Haft, Fritjof/Schlieffen, Katharina von (Hrsg.), Handbuch Mediation, 3. Auflage, München 2016.

Hammer, Volker/Knopp, Michael, Datenschutzinstrumente Anonymisierung, Pseudonyme und Verschlüsselung, DuD 2015, S. 503–509.

Hansen, Marit/Kosta, Eleni/Nai-Fovino, Igor/Fischer-Hübner, Simone (Hrsg.), Privacy and Identity Management – The Smart Revolution, Berlin 2017.

Harari, Yuval Noah, Homo Deus – Eine Geschichte von Morgen, München 2017.

Härting, Niko/Gössling, Patrick, Study on the Impact of the Proposed Draft of the ePrivacy-Regulation, CRi 2018, S. 6–11.

Herfurth, Constantin, Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, ZD 2018, S. 514–520.

Hermstrüwer, Yoan, Informationelle Selbstgefährdung – zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, München 2016, (Diss. Bonn 2015/2016).

—, Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data, JIPITEC 2017, S. 9–26.

Hermstrüwer, Yoan/Dickert, Stephan, Tearing the Veil of Privacy Law – An Experiment on Chilling Effects and the Right to be Forgotten, 2013, abrufbar unter: www.econstor.eu/bitstream/10419/84983/1/757205445.pdf (zuletzt aufgerufen am 20.6.2020).

Herrmann, Dominik/Federrath, Hannes, Unbemerktes Tracking im Internet: Unsere unerwünschte Identität, in: Hornung, Gerrit/Engemann, Christoph (Hrsg.), Der digitale Bürger und seine Identität, Baden-Baden 2016, S. 131–152.

Hildebrandt, Mireille, Privacy and Identity, in: Claes, Erik/Gutwirth, Serge/Duff, Anthony (Hrsg.), Privacy and the criminal law, Antwerpen 2006, S. 43–62.

—, Profiling and AmI, in: Rannenberg, Kai/Royer, Denis/Deuker, André (Hrsg.), The Future of Identity in the Information Society – Challenges and Opportunities, Berlin, Heidelberg 2009, S. 274–310.

—, Smart technologies and the end(s) of law – Novel entanglements of law and technology, Cheltenham, UK/Northampton, MA, USA 2015.

Hoffmann-Riem, Wolfgang, Wissen als Risiko – Unwissen als Chance, in: Augsberg, Ino (Hrsg.), Ungewissheit als Chance – Perspektiven eines produktiven Umgangs mit Unsicherheit im Rechtssystem, Tübingen 2009, S. 17–38.

—, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017), S. 1–42.

Hornung, Gerrit, Die digitale Identität – Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005, (Diss. Kassel 2005).

—, Zwischen Rechtssicherheit und Persönlichkeitsschutz: Rechtsfragen des Identitätsmanagements, in: Roßnagel, Alexander (Hrsg.), Wolken über dem Rechtsstaat? – Recht und Technik des Cloud Computing in Verwaltung und Wirtschaft, Baden-Baden 2015, S. 189–216.

Hornung, Gerrit/Möller, Jan, Passgesetz, Personalausweisgesetz – Kommentar, München 2011.

Janal, Ruth, Data Portability – A Tale of Two Concepts, JIPITEC 2017, S. 59–69.

Janeček, Václav, Ownership of personal data in the Internet of Things, CLSR 2018, S. 1039–1052.

Jarass, Hans D., Kommentar, Charta der Grundrechte der EU, 3. Auflage, München 2016.

Jay, Rosemary, Data protection law and practice, 4. Auflage, London 2012.

Jestaedt, Matthias, Rechtswissenschaft als normative Disziplin, in: Kirste, Stephan (Hrsg.), Interdisziplinarität in den Rechtswissenschaften – Ein interdisziplinärer und internationaler Dialog, Berlin 2016.

Jóri, András, Shaping vs applying data protection law: two core functions of data protection authorities, IDPL 2015, S. 133–143.

Kahneman, Daniel, Schnelles Denken, langsames Denken, München 2012.

Kahneman, Daniel/Tversky, Amos, Prospect Theory: An Analysis of Decision under Risk, Econometrica 1979, S. 263–291.

Kalabis, Lukas/Selzer, Annika, Das Recht auf Vergessenwerden nach der geplanten EU-Verordnung, DuD 2012, S. 670–675.

Karg, Moritz, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, S. 520–526.

KASTEL-Kompetenzzentrum, Begriffsdefinitionen in KASTEL, abrufbar unter: www.kastel.kit.edu/downloads/Begriffsdefinitionen_in_KASTEL.pdf (zuletzt aufgerufen am 20.6.2020).

Kaulartz, Markus, Smart Dispute Resolution, DSRI 2017, S. 599.

Kaulartz, Markus/Heckmann, Jörn, Smart Contracts – Anwendungen der Blockchain-Technologie, CR 2016, S. 618–624.

Kerber, Wolfgang/Schweitzer, Heike, Interoperability in the digital economy, JIPITEC 2017, S. 39–58.

Keupp, Heiner, Identitätskonstruktionen – Das Patchwork der Identitäten in der Spätmoderne, Reinbek bei Hamburg 1999.

Kieck, Annika, Der Schutz individueller Identität als verfassungsrechtliche Aufgabe – Am Beispiel des geschlechtlichen Personenstands, Berlin 2019, (Diss. Passau 2018).

Kingreen, Thorsten/Poscher, Ralf, Grundrechte: Staatsrecht II, 35. Auflage, Heidelberg 2019.

Kischel, Uwe, Rechtsvergleichung, München 2015.

Klaes, Silke, Alternative Streitbeilegung für Verbraucher in der Telekommunikation – Der Entwurf des Verbraucherstreitbeilegungsgesetzes im Lichte der Anforderungen der TK-Branche, MMR 2015, S. 299–302.

Kneidinger-Müller, Bernadette, Identitätsbildung in sozialen Medien, in: Schmidt, Jan-Hinrik/Taddicken, Monika (Hrsg.), Handbuch Soziale Medien, Wiesbaden 2017.

Knopp, Micheal, Stand der Technik, DuD 2017, S. 663–666.

Köhler, Helmut, Datenschutz – eine neue Aufgabe für das Wettbewerbsrecht?, ZD 2019, S. 285–286.

Kokott, Juliane/Sobotta, Christoph, The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, IDPL 2013, S. 222–228.

Korsgaard, Christine M., Self-Constitution – Agency, Identity, and Integrity, Oxford 2009.

Kracht, Stefan, § 13 Rolle und Aufgabe des Mediators – Prinzipien der Mediation, in: Haft, Fritjof/Schlieffen, Katharina von (Hrsg.), Handbuch Mediation, 3. Auflage, München 2016.

Kremer, Sascha, Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, CR 2012, S. 438–446.

Kring, Markus/Marosi, Johannes, Elefant im Porzellanladen, K&R 2016, S. 773–776.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Kommentar, DS-GVO, BDSG, 2. Auflage, München 2018.

Kühling, Jürgen/Klar, Manuel, Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, S. 3611.

Kühling, Jürgen/Klar, Manuel/Sackmann, Florian, Datenschutzrecht, 4. Auflage, Heidelberg 2018.

Kühling, Jürgen/Sackmann, Florian, Rechte an Daten – Regulierungsbedarf aus Sicht des Verbraucherschutzes? Rechtsgutachten im Auftrag der Verbraucherzentrale Bundesverband, 20. November 2018, abrufbar unter: www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_kuehling-sackmann-rechte-an-daten.pdf (zuletzt aufgerufen am 20.6.2020).

Kühling, Jürgen/Schall, Tobias, WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts, CR 2015, S. 641–655.

Kühling, Jürgen/Schall, Tobias/Biendl, Michael, Telekommunikationsrecht, 2. Auflage, Heidelberg 2014.

Kuhn, Thomas S., Die Struktur wissenschaftlicher Revolutionen, 30. Auflage, Frankfurt am Main 2003.

Kulhari, Shraddha, Building-Blocks of a data protection revolution – The uneasy case for blockchain technology to secure privacy and identity, Baden-Baden 2018.

Kuner, Christopher/Kate, Fred/Millard, Christopher/Svantesson, Dan/Lynskey, Orla, Editorial: Risk Management in Data Protection, IDPL 2015, S. 95–98.

Lanzing, Marjolein, The transparent self, Ethics and Information Technology 2016, S. 9–16.

Laue, Philip/Nink, Judith/Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Auflage, Baden-Baden 2019.

Lehnert, Volker/Luther, Iwona/Christoph, Björn/Pluder, Carsten, Datenschutz mit SAP – SAP Business Suite und SAP S/4HANA, Bonn 2018.

Lewinski, Kai von, Die Matrix des Datenschutzes – Besichtigung und Ordnung eines Begriffsfeldes, Tübingen 2014.

Lippmann, Eric, Identität im Zeitalter des Chamäleons – Flexibel sein und Farbe bekennen, 2. Auflage, Göttingen/Bristol 2014.

Luhmann, Niklas, Identitätsgebrauch in selbstsubstitutiven Ordnungen, besonders Gesellschaften, in: Marquard, Odo/Stierle, Karlheinz (Hrsg.), Identität – „Poetik und Hermeneutik", 8. Kolloquium vom 5. bis 11. September 1976 in Bad Homburg, München 1979.

—, Das Risiko und Kausalität, in: Baecker, Dirk (Hrsg.), Die Kontrolle von Intransparenz, 2017, S. 46–64.

—, Die Kontrolle von Intransparenz, in: Baecker, Dirk (Hrsg.), Die Kontrolle von Intransparenz, 2017, S. 96–120.

—, Erkenntnis als Konstruktion, in: Baecker, Dirk (Hrsg.), Die Kontrolle von Intransparenz, 2017, S. 9–29.

—, Legitimation durch Verfahren, 10. Auflage, Frankfurt am Main 2017.

Luu, Loi/Teutsch, Jason/Kulkarni, Raghav/Saxena, Prateek, Demystifying Incentives in the Consensus Computer, in: Ray, Indrajit/Li, Ninghui/Kruegel, Christopher (Hrsg.), CCS'15 – Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security: October 12-16, 2015, Denver, Colorado, USA, New York 2015, S. 706–719.

Maier, Natalie/Schaller, Fabian, ePrivacy-VO – alle datenschutzrechtlichen Risiken der elektronischen Kommunikation gebannt – Entwurf ohne Regelungen für P2P-Kommunikationsdienste, ZD 2017, S. 373–377.

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht – Grundlagen, Dimensionen, Verflechtungen, Tübingen 2018, (Habil. Freiburg i. Br. 2017).

Masing, Johannes, Herausforderungen des Datenschutzes, NJW 2012, S. 2305–2311.

Matzutt/Müllmann/Zeissig/Horst/Kasugai/Lidynia/Wieninger/Ziegeldorf/Gudergan/Spiecker gen. Döhmann/Wehrle/Ziefle, myneData: Towards a Trusted and User-controlled Ecosystem for Sharing Personal Data, in: Eibl, Maximilian/Geadke, Martin (Hrsg.), INFORMATIK 2017 – Gesellschaft für Informatik, Bonn, S. 1073–1084.

Maus, Moritz, Der grundrechtliche Schutz des Privaten im europäischen Recht, Frankfurt am Main 2007, (Diss. Gießen 2006).

Meuter, Norbert, Identität, in: Kolmer, Petra/Wildfeuer, Armin G. u.a. (Hrsg.), Neues Handbuch philosophischer Grundbegriffe, Freiburg im Breisgau 2011.

Meyer, Jürgen/Bernsdorff, Norbert (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage, Baden-Baden 2014.

Meyer-Goßner/Schmitt, Bertram, Strafprozessordnung – Kommentar, 62. Auflage, München 2019.

Mnookin, Robert H./Kornhauser, Lewis, Bargaining in the shadow of the law: The case of divorce, Yale L. J. 1978, S. 950–997.

Müller-Henstenberg, Claus/Kirn, Stefan, Intelligente (Software-) Agenten: Eine neue Herausforderung unseres Rechtssystems, MMR 2014, S. 307–313.

Nash, John, The Bargaining Problem, Econometrica 1950, S. 155–162.

Nettesheim, Martin, Grundrechtsschutz der Privatheit, in: Diggelmann, Oliver/Lege, Joachim/Nettesheim, Martin (Hrsg.), Der Schutzauftrag des Rechts – Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, Berlin 2011, S. 8–49.

Nissenbaum, Helen, Privacy as contextual integrity, Wash. L. Rev. 2004, S. 119–157.

Orwat, Carsten/Raabe, Oliver/Buchmann, Erik/Anandasivam, Arun/Freytag, Johan-Christoph/Helberger, Natali/Ishii, Kei/Lutterbeck, Bernd/Neumann, Dirk/Otter, Thomas/Pallas, Frank/Reussner, Ralf/Sester, Peter/Weber, Karsten/Werle, Raymund, Software als Institution und ihre Gestaltbarkeit, Informatik Spektrum 2010, S. 626–633.

Paal, Boris P./Pauly, Daniel A./Ernst, Stefan (Hrsg.), Kommentar, DS-GVO, 2. Auflage, München 2018.

Palandt, Otto, Kommentar, BGB, 79. Auflage, München 2020.

Pap, Arthur, Theory of definition, Philosophy of science 1964, S. 49–54.

Pearson, Siani/Casassa-Mont, Marco, Sticky policies: An approach for managing privacy across multiple parties, Computer 2011, S. 60–68.

Peck, Morgen E., Blockchains: How they work and why they'll change the world, IEEE Spectrum 54 (2017), S. 26–35.

Pfitzmann, Andreas, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, 2006, abrufbar unter: www.dud. inf. tu-dresden. de/literatur/Anon_Terminology_v0. 28. pdf (zuletzt aufgerufen am 20.6.2020).

Pfitzmann, Andreas/Köhntopp, Marit, Anonymity, Unobservability, and Pseudonymity – a proposal for terminology, in: Federrath, Hannes (Hrsg.), Designing Privacy Enhancing Technologies, Berlin, Heidelberg 2001, S. 1–9.

Platon, Symposion, München 2008.

Pörksen, Bernhard, Die unerträgliche Gleichzeitigkeit des Seins, NZZ vom 12.7.2018, S. 37.

Pretschner, Alexander/Walter, Thomas, Negotiation of Usage Control Policies – Simply the Best? – Third International Conference on Availability, Reliability and Security, IEEE 2008, S. 1135–1136.

Prosser, William, Privacy, Cal. Law Review 1960, S. 383–423.

Pünder, Hermann/Schellenberg, Martin (Hrsg.), Vergaberecht – GWB – VgV – VS-VgV – SektVO – VOL/A – VOB/A – VOF – Haushaltsrecht – Öffentliches Preisrecht, 3. Auflage, Baden-Baden 2019.

Quelle, Claudia, Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach, European Journal of Risk Regulation 2018, S. 502–526.

Raabe, Oliver, Datenschutz- und IT-Sicherheitsrechtliche Risikomodelle, in: Beyerer, Jürgen/Winzer, Petra (Hrsg.), Beiträge zu einer Systemtheorie Sicherheit (acatech DISKUSSION), München 2018, S. 97–120.

Raabe, Oliver/Lorenz, Mieke, Die datenschutzrechtliche Einwilligung im Internet der Dienste, DuD 2011, S. 279–284.

Raabe, Oliver/Lorenz, Mieke/Pallas, Frank/Weis, Eva, Harmonisierung konträrer Kommunikationsmodelle im Datenschutzkonzept des EnWG – „Stern" trifft „Kette", CR 2011, S. 831–840.

Raabe, Oliver/Schallbruch, Martin/Steinbrück, Anne, Systematisierung des IT-Sicherheitsrechts, CR 2018, S. 706–715.

Radlanski, Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Tübingen 2016, (Diss. Regensburg 2015).

Rajbhandari, Lisa/Snekkenes, Einar, Using game theory to analyze risk to privacy: An initial insight, in: IFIP Advances in Information and Communication Technology, vol. 352, Berlin, Heidelberg 2010, S. 41–51.

Raschke, Philip/Küpper, Axel/Drozd, Olha/Kirrane, Sabrina, Designing a GDPR-Compliant and Usable Privacy Dashboard, in: Hansen, Marit/Kosta, Eleni u.a. (Hrsg.), Privacy and Identity Management – The Smart Revolution, Berlin 2017, S. 221–236.

Rasmusen, Eric, Games and information – An introduction to game theory, 4. Auflage, Oxford, Malden, Victoria 2009.

Reinhardt, Jörn, Konturen des europäischen Datenschutzgrundrechts – Zu Gehalt und horizontaler Wirkung von Art. 8 GRCh, AöR 142 (2017), S. 528–565.

Reisinger, Leo, Rechtsinformatik, Berlin/Boston 2016.

Ricœur, Paul, Oneself as another, Chicago 1994.

Roßnagel, Alexander, 3.4. Konzepte des Selbstdatenschutzes, in: Roßnagel, Alexander/Abel, Ralf Bernd (Hrsg.), Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003.

—, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, S. 71–75.

—, Rechtsregeln für einen sicheren elektronischen Rechtsverkehr, CR 2011, S. 23–30.

—, Neue Regeln für sichere elektronische Transaktionen, NJW 2014, S. 3686–3692.

—, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, S. 1–5.

Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi, Besserer Internetdatenschutz für Europa. Vorschläge zur Spezifizierung der DS-GVO, ZD 2013, S. 103–108.

Rubinstein, Ariel, Economic fables, Cambridge 2012.

Schallaböck, Jan, Identitätsmanagement als Grundlage von Verhaltenssteuerung, in: Hornung, Gerrit/Engemann, Christoph (Hrsg.), Der digitale Bürger und seine Identität, Baden-Baden 2016, S. 103–130.

Schallbruch, Martin, Die EU-Richtlinie über Netz- und Informationssicherheit: Anforderungen an digitale Dienste, CR 2016, S. 663–670.

—, Schwacher Staat im Netz – Wie die Digitalisierung den Staat in Frage stellt, Wiesbaden 2018.

Schelling, Thomas C., The strategy of conflict, Oxford u.a. 1969.

Schirrmacher, Frank, Ego – Das Spiel des Lebens, München 2013.

Schliesky, Utz, Eine Verfassung für den digitalen Staat?, ZRP 2015, S. 56–58.

Schmidt, Klaus, § 8 Entstehung und Bearbeitung von Konflikten, in: Haft, Fritjof/Schlieffen, Katharina von (Hrsg.), Handbuch Mediation, 3. Auflage, München 2016.

Schmidt, Markus/Pruß, Michael, § 3 Technische Grundlagen des Internets, in: Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage, München 2018.

Schneider, Christoph/Weinmann, Markus/Vom Brocke, Jan, Digital Nudging – Guiding Choices by Using Interface Design, Communications of the ACM 2018, S. 67–73.

Schönke, Adolf/Schröder, Horst/Eser, Albin/Perron, Walter (Hrsg.), Strafgesetzbuch – Kommentar, 30. Auflage, München 2019.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor/Kugelmann, Dieter (Hrsg.), DS-GVO/BDSG, Kommentar, Heidelberg 2018.

Schwarze, Jürgen/Becker, Ulrich/Hatje, Armin/Schoo, Johann (Hrsg.), EU-Kommentar, 4. Auflage, Baden-Baden 2019.

Seibel, Mark, Abgrenzung der „allgemein anerkannten Regeln der Technik" vom „Stand der Technik", NJW 2013, S. 3000–3004.

Sester, Peter/Nitschke, Tanja, Software-Agent mit Lizenz zum…, CR 2004, S. 548–554.

Shapiro, Daniel, Negotiating the nonnegotiable, New York 2017.

Siegwart, Geo, Identität, in: Sandkühler, Hans Jörg (Hrsg.), Enzyklopädie Philosophie – In drei Bänden, Hamburg 2010.

Smart Data Begleitforschung, Smart Data – Smart Privacy? – Impulse für eine interdisziplinär rechtlich-technische Evaluation. Technical Report des BMWi-Technologieprogramms „Smart Data – Innovationen aus Daten", 2015, abrufbar unter: www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData_Thesenpapier_smart_Privacy.html (zuletzt aufgerufen am 20.6.2020).

—, Sicheres Identitätsmanagement im Internet – Eine Analyse des ISÆN-Konzepts, 2017, abrufbar unter: www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smartdata_studie_isaen.html (zuletzt aufgerufen am 20.6.2020).

Smedinghoff, Thomas, Introduction to Online Identity Management, abrufbar unter: www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff_Paper_-_Introduction_to_Identity_Management.pdf (zuletzt aufgerufen am 20.6.2020).

Soiné, Michael/Engelke, Hans-Georg, Das Gesetz zur Harmonisierung des Schutzes gefährdeter Zeugen (Zeugenschutz-Harmonisierungsgesetz-ZSHG), NJW 2002, S. 470–476.

Solove, Daniel J., Privacy Self-Management and the Consent Dilemma, Harv. L. R. 2013, S. 1880–1903.

Sorge, Christoph/Wethoff, Dirk, eIDs und Identitätsmanagement, DuD 2008, S. 337–341.

Sosna, Sabine, EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten-eIDAS-Verordnung, CR 2014, S. 825–832.

Specht, Louisa, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, S. 288–296.

Spiecker gen. Döhmann, Indra, Zur Zukunft systemischer Digitalisierung – Erste Gedanken zur Haftungs- und Verantwortungszuschreibung bei informationstechnischen Systemen, CR 2016, S. 698–704.

—, Teil-Verfassungsordnung Datenschutz, in: Vesting, Thomas (Hrsg.), Der Eigenwert des Verfassungsrechts – Was bleibt von der Verfassung nach der Globalisierung?, Tübingen 2011, S. 263–285.

—, Steuerung im Datenschutzrecht: Ein Recht auf Vergessen wider Vollzugsdefizite und Typisierung, KritV 2014, S. 28–43.

—, 30 Thesen: Der Mensch, der Netzbürger, die Algorithmen, das Internt und das Recht, K&R 2017, S. 4–6.

Spiecker gen. Döhmann, Indra/Tambou, Olivia/Bernal, Paul/Hu, Margaret, The Regulation of Commercial Profiling–A Comparative Analysis, EDPL 2016, S. 535–554.

Spina, Alessandro, Risk Regulation of Big Data: Has the Time arrived for a Paradigm Shift in EU Data Protection Law?, EJRR 2014, S. 248–252.

Spindler, Gerald, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung – Gutachten F zum 69. Deutschen Juristentag, in: Verhandlungen des 69. Deutschen Juristentages, München 2012.

Spindler, Gerald/Schmitz, Peter (Hrsg.), Kommentar, TMG, 2. Auflage, München 2018.

Spindler, Gerald/Thorun, Christian, Die Rolle der Ko-Regulierung in der Informationsgesellschaft Handlungsempfehlung für eine digitale Ordnungspolitik, MMR-Beilage 2016, S. 1–28.

Steinbrück, Anne, Identitätsverwaltung über die Blockchain? Rechtliche Betrachtungen am Beispiel des Internet of Things, in: Schweighofer, Erich/Kummer, Franz/Saarenpää, Ahti (Hrsg.), Tagungsband, IRIS 2019 – Internets der Dinge, Bern 2019, S. 283–288.

Steinmüller, Wilhelm, Information, Modell, Informationssystem – Report Nr. 5 / 1991,

—, Das informationelle Selsbtestimmungsrecht – Wie es entstand und was man daraus lernen kann, RDV 2007, S. 158–161.

Stern, Klaus/Sachs, Michael (Hrsg.), Europäische Grundrechte-Charta – Kommentar, München 2016.

Sullivan, Clare, Digital Identity – From emergent legal concept to new reality, CLSR 2018, S. 723–731.

Talidou, Zoi, Regulierte Selbstregulierung im Bereich des Datenschutzes, Frankfurt am Main 2005, (Diss. Freiburg i. Br. 2005).

Teletrust, Handreichung zum „Stand der Technik", 2018, abrufbar unter: www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik_-_Ausgabe_2018.pdf (zuletzt aufgerufen am 20.6.2020).

Teubner, Gunther, Elektronische Agenten und große Menschenaffen: Zur Ausweitung des Akteurstatus in Recht und Politik, Zeitschrift für Rechtssoziologie 2006, S. 5–30.

Turkle, Sherry, Leben im Netz – Identität in Zeiten des Internet, Reinbek bei Hamburg 1999.

Tversky, Amos/Kahneman, Daniel, Judgement under Uncertainty: Heuristics and Biases, Science 1974, S. 1124–1131.

Unabhängiges Landeszentrum für Datenschutz (ULD), Identity Management Systems (IMS) – Identification and Comparison Study Independent Centre for Privacy Protection (ICPP), 2004, abrufbar unter: www.slidex.tips/download/identity-management-systems-ims-identification-and-comparison-study (zuletzt aufgerufen am 20.6.2020).

van Aaken, Anne, Towards a Psychological Concept of Law, in: Kirste, Stephan (Hrsg.), Interdisziplinarität in den Rechtswissenschaften – Ein interdisziplinärer und internationaler Dialog, Berlin 2016, S. 187–204.

Veil, Winfried, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, ZD 2015, S. 347–354.

—, Accountability – Wie weit reicht die Rechenschaftspflicht der DS-GVO?, ZD 2018, S. 9–16.

—, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider – Der gefährliche Irrweg des alten wie des neuen Datenschutzrechts, NVwZ 2018, S. 686–696.

—, Einwilligung oder berechtigtes Interesse? – Datenverarbeitugn zwischen Skylla und Charybdis, NJW 2018, S. 3337–3344.

Wagner, Gerhard, § 823 BGB, in: Säcker, Franz Jürgen (Hrsg.), Münchener Kommentar – BGB, Bd. 5, 7. Auflage, München 2015.

Warnecke, Thomas, Identitätsmanagement und Datenschutz – Verantwortung für einen datenschutzgerechten Zugang zu transaktionsbezogenen E-Government-Anwendungen unter besonderer Berücksichtigung der De-Mail-Dienste und des neuen Personalausweises, Baden-Baden 2019, (Diss. Kiel 2017).

Warren, Samuel D./Brandeis, Louis D., Right to Privacy, Harv. L. R. 1890, S. 193–220.

Wattenhofer, Roger, The science of the blockchain, Aalborg 2017.

Watzlawick, Paul/Beavin, Janet H./Jackson, Don D., Menschliche Kommunikation – Formen, Störungen, Paradoxien, 13. Auflage, Bern 2016.

Weichert, Thilo, Der Personenbezug von Geodaten, DuD 2007, S. 17–23.

Wendehorst, Christiane/Graf von Westphalen, Friedrich, Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, S. 3745–3750.

Wendenburg, Felix, Der Schutz der schwächeren Partei in der Mediation, Tübingen 2013, (Diss. Hamburg 2012).

Weyh, Florian Felix, Philosophie in der digitalen Welt – DigiKant oder: Vier Fragen, frisch gestellt, abrufbar unter: www.deutschlandfunk.de/philosophie-in-der-digitalen-welt-digikant-oder-vier-fragen.1184.de.html?dram:article_id=454492 (zuletzt aufgerufen am 20.6.2020).

White House, National Strategy for Trusted Identities in Cyberspace – Enhancing Online Choice, Efficiency, Security, and Privacy, 2011, abrufbar unter: www.hsdl.org/?view&did=7010 (zuletzt aufgerufen am 20.6.2020).

Whitman, James Q., The Two Western Cultures of Privacy: Dignity Versus Liberty, Yale L. J. 2004, S. 1151–1221.

Wieduwilt, Hendrik, Datenschützer einigt Euch!, FAZ vom 20.10.2018, S. 17.

Windley, Phillip J., Digital identity – Unmasking identity management architecture (IMA), Beijing 2005.

Winheller, Andreas, Framing in der Mediation – Teil 1, ZKM 2018, S. 116–121.

—, Framing in der Mediation – Teil 2, ZKM 2018, S. 175–181.

Wischmeyer, Thomas, Regulierung intelligenter Systeme, AöR 143 (2018), S. 1–66.

Wittmann, Philipp, Nobody Watches the Watchmen-Rechtliche Rahmenbedingungen und zunehmende Ausweitung der öffentlichen Videoüberwachung in den USA, ZaöRV 73 (2013), S. 373–426.

Wright, Aaron/Filippi, Primavera de, Decentralized blockchain technology and the rise of lex cryptographia, 2015, abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 (zuletzt aufgerufen am 20.6.2020).

Wüsthof, Lukas, OTT-Dienste und Telekommunikationsregulierung, N&R 2019, S. 275–279.

Zander, Tim/Steinbrück, Anne/Birnstill, Pascal, Game-theoretical Model on the GDPR – Market for Lemons?, JIPITEC 2019, S. 200–208.

—, Spieltheoretische Modellierung der Verarbeitung personenbezogener Daten, DuD 2019, S. 270–275.

Zippelius, Reinhold, Das Wesen des Rechts – Eine Einführung in die Rechtstheorie, 6. Auflage, Stuttgart 2012.

Zuboff, Shoshana, Überwachen und Verkaufen, FAZ vom 24.9.2018, 12.