KARLSRUHER INSTITUT FÜR TECHNOLOGIE (KIT)
SCHRIFTEN DES ZENTRUMS FÜR ANGEWANDTE RECHTSWISSENSCHAFT 19

OLIVER VETTERMANN

Der grundrechtliche Schutz der digitalen Identität unter Berücksichtigung von Datenschutz- und IT-Sicherheitsrecht

Oliver Vettermann

Der grundrechtliche Schutz der digitalen Identität unter Berücksichtigung von Datenschutz- und IT-Sicherheitsrecht

Schriften des Zentrums für angewandte Rechtswissenschaft

BAND 19

ZAR | Zentrum für angewandte Rechtswissenschaft
Karlsruher Institut für Technologie (KIT)

HERAUSGEBER DER SCHRIFTENREIHE

Prof. Dr. Thomas Dreier M.C.J.

Der grundrechtliche Schutz der digitalen Identität unter Berücksichtigung von Datenschutz- und IT-Sicherheitsrecht

von
Oliver Vettermann

KIT Scientific Publishing

Inauguraldissertation zur Erlangung des Grades eines Doktors der Rechte
durch die Juristenfakultät der Universität Leipzig

Der grundrechtliche Schutz der digitalen Identität unter Berücksichtigung
von Datenschutz- und IT-Sicherheitsrecht

Dekan: Prof. Dr. Tim Drygala

Erstgutachter: Prof. Dr. Hubertus Gersdorf
Leiter Institut für Medien- und Datenrecht sowie Digitalisierung
Universität Leipzig

Zweitgutachterin: Prof. Dr. Franziska Boehm
Karlsruher Institut für Technologie (KIT)

Ort und Tag der mündlichen Prüfung:
Leipzig, 22.06.2022

Impressum

KIT Scientific Publishing

Karlsruher Institut für Technologie (KIT)
KIT Scientific Publishing
Straße am Forum 2
D-76131 Karlsruhe

KIT Scientific Publishing is a registered trademark
of Karlsruhe Institute of Technology.
Reprint using the book cover is not allowed.

www.ksp.kit.edu

Print on Demand 2022 – Gedruckt auf FSC-zertifiziertem Papier

ISSN 1860-8744
ISBN 978-3-7315-1213-4
DOI 10.5445/KSP/1000148103

„Das Internet ist nur ein Hype.“
Bill Gates, Microsoft-Gründer, 1993

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2020/2021 von der Juristenfakultät der Universität Leipzig als Dissertation angenommen. Sie entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter an der Universität Leipzig sowie bei FIZ Karlsruhe, insbesondere angelehnt an das interdisziplinäre und BMBF-geförderte Forschungsprojekt zur effektiven Information nach digitalem Identitätsdiebstahl (kurz: EIDI). Veröffentlicht ist die Arbeit sowohl als physisches Druckwerk als auch als digitale Open-Access-Fassung, um die weitere inter- wie intradisziplinäre Forschung und Diskussion der in der Arbeit enthaltenen Theorien zu ermöglichen. Für die Veröffentlichung konnten Rechtsprechung, Literatur und Weblinks bis einschließlich Juni 2022 berücksichtigt werden.

Mein besonderer Dank gilt meinem Doktorvater *Prof. Dr. Hubertus Gersdorf* für seinen fachlichen Rat bei der Erstellung dieser Arbeit, die wissenschaftliche Freiheit bei der Bearbeitung der vorliegenden Thematik und die Unterstützung meiner Tätigkeit beim Forschungsprojekt EIDI.

Gleichermaßen danke ich *Prof. Dr. Franziska Boehm* für die Anfertigung des Zweitgutachtens und die Möglichkeit der Mitwirkung am Forschungsprojekt EIDI einschließlich der damit verbundenen Erfahrungen aus Wissenschaft, Forschung, Lehre und Praxis, welche Eingang in die Bearbeitung der Thematik gefunden haben.

Im gleichen Atemzug danke ich ebenfalls meinen Kolleginnen und Kollegen beim Projekt EIDI, insbesondere *Prof. Dr. Michael Meier*, *Dr. Matthias Wübbeling* und *Timo Malderle* für die Förderung meiner informatischen Denkweise und LaTeX-Kenntnisse sowie *Susan Gonscherowski* für den Austausch auf dem Gebiet des Datenschutzes.

Nicht minder schätzend danke ich *Dr. Barbara Sandfuchs* und *Prof. Dr. Wilfried Bernhardt* dafür, dass sie mein wissenschaftliches Interesse für das IT- und Datenschutzrecht im Rahmen gemeinsamer Seminare gefördert und gefordert haben, sowie *Prof. Dr. Christoph Degenhart* als Wegbereiter meiner wissenschaftlichen Laufbahn.

Meine Danksagung gilt aber auch zu großen Teilen meinem privaten Umfeld: Ich danke *Christian Vettermann* dafür, mich durch die gesamte Zeit der Promotion in Höhen und Tiefen begleitet zu haben. *Christiane Attig* danke ich für Gespräche über Bindungen, Identität und viele nicht-akademische Themen, die mir immer ein Rückhalt waren. *Julius Herold* sei für seine ludonautische Ablenkung zwischen meinen Schreibphasen gedankt. Meiner Familie *Diana Bizuga*, *Ronald Götz* und *Franziska Bizuga* danke ich dafür, dass sie nie das Vertrauen in mich verloren hat.

Abschließend danke ich *Philipp Gleiche*, der mir in den letzten Phasen der Fertigstellung meiner Arbeit als Mensch an meiner Seite eine stetige Quelle des Optimismus, der Motivation und Inspiration war.

Leipzig, Juli 2022 Oliver Vettermann

Inhaltsverzeichnis

Abkürzungsverzeichnis

<kes>	Zeitschrift für Informations-Sicherheit
a.A.	anderer Ansicht
Abs.	Absatz
AcP	Archiv für civilistische Praxis (Zeitschrift)
AfP	Archiv für Presserecht (Zeitschrift)
aE	am Ende
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AGB	Allgemeine Geschäftsbedingungen
AI	Artificial Intelligence, dt. Künstliche Intelligenz
Alt.	Alternative
Anm.	Anmerkung
AöR	Archiv des öffentlichen Rechts (Zeitschrift)
Az.	Aktenzeichen
BAGE	Entscheidung des Bundesarbeitsgerichts
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
BfDI	Bundesbeauftragte für Datenschutz und Informationsfreiheit

BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BHO	Bundeshaushaltsordnung
BlnDSG	Berliner Datenschutzgesetz
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesmeldegesetz
BNetzA	Bundesnetzagentur
BonnK	Bonner Kommentar zum Grundgesetz
BReg	Bundesregierung
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-G	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BVerwGE	Entscheidung des Bundesverwaltungsgerichts
bzw.	beziehungsweise
c't	Magazin für Computertechnik
COVID-19	Coronavirus-Erkrankung
CR	Computer und Recht (Zeitschrift)
DGA	Data Governance Act
dGrC	Digitale Grundrechte-Charta
DMA-E	Entwurf des Digital Market Acts
DNA	Desoxyribonucleinsäure, auch: genetisches Erbgut

DÖV	Die öffentliche Verwaltung (Zeitschrift)
DSA-E	Entwurf des Digital Services Acts
DSAnpUG	Datenschutz-Anpassungs- und Umsetzungsgesetz
DSB	Datenschutzberater (Zeitschrift)
DSGVO	Datenschutz-Grundverordnung
DSRITB	Tagungsband der Deutschen Stiftung für Recht und Informatik
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DVBl	Deutsche Verwaltungsblätter (Zeitschrift)
E	Entscheidung
eID	elektronische Identität
eIDAS-VO	Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
EMRK	Europäische Menschenrechtskonvention
ePerson	elektronische Person
ePrivacy-VO	Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG
EuGRZ	Europäische Grundrechte Zeitschrift
EuR	Europarecht (Zeitschrift)
ErwGr	Erwägungsgrund
et al.	und andere
etc.	et cetera/und so weiter
EU	Europäische Union

EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
f	folgende
ff	fortfolgende
FS	Festschrift
GeschGehG	Geschäftsgeheimnisgesetz
GewArch	Gewerbearchiv, Zeitschrift für Wirtschaftsverwaltungsrecht
GG	Grundgesetz
GGVIS	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
GrC	Grundrechte-Charta
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR Int.	International Journal of European and International IP Law
GRUR-Prax	Praxis im Immaterialgüter- und Wettbewerbsrecht (Zeitschrift)
GWB	Gesetz gegen Wettbewerbsbeschränkungen
HGr	Handbuch der Grundrechte
h.M.	herrschende Meinung
HStR	Handbuch des Staatsrechts
IDNrG	Identifikationsnummerngesetz
idR	in der Regel
IMS	Identity Management System
InTeR	Zeitschrift für Innovations- und Technikrecht
IoTBDS	International Conference on Internet of Things, Big Data and Security

IPRB	IP-Rechtsberater (Zeitschrift)
iSd	im Sinne des/der
iSe	im Sinne eines/einer
iSv	im Sinne von
IT	Informationstechnik
JA	Juristische Arbeitsblätter (Zeitschrift)
JURA	Juristische Ausbildung (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	JuristenZeitung (Zeitschrift)
KG	Kammergericht
KI	Künstliche Intelligenz, auch: Zeitschrift der Gesellschaft fuer Informatik
KIT	Karlsruher Institut für Technologie
KMU	kleine und mittelständische Unternehmen
K&R	Kommunikation und Recht (Zeitschrift)
lit.	litera/Buchstabe
LVerf	Landesverfassung
MMORPG	Massively Multiplayer Online Role-Playing-Game
MMR	Zeitschrift für IT-Recht und Recht der Digitalisierung
MüKo	Münchener Kommentar
mwN	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NIS-RL	Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZFam	Neue Zeitschrift für Familienrecht
NZKart	Neue Zeitschrift für Kartellrecht
OAuth	Open-Authorization, Internetprotokoll
OZG	Onlinezugangsgesetz
PAuswG	Personalausweisgesetz
PinG	Privacy in Germany (Zeitschrift)
PIMS	Personal Information Management System
RDi	Recht Digital (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegModG	Registermodernisierungsgesetz
RL	Richtlinie
Rn.	Randnummer
RuS	Recht und Schaden (Zeitschrift)
S.	Seite
sog.	sogenannte/-r
StaatsR	Staatsrecht
StGB	Strafgesetzbuch
stRspr	stetige Rechtsprechung
StV	Strafverteidiger (Zeitschrift)
TKG	Telekommunikationsgesetz
TierSchG	Tierschutzgesetz

TMG	Telemediengesetz
TOR	The Onion Router
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
ugs.	umgangssprachlich
UWG	Gesetz gegen den unlauteren Wettbewerb
Var.	Variante
vgl.	vergleichend
VerfR	Verfassungsrecht
VersR	Zeitschrift für Versicherungsrecht, Haftungs- und Schadensrecht
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
vzbv	Verbraucherzentrale Bundesverband
WP	Working Paper
WP29	Article 29 Working Party, dt.: Artikel-29-Datenschutzgruppe
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZEV	Zeitschrift für Erbrecht und Vermögensnachfolge
ZG	Zeitschrift für Gesetzgebung
ZLR	Zeitschrift für das gesamte Lebensmittelrecht
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht
zT	zum Teil

A. Einleitung

Zu niemandem ist man ehrlicher als zum Suchfeld von Google.
– Constanze Kurz, Sprecherin des Chaos Computer Clubs

Nicht erst bei Beginn der Forschung im Rahmen der Dissertation im April 2017 zeichnete sich am digitalen wie juristischen Horizont ein Wandel ab. Zumindest kann sowohl mit den Snowden-Veröffentlichungen im (öffentlich-rechtlichen) Geheimdienstbereich seit Mai/Juni 2013[1] als auch mit Beginn des Zeitalters von Big Data – das mangels festen Zeitpunkts eher als Prozess zu begreifen ist – für den privaten Bereich angenommen werden: Kein Datum ist mehr „belanglos", keine Verknüpfung mehr unmöglich. Jedes Datum kann potentiell zu neuen Schlussfolgerungen führen, wenn auch in ferner Zukunft und in Kombination erst dann entstandener Daten. Zu diesem Schluss trägt auch die stetige Vernetzung der Welt, die zunehmende Geschwindigkeit der Datenübertragung und wachsende Speicherkapazitäten bei. Datenqualität und -quantität sind damit von signifikanter Bedeutung geworden.

Diese Entwicklung endet jedoch nicht mit Einführung von Datenschutz und Datensicherheit als Gegenstände der Rechtswissenschaften, wenngleich die mit Geltung der Datenschutzgrundverordnung ab dem 23. Mai 2018 befürchtete Abmahn-Welle[2] zunächst ein härteres, strengeres und durchgreifendes Datenschutzrecht versprach. Vielmehr gibt es einen Rahmen und Instrumente, die den brachliegenden Schutz der digitalen Identität teilweise erst aufzeigten. Die Verpflichtung

1 Exemplarisch hierzu die chronistische Aufarbeitung von *Constanze Kurz* und *Frank Rieger* mit dem Titel „Now you know. Vier Jahre Snowden", abrufbar unter https://www.nowyouknow.eu/.
2 Exemplarisch *Baumgartner*/*Sitte*, ZD 2018, 555 ff.

der Diensteanbieter aus Art. 33, 34 DSGVO zur Meldung von Datenlecks und abhandengekommenen Daten führte erst zum Bekanntwerden von Schutzlücken bei uber[3], DomainFactory[4] und Facebook[5]. Während im Jahr 2018 die Berichterstattung vom Cambridge-Analytica-Skandal[6] dominiert wurde, begann 2019 mit der Veröffentlichung zahlreicher persönlicher bzw. personenbezogener Daten von Abgeordneten und Prominenten durch den Hacker g0d[7] auf öffentlich zugänglichen Plattformen über Links zu öffentlich zugänglichen Repositories auf Twitter. Die Entwicklung des Big Data kulminierte folglich darin, dass auch in den dunkleren Ecken des Internets das Zeitalter von Big Data begonnen hatte und dies zunehmend wahrnehmbar wurde in Alltag und Öffentlichkeit.

Kurzum: Allerorts im Internet befinden sich personenbezogene Daten, oder zumindest solche, die es werden können, die jedoch vereinzelt keinem (effektiven) Schutz unterliegen. Teilweise ist dies der Fall, wenn die Wirksamkeit geltender Normen über Grenzen hinweg nicht verfolgt bzw. durchgesetzt werden kann. Schließlich kennt das Internet keine Staatsgrenzen, einmal abgesehen von der Möglichkeit des Geofencings[8]. Ferner sind anonyme Datensätze von keinerlei Norm umfasst oder der Umgang und die Verwendungsweise der Daten explizit geregelt. Ein Stand der Technik hat sich bislang ebenfalls nicht so etabliert, dass er von staatlichen Stellen einheitlich angeboten oder empfohlen wird. Kanäle der verschlüsselten E-Mail-Kommunikation sucht man vergebens, auch wenn diese

3 Siehe die Pressemitteilung von uber unter https://www.uber.com/newsroom/2016-data-incident/.

4 Hierzu https://www.heise.de/newsticker/meldung/Datenleck-bei-Domainfactory-Hacker-knackt-Systeme-laesst-Kundendaten-mitgehen-4102881.html.

5 Siehe https://www.heise.de/newsticker/meldung/Fast-50-Millionen-Facebook-Nutzer-von-Hacker-Angriff-betroffen-4178529.html.

6 Siehe hierzu https://netzpolitik.org/2018/wie-facebook-betroffene-ueber-den-datenfluss-an-cambridge-analytica-informiert/; https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

7 Dazu nur https://www.heise.de/newsticker/meldung/Massen-Doxxing-Beschuldigter-soll-Passwoerter-teilweise-im-Darknet-gekauft-haben-4270379.html.

8 Zum Begriff *Franck/Müller-Peltzer*, K&R 2016, 718 (718 f).

nunmehr durch die Datenschutz-Konferenz empfohlen werden[9]. Ferner sind Pläne wie die sichere elektronische Patientenakte, ebenfalls ein digitales Persönlichkeitsabbild, sowohl rechtlich[10] als auch technisch[11] auf unsicherem Fundament gebaut. Der Begriff „Datenschutzland Deutschland" ist in dieser Hinsicht wohl als futurologischer Fehlschluss zu begreifen.

I. Gegenstand und Ziel dieser Arbeit

Mit Blick auf die beschriebene Lage war es nur eine Frage der Zeit, bis die Digitalisierung in diesem Punkt auch rechtswissenschaftlich betrachtet wird. Der einst vom Bundesverfassungsgericht geformte Begriff des Persönlichkeitsprofils[12], welcher später im Bundesdatenschutzgesetz seine Konkretisierung fand, bedarf aufgrund der beschriebenen Entwicklung einer Überprüfung. Während dieser Begriff bislang an das personenbezogene Datum gebunden war, stellt sich die Frage, ob bei Allgegenwärtigkeit von und einfachem Zugang zu Datensätzen noch ein Personenbezug einwandfrei festgestellt werden kann oder ob der Begriff mit zunehmender digitaler Vermessung der Welt und des Menschen verschwimmt. Zu diesem Zweck wird der in der Rechtswissenschaft nur selten diskutierte, wohl aber von Marit Hansen[13] erstmals manifestierte Begriff der digitalen Identität aufgegriffen und mit Leben gefüllt. Hauptgegenstand und Ziel dieser Arbeit ist daher zum einen die Definition der digitalen Identität. Mit der dann gefassten Definition soll sich dem zweiten Komplex der Frage gewidmet werden: Ob und

9 *Datenschutzkonferenz des Bundes und der Länder*, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, insbesondere S. 7 ff.

10 Zu den verfassungsrechtlichen Anforderungen im Einzelnen *Schneider*, Einrichtungsübergreifende elektronische Patientenakten, S. 82 ff, insbes. die offen bleibenden Fragen einer nationalen Umsetzung auf S. 539. Vgl. zur elektronischen Gesundheitskarte *Ebersbach*, DSB 2013, 272 ff.

11 Hierzu anschaulich der Vortrag von *Tschiersich* „All Gesundheitsdaten Are Belong To Us" auf dem 35c3, abrufbar unter https://media.ccc.de/v/35c3-9992-all_your_gesundheitsakten_are_belong_to_us.

12 BVerfGE 65, 1 (17); 120, 274 (305); Beschluss vom 6.11.2019, Az. 1 BvR 16/13, Rn. 103 = K&R 2020, 51 (54).

13 *Hansen*/*Meints*, DuD 2006, 543 ff.

wie ist die digitale Identität im Sinne dieser Arbeit von geltendem Verfassungsrecht und seiner Konkretisierung umfasst?

Beide Kernpunkte sollten abschließend aufzeigen, welches Schutzniveau bereits exisitiert. Die Arbeit soll Lücken aufzeigen, aber auch tradierte Gedanken auf ein modernes Niveau heben und sie auf ihre Bestandskraft prüfen. Sie gleicht damit einem Stresstest für das Grundrecht auf informationelle Selbstbestimmung, das personenbezogene Datum im Datenschutzrecht oder die IT-Sicherheit des Grundrechtsträgers. Der Status Quo ist jedoch nur soweit interessant, wie er bereits beschrittenes Terrain des Neulands als Lehren des Status Quo Ante abbildet. Damit verbleibt diese Untersuchung zuletzt nicht nur bei Feststellungen, sondern gibt Ausblick auf den Status Futurus der digitalen Identität.

II. Gang der Untersuchung

Um den ersten Komplex und die Definition der digitalen Identität umzusetzen, widmet sich die vorliegende Untersuchung diesem Begriff zunächst deskriptiv, was auch auf die mangelnde juristische Literatur zur Thematik zurückzuführen ist. Daher wird zunächst inter- wie intradisziplinär auf Bruchstücke der Definition zurückgegriffen, um einzelne Merkmale der digitalen Identität herauszubilden. Sie dienen dann als Fixpunkte für die weitere Untersuchung und begrenzen den Untersuchungsgegenstand in zeitlicher wie sachlicher Hinsicht. Insbesondere ist darzustellen, ob und wie neben natürlichen Personen auch juristische Personen im Sinne des Art. 19 Abs. 3 GG als gekorene Grundrechtsträger eine digitale Identität innehaben können. Zusätzlich ist der Begriff noch zu künstlichen (virtuellen) Identitäten abzugrenzen.

Anschließend bedarf es einer Erläuterung der verfassungsrechtlichen Schutzkonzepte in Bezug auf die digitale Identität und die bereits leicht umrissenen grundrechtlichen Aspekte. Dies ist insofern notwendig, um die digitale Identität als Novum im Grundrechtsgefüge einzuordnen und abstrakt mögliche Schutzrichtungen

aufzuzeigen. Mithin dienen die Erläuterungen als Grundlage für das anschließende Kapitel.

Demgemäß sind die abstrakten Schutzaspekte zu konkretisieren, um besagten Status Quo abzubilden und Schutzlücken sowie „Updates“ vorzunehmen. Dabei ist allerdings zwischen den eingangs herausgebildeten potentiellen Grundrechtsträgern zu unterscheiden, wo sich entsprechend dem Naturell auch unterschiedlich typische Grundrechtskonstellationen bzw. Gefährdungslagen ergeben. So ist für natürliche Personen das Grundrecht auf informationelle Selbstbestimmung der Kern der Untersuchung, während für juristische Personen im Sinne des Art. 19 Abs. 3 GG vielmehr unternehmenstypische Grundrechte wie die Berufsfreiheit des Art. 12 Abs. 1 GG in Betracht kommen. Dennoch ist darzustellen, ob nicht einzelne Aspekte der digitalen Identität durch das Unternehmenspersönlichkeitsrecht geschützt sein könnten und inwiefern sich dies von der bisherigen Debatte um ein unternehmerisches Datenschutzrecht als Teil des Allgemeinen Persönlichkeitsrechts unterscheidet. Diese Untersuchung auf informationell-datenschutzrechtlicher Ebene ist um die technische Betrachtungsweise zu erweitern, sodass selbige Grundrechte auf ihren systembezogenen Schutz für natürliche und juristische Personen hin zu überprüfen sind.

Abschließend ist sich nach einer Conclusio des Kerns der Untersuchung überblickshaft dem einfachgesetzlichen Schutz de lege lata zuzuwenden und durch beabsichtigte Verbesserungen de lege ferenda zu erweitern. Auch die Möglichkeit der Verfassungsänderung am Beispiel der Charta der Digitalen Grundrechte ist zu untersuchen. Ferner wird auch zu fragen sein, ob bestehende Standards und Regelungswerke – verfassungsrechtlich wie einfachgesetzlich konkretisiert – zum Schutz der digitalen Identität in der Zukunft ausreichen.

B. Digitale Identitäten

Sämtliche Informationen, die ein Mensch in seinem Leben sammelt,
sind wie ein Tropfen im Ozean.
– Masamune Shirow, „Ghost In The Shell"

I. Inter- und intradisziplinäre Begriffsklärung

Grundlegend ist für den Gang der Untersuchung erforderlich, die Begrifflichkeit der „Digitalen Identität" zu definieren. Rein terminologisch ist sich mangels klarer Definition durch Literatur[14] oder Rechtsprechung[15] zunächst der analogen Identität interdisziplinär zuzuwenden und sodann aus einem digitalen, technischen Blickwinkel zu analysieren. Auf diesem Weg soll „die Unschärfe offengelegt und

14 Vgl. zur Menschenwürde etwa *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 1; *Kloepfer*, VerfR II, § 55, Rn. 4; *Zippelius* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 I und II GG, Rn. 15: „große Unschärfe". Nur Ansätze aufzeigend *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2, Rn. 114: „Personenbezogene Daten spiegeln ein Stück der Persönlichkeit des Menschen wider, die durch Datenerfassung, -verarbeitung usf. beeinträchtigt wird." Technisch dagegen *Strauß*, DuD 2018, 497 (498 f). Lediglich die Begrifflichkeit erwähnend *Stuckenberg*, ZIS 2016, 526 (528).

15 So äußert sich das BVerfG bislang nur verhalten und beschreibt im Rahmen der E 6, 32 (36), dass der Kernbereich der Persönlichkeit im Wesen des Menschen als geistig-sittliche Person bestehe. Diese – so E 88, 203 (251 f) – weise eine (genetische) Identität auf, welche einmalig und unverwechselbar sei und sich stetig entwickle. Der Mensch habe sich „nicht erst zum Menschen, sondern als Mensch entwickelt". An einer ausdrücklichen Definition der Identität, beispielsweise auf Ebene des Allgemeinen Persönlichkeitsrechts, fehlt es jedoch weiterhin.

produktiv genutzt werden“[16]. Dem Präfix „digital“ kommt dabei nur ein einschränkender, deskriptiver Charakter zu. Dadurch wird der Fokus auf eine bestimmte Teilmenge des allgemeinen Identitätsbegriffs auch terminologisch abgebildet.[17]

1. Analoge und philosophische Ansätze

Als Identität einer Person (in der analogen Welt) wird jener Teil bezeichnet, welcher eine Vielzahl charakteristischer Wesenszüge beinhaltet, die besonders kennzeichnend sind und so das Wesen eines Menschen einzigartig machen. Abgeleitet aus dem lateinischen Wort ĭdem, stehend für derselbe/dasselbe,[18] bezieht es sich terminologisch dagegen auf „das Gleiche“ – also entgegen der beschriebenen Diversität der Wesensmerkmale. Diese Gleichheit greift jedoch nicht die Beziehung zwischen Personen auf, sondern die fortwährende Betrachtung der Person selbst. Obschon sich die Person in ihrem Wesen von anderen unterscheidet und verändert, handelt es sich dennoch um die „gleiche“ (exakter: dieselbe)[19] Person im materiellen Sinne. Gemeint ist also vielmehr eine surjektive Beziehung zwischen einer Menge von Eigenschaften und der betrachteten Persönlichkeit.[20] So Platon: „Denn selbst solange man auch von jedem einzelnen unter den lebenden Wesen sagt, es lebe und sei dasselbe so wie man von Kindesbeinen auf derselbe genannt wird bis zum Alter. – so wird ihm diese Bezeichnung doch nur dem zum Trotze gegeben, daß man niemals dieselben Teile in sich faßt, sondern sie beständig erneuert und wieder abwirft: so Haare, Fleisch, Knochen, Blut und

16 *Hornung*/*Engemann*, Einleitung, S. 11.

17 Vgl. *Hornung*/*Engemann*, Einleitung, S. 11 (12); *Kalscheuer*/*Jacobsen*, NJW 2018, 2358 (2358).

18 Siehe Duden: http://www.duden.de/rechtschreibung/Identitaet.

19 Ebenso *Meyer*, Virtuelle Identität, S. 24 f.

20 Zumindest kann diese nur vereinzelt bijektiv sein. Bijektivität setzt voraus, dass jeder Person genau eine Eigenschaft zugeordnet werden kann, vergebene Eigenschaften letztlich nicht erneut anderen Personen zugeordnet werden können. Dies ist beispielsweise bei biologischen bzw. genetischen Faktoren wie dem Fingerabdruck oder der DNA der Fall. Surjektivität dagegen meint, dass jedem Wert X – also jeder Person – mindestens ein Wert der Menge Y – also der Menge an Eigenschaften – zugeordnet werden kann. Dies trifft z.B. auf das Geburtsdatum zu. Zu den einzelnen Begriffen siehe *Forster*, Analysis I, S. 91. Vgl. auch *Kochheim*, Cybercrime in IuK, Rn. 482.

überhaupt den gesamten Körper. Und nicht bloß mit dem Körper steht es also, sondern *auch in der Seele bleiben der Charakter, die Gewohnheiten, Meinungen, Begierden, Freude, Schmerz, Furcht, in einem jeden niemals dieselben, sondern das eine von ihnen ist erst im Entstehen, während das andere schon wieder im Vergehen begriffen ist*."[21] Es war also auch in der Philosophie ersichtlich, in welchem Umfang die Identität das Innere des Menschen bzw. die Seele einnimmt, dieser möglicherweise sogar entspricht.

2. Psychologische Ansatzpunkte

Ganz ähnliche Betrachtungen finden sich in psychologischer Hinsicht: In der Entwicklungspsychologie wird unter der Identität unter anderem das „Ergebnis" des Vorgangs verstanden, in dem das Individuum seine Persönlichkeit unter Einbeziehung der bekannten Normen und Werte, des Gelernten und Erlebten und die Einflüsse weiterer Umweltfaktoren verarbeitet und entwickelt. Sie besteht damit nicht nur aus Fakten wie Name, Adresse und Geburtsdatum, sondern auch aus Persönlichkeitsattributen, Fähigkeiten und Werten, mit denen sich eine Person definiert bzw. identifiziert und interpretiert – ist also nicht unbedingt von Geburt an vorhanden. In diesen Prozess fließen mithin Entscheidungen und deren Folgen ein.[22] Folglich richtet sich auch das Tun und Sein einer Person immer wieder neu aus. Daraus ergibt sich jedoch erst die Abgrenzbarkeit von anderen Individuen, sodass jeder Mensch einzigartig und unverwechselbar wird – oder zumindest danach strebt.[23] Einfluss auf diesen Prozess der Individualisierung nimmt darüber hinaus auch die Außenwelt, mit welcher es durch stetigen Ausgleich und fortwährende Anpassung in Relation steht.[24] Aus dem Wechselspiel von Gleichheit und Diversität ergibt sich also eine Doppelnatur, welche durch die Arbeit an und mit

21 *Platon*, Das Gastmahl (Symposion), S. 127 f. Kursive Hervorhebung nicht im Original enthalten.

22 *Roesler*, Identitätskonstruktion, S. 7 f; *Doring*, Sozialpsychologie im Internet, S. 325; *Bohley*, Identität: Wie sie entsteht und warum der Mensch sie braucht, S. 10 f sowie zur Entstehung im Detail S. 43, 45 f.

23 *Wicki*, Entwicklungspsychologie, S. 117 ff; *Keupp* in: Spektrum, Lexikon der Psychologie, Begriff Identität, Abschnitt „Begriff"; *Roesler*, Identitätskonstruktion, S. 5.

24 *Bleuler*, Schizophrenie als besondere Entwicklung, S. 19.

der Identität geprägt wird. Gerade dieser Balanceakt ist kennzeichnend für die Identitätsarbeit bzw. -konstruktion.[25] Insgesamt stellt sich die Identität damit eher als Momentaufnahme in einem komplexer Vorgang dar, welcher die Lebensaufgabe beinhaltet „die verschiedenen, oft sich widersprechenden inneren Strebungen [zu] harmonisieren, so daß [sic] wir ihrer Widersprüchlichkeit zum Trotz ein Ich, eine ganze Persönlichkeit werden und bleiben."[26]

3. Juristische Bezugspunkte der Definition

a) Natürliche Personen

Anders ist dies in juristischer Hinsicht: Der Begriff der Identität besteht vielmehr in Form der Rechte, die einer Person zustehen – sie wird zum Rechtssubjekt. Mit dem Begriff der Persönlichkeit, beispielsweise im Sinne des Allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG, ist der Begriff der Identität allerdings nicht juristisch gleichzusetzen, obschon sich Schnittpunkte und Kongruenzen beider Begriffe ergeben.[27] Mangels Erläuterungen in der Verfassung

25 So spricht *Keupp* auch vom Akt sozialer Konstruktion, siehe *ders.* in: Spektrum, Lexikon der Psychologie, Begriff: Identität, Abschnitte „Begriff" sowie „Identitätsarbeit und Identitätskonstruktion". Am Beispiel der Entwicklung in der Adoleszenz auch *Bohley*, Identität: Wie sie entsteht und warum der Mensch sie braucht, S. 46/47. Vergleichbar kennzeichnet den beschriebenen Prozess auch das Private bzw. die Privatsphäre, welche einen „vielfältig schillernden, stofflich komplexen, mitunter inkonsistenten, kulturell mehr oder weniger tief verankerten, kontextabhängigen und entwicklungssensiblen Aspekt der conditio humana" darstellen – so *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 6.

26 *Bleuler*, Schizophrenie als besondere Entwicklung, S. 19; vgl. auch *Doring*, Sozialpsychologie im Internet, S. 325.

27 Während die Identität sich schwerpunktmäßig auf der seelisch-psychischen Ebene bewegt und auch das Wechselspiel mit äußeren Reizen einbezieht, meint die Persönlichkeit im juristischen Sinne vielmehr das nach außen hin wahrnehmbare Wesen. Dennoch bedingen sich beide Begriffe; sie sind nicht sauber voneinander zu trennen. Dies zeigt sich auch an der Zitierweise des Persönlichkeitsrechts: Art. 2 Abs. 1 **iVm** 1 Abs. 1 GG – Vgl. *Stern*, StaatsR IV/1, § 97, S. 97 f sowie § 99, S. 185; *Höfling* in: Sachs, GG, Art. 1, Rn. 37 f; *Hufen*, Staatsrecht II, § 10, Rn. 14. Die Identität als Schutzrichtung des Persönlichkeitsrechts annehmend *Herrmann*, ZUM 1990, 542. Dagegen ablehnend, da keine feste Substanz aufweisend *Ladeur* in: Götting/Schertz/Seitz, Handbuch des Persönlichkeitsrechts, § 7, Rn. 8.

ergeben sich weitere Kriterien für das Dasein des Rechtssubjekts aus einfachgesetzlichen Regelungen, welche letztlich die Ausgestaltung der Verfassung darstellen. So beginnt die Rechtsfähigkeit gem. § 1 BGB bereits mit der Vollendung der Geburt. Ab diesem Zeitpunkt ist der Säugling Träger von Rechten und Pflichten. Es kommt also nicht auf eine tatsächliche Handlungsfähigkeit in juristischer Hinsicht an.[28] Hiervon ist die juristische Handlungsfähigkeit im Sinne der Geschäftsfähigkeit der §§ 104 ff BGB – also der Fähigkeit, wirksam Rechtsgeschäfte abzuschließen und so Rechtsbeziehungen zu anderen Rechtssubjekten einzugehen – zu trennen.[29] Die Fähigkeit, Träger von Rechten und Pflichten zu sein, fußt mithin nicht auf einer liberalen Weltanschauung des homo oeconomicus[30], sondern auf der Menschenwürde-Formel des Art. 1 Abs. 1 GG. Die Rechtsfähigkeit des Menschen ist Teil der Würde, ihre Nutzung Ausdruck von Selbstbestimmung und freier Entfaltung.[31] Sie ist damit zugleich Vorbedingung für die Grundrechte, insbesondere für jene aus Art. 2 Abs. 1 sowie Art. 2 Abs. 1 iVm 1 Abs. 1 GG.[32] Teil der Menschenwürde sind daneben sämtliche identitätsstiftenden und -prägenden

28 *Bamberger/Poseck* in: Hau/Poseck, BeckOK BGB, § 1 BGB, Rn. 10.

29 Schließlich stellt die Geschäftsfähigkeit die Fähigkeit dar, Rechtsgeschäfte wirksam und selbstständig vornehmen zu können – *Wendtland* in: Hau/Poseck, BeckOK BGB, § 104 BGB, Rn. 1.

30 Bezugnehmend darauf, dass der homo oeconomicus unter Kenntnis aller Rechte von Beginn an diese gewinnbringend gemäß der Zweck/Mittel-Relation nutzen würde. Vgl. *Kirchgässner*, Homo Oeconomicus, S. 13 ff, 47 f; *Eidenmüller*, JZ 2005, 216 (217 f).

31 Vgl. BVerfGE 45, 187 (227).

32 *Bamberger/Poseck* in: Hau/Poseck, BeckOK BGB, § 1 BGB, Rn. 1; vgl. *Kloepfer*, VerfR II, § 55, Rn. 23; *Zippelius* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 I und II GG, Rn. 79 f. Eine naturrechtliche Herleitung der Freiheit bemühend *Nipperdey* in: Neumann/Nipperdey/Scheuner, Grundrechte II, S. 1 f.

Merkmale, wie zum Beispiel der eigene Name[33] oder dazugehörige Pseudonyme[34] sowie Sexualität[35], Religiösität[36] und die Gedankenfreiheit[37].[38] Mehr noch, bilden die nachfolgenden Grundrechte in ihrem Charakter als objektive Normen- und Wertordnung ein „Menschenbild des Grundgesetzes“[39], sodass einzelne Teile der Identität durch spezielle Grundrechte besonderen Schutz genießen.[40] So bildet sich unter dem Schutzmantel der objektiven Wertordnung die in einem Menschen verkörperte, einzigartige, unauswechselbare und unvertretbare Identität heraus.[41]

b) Juristische Personen

Im Laufe der bereits dargelegten Betrachtung mag der Eindruck entstanden sein, dass Rechtssubjekte in verfassungsrechtlicher Hinsicht nur natürliche Personen sein können. Dem Eindruck kann jedoch nicht entsprochen werden. Richtet man den Blick auf Art. 19 Abs. 3 GG, wonach eine Grundrechtsträgerschaft juristischer Personen des Privatrechts grundsätzlich möglich ist, sind auch diese verfassungsrechtlichen Rechtssubjekte in die Untersuchung einzubeziehen.[42] Für bestimmte

33 Vgl. BVerfGE 97, 391 (399). Zum Rufnamen insbesondere *Döring*, DVBl 2018, 560 (561).

34 Allerdings nur, soweit sich mit ihnen die Identität und Individualität des Pseudonym-Nutzers verfestigt haben – vgl. BVerfG, Nichtannahmebeschluss vom 21. August 2006 – 1 BvR 2047/03 –, Rn. 15; vgl. auch *Kochheim*, Cybercrime in IuK, Rn. 492.

35 *Kloepfer*, VerfR II, § 55, Rn. 27.

36 Zur religiösen Prägung des Menschenwürde-Begriffs *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 55 ff.

37 Vgl. BVerfG NJW 1982, 375 in Bezug auf Lügendetektoren oder seien es verkörperte Gedanken als Tagebuch wie in BVerfGE 80, 367 (373 f).

38 Zu beachten ist, dass es sich vorliegend nur um eine exemplarische Aufzählung handelt. Sowohl Menschenwürde als auch Identität unterliegen einem ständigen Wandel und in einer pluralistischen Gesellschaft auch einem immer anders geprägten Verständnis. Eine trennscharfe Einordnung ist danach nicht möglich. – Vgl. *Kloepfer*, VerfR II, § 55, Rn. 4. Eine Erläuterung versuchend *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 2, 6, 45 ff; ebenso *Stern*, StaatsR IV/1, § 97, II. 4. b). Weitere identitätsstiftende Merkmale nennend *Enders* in: Merten/Papier, HGr IV, § 89, Rn. 6 sowie *Meyer*, Virtuelle Identität, S. 23.

39 BVerfGE 4, 7 (15 f); 41, 29 (50); *Kloepfer*, VerfR II, § 55, Rn. 3 aE.

40 Vgl. *Kloepfer*, VerfR II, § 55, Rn. 78; kritisch zum Verhältnis zu anderen Grundrechten *Nipperdey* in: Neumann/Nipperdey/Scheuner, Grundrechte II, S. 14 f.

41 *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 169.

42 Eine Untersuchung öffentlich-rechtlicher juristischer Personen entfällt vorliegend mangels einer Grundrechtsträgerschaft. Zur Unterscheidung sub B.III.2.

Aspekte des Persönlichkeitsrechts kann dies beispielsweise angenommen werden,[43] gegebenenfalls könnte auf Art. 12 Abs. 1 und 14 Abs. 1 GG zurückgegriffen werden. Eine detailliertere Prüfung, ob und welche Aspekte der digitalen Identität dem verfassungsrechtlichen Schutz unterliegen, wird zu einem späteren Zeitpunkt vorgenommen.[44] Hierfür ist allerdings Voraussetzung, dass auch juristische Personen eine digitale Identität besitzen bzw. entwickeln können.

Entsprechend der vorangegangenen Prüfung bedarf es ebenfalls einer analogen Identität eines Unternehmens. Schon terminologisch andeutend, bietet sich hierfür der Begriff der Corporate Identity an – zu deutsch: Unternehmensidentität. In seine Einzelteile zerlegt, verweist der Begriff „Corporate" zunächst auf die Eigenart der *unternehmerischen* Identität und so auf die Unterscheidung zur menschlichen Identität. „Identity" bezieht sich dagegen auf den Identitätsbegriff, welcher sich zunächst aus dem bereits dargelegten speist. Kennzeichnend für Unternehmen ist aber nicht der seelisch-emotionale Bezug zur Außenwelt ähnlich des Menschenwürde-Aspekts im Rahmen des Persönlichkeitsrechts des Art. 2 Abs. 1 iVm 1 Abs. 1 GG bei natürlichen Personen[45], sondern der Bezug zwischen Unternehmen und Mitarbeitern. Jeder Mitarbeiter soll sich dem Unternehmen zugehörig fühlen und die Relevanz des Selbst im „großen Getriebe" des Unternehmens kennen. Um trotz der aufgrund der verschiedenen Mitarbeiter-Persönlichkeiten existierenden Diversität eine Einheitlichkeit des Unternehmensbildes unter den Mitarbeitern zu schaffen, bedarf es der Formung einer Unternehmenspersönlichkeit. Oftmals enthält diese einheitliche Maßstäbe oder Leitlinien zum Denken

43 Vorweggenommen sei an dieser Stelle, dass eine Anwendung nach wie vor umstritten ist und durch das BVerfG zT abgelehnt wurde – BVerfGE 95, 220 (242); auch *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2 GG, Rn. 50. Anders dagegen *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 33 f.

44 Siehe Kapitel D.I.2.

45 Vgl. BVerfGE 65, 1 (41 f) sowie *Gurlit*, NJW 2010, 1035 (1036) mwN zum Ausschluss der Eigenschaft für juristische Personen: Soweit die informationelle Selbstbestimmung fernab der wesensmäßigen Eigenschaften der natürlichen Personen aus Art. 1 Abs. 1 GG anknüpft, sondern sich auf unternehmensbezogene Informationen bezieht, ist schwerpunktmäßig die informationelle Selbstbestimmung mit ihrem Kern in Art. 2 Abs. 1 GG anwendbar.

und Handeln sowie den Leistungen des Unternehmens.[46] Indem sie durch die Mitarbeiter gelebt und repräsentiert bzw. in (Re-)Präsentationen des Unternehmens (z.B. Werbung, öffentlichkeitswirksame Präsentationen, etc) berücksichtigt werden, bilden sich die abstrakten Merkmale und Attribute der Unternehmensrichtlinien in der Unternehmenspersönlichkeit aus. Die Kernfragen der Identität – Wer bin ich? Wer möchte ich sein? Wie werde ich wahrgenommen? –, aus denen sich die Antworten und somit die Unternehmensidentität ergeben,[47] stimmen daher spiegelbildlich mit denen der menschlichen Identitätskonstruktion überein. Anstatt Aussagen mit möglicherweise seelisch-moralischem Ursprung entwickeln Unternehmen zum Herausstellen der Einzigartigkeit des Unternehmens bestimmte Kennzeichen (z.B. Jingles/Tonmarken, Logos, Werbefiguren, Designs, Düfte) oder ein bestimmtes Image, um die o.g. Fragen zu beantworten. Insofern besteht ein Zusammenhang mit dem „Inneren" des Unternehmens nicht aufgrund einer Würde iSd Art. 1 Abs. 1 GG, sondern eher um Aspekte der Zielgruppe des Unternehmens widerzuspiegeln oder Unternehmenszwecke nach Außen zu bringen.[48] Der Firmenkern[49] und die damit verknüpften Merkmale des Unternehmens als Teil des Corporate Designs[50] dienen folglich als Pendant zum menschlichen Persönlichkeitskern.

Zweck der Corporate Identity ist des weiteren die Differenzierung von und Profilierung gegenüber anderen Unternehmensidentitäten in der Außenwirkung.[51] Als Indiz hierfür lässt sich § 18 HGB anführen, welcher ausdrücklich die Unterscheidungskraft des Firmennamens zum Zwecke der Individualisierung benennt.[52] Dies lässt auf Parallelen zum Wechselspiel im Außenverhältnis bei der menschlichen

46 *Herbst*, Corporate Identity, S. 28 f; *Kiessling*/*Spannagl*, Corporate Identity, S. 12; *Quante*, Das allgemeine Persönlichkeitsrecht juristischer Personen, S. 94 f; vgl. auch *Regenthal*, Ganzheitliche Corporate Identity, S. 18 f sowie Abb. 3 auf S. 25.

47 *Herbst*, Corporate Identity, S. 28; vgl. *Kiessling*/*Spannagl*, Corporate Identity, S. 16 f.

48 Vgl. zu Corporate Behaviour und Corporate Communications *Kiessling*/*Spannagl*, Corporate Identity, S. 18 ff.

49 Vgl. *Merkt* in: Baumbach/Hopt, HGB, § 18 HGB, Rn. 8.

50 *Kiessling*/*Spannagl*, Corporate Identity, S. 32 f.

51 *Herbst*, Corporate Identity, S. 34 f; als Wiedererkennungswert beschreibend *Kiessling*/*Spannagl*, Corporate Identity, S. 34.

52 Vgl. *Merkt* in: Baumbach/Hopt, HGB, § 18 HGB, Rn. 4 f.

Identität schließen. So kann sich durch die unternehmerische Beziehung zur Außenwelt auf dem Markt zunächst die Identität aus den Interessen des Marktes generieren. Zugleich aber wirkt der stetig verändernde Markt auch in Zukunft auf die Unternehmensidentität ein und prägt diese mit.[53] Dies wird zum Beispiel bei einer Veränderung einer Marke trotz (teilweise) gleichbleibender Werte der Corporate Identity deutlich.[54] Mit dem Fortschritt und der Entwicklung der Ansichten und Interessen innerhalb einer Gesellschaft geht oftmals ein Wandel des Unternehmensbildes einher, um weiterhin die Interessen der Konsumenten abdecken zu können. Auf diese Weise entsteht auch hier ein Wechselspiel aus den verschiedenen inneren – innerhalb des Unternehmens zwischen den Mitarbeitern – und äußeren – aus den verschiedenen Interessen von Markt und Unternehmen – Einflüssen.[55] Resultat dieses Prozesses ist sodann eine Corporate Identity, welche aufgrund der Nähe zum Menschen wiederum selbst nahezu menschenähnlich wird. Dies ergibt sich schon aus dem Offensichtlichen; Unternehmen bestehen aus einer Vielzahl an Menschen und Persönlichkeiten. Aber auch aus den identitätsbildenden Fragen ergeben sich Attribute oder Merkmale, welche üblicherweise Menschen zuzuordnen sind. Unternehmen sind „cool", „sexy" oder „konservativ" und „traditionsbewusst".[56] Grund hierfür ist wiederum die Beziehung zum Kunden im Außenverhältnis, damit sich der Kunde mit den Werten der Corporate Identity identifiziert;[57] Marken und Produkte des Unternehmens werden „personalisiert"[58]. Unter anderem soll im Unternehmen auch der beste Freund gesehen werden[59] oder als Unternehmen, das sich besonders für die Rechte von sog.

53 So auch BVerfGE 105, 252 (278).

54 Hierzu *Herbst*, Corporate Identity, S. 42 f am Beispiel des BMW-Logos. Weitere Gründe für eine Modernisierung der Corporate Identity können auch eine Änderung des Aufgabenprofils oder eine generelle (auch personelle) Umstrukturierung sein – siehe *Kiessling*/*Spannagl*, Corporate Identity, S. 45 f.

55 Diesen Prozess beschreibend siehe *Regenthal*, Ganzheitliche Corporate Identity, S. 14 f sowie schematisch Abb. 6 auf S. 29.

56 *Herbst*, Corporate Identity, S. 35; *Kiessling*/*Spannagl*, Corporate Identity, S. 33.

57 *Herbst*, Corporate Identity, S. 70; *Kiessling*/*Spannagl*, Corporate Identity, S. 41; *Korneeva*, Das Persönlichkeitsrecht des Unternehmens, S. 139.

58 *Meissner*, Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht, S. 159.

59 *Herbst*, Corporate Identity, S. 35.

Core-Gamern einsetzt[60]. Hinzu tritt die Möglichkeit, dem Unternehmen durch bestimmte Handlungsweisen der Unternehmenspersönlichkeit Emotionen zu verleihen bzw. mit diesen Emotionen bei Kunden hervorzurufen. Dies kann, um nur einige Methoden zu nennen, durch die persönliche Ansprache der Mitarbeiter[61] (Nähe, Freundschaft, Familie, Sicherheit) oder vorgeschriebene formelle Kleidung (Autonomie, Elite, Stolz, Ruhm) bewirkt werden.[62] Berücksichtigt man nun das bereits zur analogen Identität des Menschen Gesagte, werden die Parallelen sichtbar, sodass nach der hier vertretenen Ansicht auch Unternehmen eine Identität iSe Unternehmenspersönlichkeit zugesagt wird.[63] Diese kann, wie sogleich erläutert, auch unter Nutzung neuer Kommunikationsmedien wie Nutzerkonten in sozialen Netzwerken[64] um entsprechende Komponenten erweitert werden und sich so in digitaler Form manifestieren.

c) Datenschutzrecht und Identitätsmanagement

Nutzt eine natürliche oder juristische Person informationstechnische Systeme jeglicher Art, überträgt sie ihre individuelle Nutzungsweise und weitere Merkmale der analogen Identität in die digitale Welt. In dieser technischen, digitalen Welt findet sich das dargestellte Konzept der menschlichen Identität als Ganzes hingegen nur bedingt wieder. An keinem öffentlich zugänglichen (Speicher-)Ort befindet

60 Bezugnehmend auf den Werbeslogan „This is for the players.“, mit welchem Sony die hauseigene Videospielkonsole bewarb. Der Solgan richtet sich hauptsächlich an Videospieler mit langjähriger Videospiel-Vergangenheit und entsprechender Erfahrung (sog. Core Gamer), um sich von anderen Videospielkonsolen-Anbietern wie Nintendo, welche hauptsächlich familienfreundliche Videospiele vertreiben, abzugrenzen.

61 Hierzu auch *Regenthal*, Ganzheitliche Corporate Identity, S. 25: „Das direkte persönliche Ansprechen bringt eine starke Bewusstmachung und Motivation.“

62 Vgl. *Herbst*, Corporate Identity, S. 52 f.

63 Dieser Ansicht ebenso *Meissner*, Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht, S. 159 ff.

64 Hierzu *Schwartmann/Ohr* in: Schwartmann, Praxishandbuch Medien-, IT- und Urheberrecht, § 11, Rn. 229 ff. Beachtenswert ist, dass *Schwartmann/Ohr* hierbei darauf hinweisen, dass die Ausbildung der digitalen Identität auch ohne Einfluss des Unternehmens vonstatten gehen kann – beispielsweise durch Bewertungsportale oder die öffentliche Diskussion in den Medien – und eine Nutzung der Plattformen notwendig ist.

sich die (vollständige) digitale bzw. digitalisierte Identität einer Person. Stattdessen entsteht bei jedem neuen Benutzerkonto oder jedem neuen Gerät eine neue Variation der digitalen Identität – auch bezeichnet als Teilidentität –, sodass eher von einer Vielzahl von digitalen Identitäten je analoger Identität auszugehen ist.[65] Eine nahezu vollständige digitale Identität kann folglich nur durch Akkumulation, Analyse und Verkettung großer Datenmengen gewonnen werden.[66] Demnach können im Folgenden nur Teilidentitäten als einzelne Fragmente der digitalen Gesamt-Identität mit dem Begriff der digitalen Identität bezeichnet werden. Mehr noch, wird diese Sichtweise durch die Ansicht der Persönlichkeit als facettenreiches und individuelles Wesen gestützt, da durch die Ausübung der Persönlichkeitsrechte der Grundrechtsträger selbst bestimmt, wie er sich darstellt und welche einzelnen Facetten er in die jeweilige digitale Identität einbringen will.[67] Es entstehen so nicht immer wieder gleiche Kopien ein und desselben Egos, sondern einzelne Spielarten, die nicht notwendigerweise einen Bezug zur Realität haben müssen.[68] So können beispielsweise gerade scheue oder introvertierte Persönlichkeiten im digitalen Raum gegensätzlich auftreten, da ihnen der Deckmantel der Pseudonymität und Anonymität gemäß Art. 2 Abs. 1 iVm 1 Abs. 1 GG sowie § 3a BDSG a.F. bzw.

65 So auch *Camenisch*/*Leenes*/*Sommer*, Digital Privacy, S. 35 f; *Hornung*/*Engemann*, Einleitung, S. 11 (13); *Kühnl*, Persönlichkeitsschutz 2.0, S. 20 f; *Pfitzmann/Borcea-Pfitzmann* in: Roßnagel, Allgegenwärtige Identifizierung?, S. 83 (84/85); *Strauß*, DuD 2010, 99 (100). Vgl. ebenfalls *Kochheim*, Cybercrime in IuK, Rn. 482, 494; *Petrlic*/*Sorge*, Datenschutz, S. 12; *BITKOM*, Web Identitäten, S. 6 f; *Herrmann*/*Federrath*, Unbemerktes Tracking im Internet: Unsere unerwünschte Identität, S. 131 (132 f); *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2, Rn. 114. In psychologischer Hinsicht auch *Doring*, Sozialpsychologie im Internet, S. 325 f, 346 sowie im Detail zur Aktivierung verschiedener Identitäten S. 354 ff. Andeutend auch BVerfG, Beschluss vom 6.11.2019 – Az. 1 BvR 16/13 –, Rn. 103.

66 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Verkettung digitaler Identitäten, S. 22 f sowie zum Vorgang der Verkettung S. 26 f. Die Erstellung einer vollständigen digitalen Identität ist gewissermaßen die Aufgabe von „Big Data" – vgl. *Hoeren*, Big Data und Recht, S. 3 ff; *Humer*, Identitätsarbeit in digitalen Systemen, S. 158; *Albrecht*/*Jotzo*, Das neue Datenschutzrecht der EU, § 3, Rn. 3.

67 *Camenisch*/*Leenes*/*Sommer*, Digital Privacy, S. 35, 36 f; *BITKOM*, Web Identitäten, S. 4, 6 f; *Meyer*, Virtuelle Identität, S. 52 f; vgl. *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 7.

68 So auch *Humer*, Identitätsarbeit in digitalen Systemen, S. 149 f sowie vgl. *Humer*, Digitale Identitäten, S. 132 f.

Art. 4 Nr. 5 DSGVO, § 46 Nr. 5 BDSG die Freiheit der Meinungsäußerung ohne eine Prangerwirkung gewährt wird.[69] Die Unternehmenspersönlichkeit juristischer Personen basiert mithin auf der Ausgestaltung der einzelnen Facetten ohne Realitätsbezug, sodass für deren Betrachtung eine derartige Sichtweise unschädlich ist. Auch wenn die digitalen Identitäten der einzelnen Mitarbeitern folgerichtig isoliert betrachtet werden können, ergibt sich aus der Gesamtheit an Attributen in Verbindung mit Charakteristika der Außenkommunikation ein eigenständiges Bild.

Zusammengefasst stellt sich die erwähnte surjektive/injektive Beziehung zwischen der Gesamtheit aus Eigenschaften, Attributen, etc. und der Persönlichkeit dar. Per definitionem sind digitale Identitäten daher, orientiert am ursprünglich technischen Begriff aus dem Identitätsmanagement in informationstechnischen Systemen,[70] als Sammlung digitaler Informationen bezüglich eines Nutzers von Informationssystemen zu definieren.[71] Unter letzteres sind regelmäßig Dienstleistungen der Telekommunikation (bspw. Übertragungsleistung und dazu erforderliche IP-Vergabe) sowie in Form von Telemedien (Apps, Webseiten, etc.) gefasst. Der Nutzer, gleich ob natürliche oder juristische Person,[72] bedient sich hierbei einer Kennung in Form bestimmter Login-Daten (regelmäßig E-Mail-Adresse und

69 Zur Anonymität im demokratischen Diskurs siehe *Kersten*, JuS 2017, 193 (201 f). Sei die Prangerwirkung – wie beispielsweise von *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 148 in Fn. 435 beschrieben – dennoch gegeben, so kann sich dieser zumindest einfacher entzogen werden, indem Nutzerkonten schlichtweg gelöscht werden oder ein neues Pseudonym genutzt wird. Dies setzt jedoch voraus, dass keine anderen „Spuren" mit in die neue digitale Identität übernommen werden. Zum Anonymitätsschutz in der Sozialsphäre siehe auch *Brost*/*Conrad*, AfP 2017, 286 (287/288). Vgl. auch BVerfGK 18, 42 (53 f).

70 *Schallaböck*, Identitätsmanagement als Grundlage von Verhaltenssteuerung, S. 103 (104 f, 107 ff); *Petrlic*/*Sorge*, Datenschutz, S. 67, 12; *Windley*, Digital Identity, chapter 2; *Hühnlein*, DuD 2008, 161.

71 *Hansen*/*Meints*, DuD 2006, 543 (543); *Meyer*, Virtuelle Identität, S. 31. Daneben sei angemerkt, dass der Terminus der digitalen Identität häufig als Synonym für die mit dem elektronischen Personalausweis und dem neuen Reisepass verbundene Identität verwendet wird – so z.B. *Doring*, Sozialpsychologie im Internet, S. 344 und *Eckert*, IT-Sicherheit, S. 540 ff.

72 *Hansen*/*Meints*, DuD 2006, 543 (543).

Passwort), um die Zuordnung zwischen digitaler Identität und Daten herzustellen. Eine Verbindung zwischen analoger und digitaler Identität im Sinne einer Personenbeziehbarkeit ist jedoch nicht immer gegeben.[73]

Konsequent muss allerdings in Anbetracht der datenschutzrechtlichen Prägung dieser Definition zwischen personenbeziehbaren und nicht-personenbeziehbaren digitalen Identitäten differenziert werden. Während erstere typischerweise dann vorliegen, wenn Profile in sozialen Netzwerken mit Identitätsdaten gespeist werden (z.B. eigenes Bild, Klarname, etc.)[74] und ggf. die Nutzung auch mit einem Pseudonym erfolgt, liegen letztere insbesondere dann vor, wenn das Profil nur an eine vom Plattformbetreiber geschaffene Identität (z.B. mittels zufallsgeneriertem Benutzernamen)[75] oder lediglich an E-Mail (ohne den Klarnamen zu enthalten) und Passwort als Login-Daten geknüpft ist – in diesem Sinne einer anonymen Nutzungsweise[76] entspricht.[77] Die Grenze zwischen beiden Varianten ist allerdings diffus, da schon durch einzelne Attribute bzw. Informationen die Verschleierung der wahren Identität aufgelöst werden kann,[78] insbesondere durch die erwähnte E-Mail-Adresse mit Klarnamen. Insoweit kann der Personenbezug, ganz nach dem Wortlaut von Art. 4 Nr. 1 sowie dem Erwägungsgrund 26 DSGVO, nur im

73 *Hansen*/*Meints*, DuD 2006, 543 (543); *Humer*, Identitätsarbeit in digitalen Systemen, S. 149.

74 *Kühnl*, Persönlichkeitsschutz 2.0, S. 21 f; *Hühnlein*, DuD 2008, 161; *Meyer*, Virtuelle Identität, S. 31; vgl. auch Art. 4 Nr. 1 DS-GVO sowie dazu *Gola* in: Gola, DS-GVO, Art. 4, Rn. 16 f sowie *Krügel*, ZD 2017, 455 (456, 459) unter Verweis auf ErwGr 26 der DSGVO.

75 Darunter fallen insbesondere jene Identitäten, die zum Zwecke des Trackings über mehrere Webseiten oder anderweitige Angebote des Plattformbetreibers angelegt werden. Neben der Datensammlung ist für diese Art der digitalen (Teil-)Identität jedoch vielmehr, dass sie ohne entsprechende aufgeklärte Einwilligung — da in AGB verklausuliert oder in Ermangelung einer Nutzungsalternative – oder gänzlich abseits des Bewusstseins des Identitätsinhabers und Nutzers angelegt wird. Wichtig ist an bei der Betrachtung von digitalen Identitäten daher nicht, ob sie bewusst oder unbewusst vom Identitätsinhaber angelegt und gepflegt wird. Schließlich unterliegen in Anlehnung an BVerfGE 65, 1 personenbezogene Daten unabhängig ihres Inhalts dem Schutz der informationellen Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Es kann daher nur auf die Rückführbarkeit und Zuordenbarkeit der generierten Daten ankommen.

76 Hierzu *Doring*, Sozialpsychologie im Internet, S. 344; *Ziebarth* in: Sydow, DS-GVO, Art. 4, Rn. 24 f unter Verweis auf ErwGr 26 der DSGVO sowie *Roßnagel*/*Scholz*, MMR 2000, 721 (723, 725 f, 727) hinsichtlich mehrerer Arten der Pseudonymität.

77 Vgl. *Ziebarth* in: Sydow, DS-GVO, Art. 4, Rn. 15 ff, 17.

78 Ähnlich *Ziebarth* in: Sydow, DS-GVO, Art. 4, Rn. 21. Vgl. EuGH, Urteil vom 19.10.2016, Az. C-582/14 – Breyer –, Rn. 25 f.

Einzelfall mit Fokus auf den Verantwortlichen bzw. Datenverarbeitenden ermittelt werden. Ein abstrakter, stets vorhandener Personenbezug für alle Beteiligten des Internets ist abzulehnen. Für den terminus der digitalen Identität ergeben dahingehend nur Unterschiede in ihrem rechtlichen Schutz, welcher in der konkreten Betrachtung zu differenzieren ist.[79] Beide Varianten der Profilbildung sind digitale Identitäten nach der dargestellten Definition.

Darüber hinaus könnte bei der vollständigen Loslösung der digitalen von der analogen Identität wiederum von einer virtuellen Identität gesprochen werden, soweit sie durch ihre Ausformung und Eigenständigkeit einer Identität im analogen Sinne nahe kommt. Nach *Meyer* ist eine virtuelle Identität hingegen jedes „Nutzerprofil einer Person, das auf Dauer angelegt ist, konsistent genutzt wird und daher für andere Nutzer wiedererkennbar ist, ohne dass sich die dahinterstehende natürliche Person erkennbar ist."[80] Ähnlich versteht *Döring* aus psychologischer Sicht darunter jede „mehrfach in konsistenter und für andere Menschen wieder erkennbarer Weise verwendete, subjektiv relevante Repräsentation einer Person".[81] Dies entspricht im Ergebnis aber auch einer pseudonymen Nutzungsweise der digitalen Identität gegenüber dem Diensteanbieter, wenn beispielsweise im Wege der Foren-Nutzung der eigene Benutzername an Beliebtheit und Bekanntheitsgrad gewinnt und sich so zu einer eigenständigen Persönlichkeit entwickelt, der Personenbezug allerdings nur für den Diensteanbieter bzw. Betreiber herstellbar ist. Auch ist dies der Fall, wenn es sich um eine Nutzung gegen Zahlung einer monatlichen Gebühr handelt, wie es regelmäßig bei Online-Rollenspielen zu finden ist.[82] Der Begriff

79 Siehe Kapitel D.I.1.a).

80 *Meyer*, Virtuelle Identität, S. 54 sowie gleichermaßen beschreibend *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 147; *Golland*/*Kriegesmann*, PinG 2017, 45 (46). Ähnlich im Bereich der MMORPG-Videospiele die Begriffe der virtuellen und digitalen Identität vermischend *Krasemann*, DuD 2008, 194 (195). Zur virtuellen Identität iSe virtuellen Persönlichkeit siehe auch *Holznagel* in: Hoeren/Sieber/Holznagel, Handbuch MultimediaR, Teil 8, Rn. 8. Dagegen nicht zu verwechseln mit dem Begriff des „digitalen Zwillings", wenngleich sich hierzu Parallelen finden lassen – hierzu *Kuhn*, Informatik Spektrum 2017, 440 (440 f).

81 *Doring*, Sozialpsychologie im Internet, S. 341. Begrifflich ähnlich, allerdings ohne definitorischen Ansatz, *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 147.

82 Das Angebot der Mitgliedschaft zur Nutzung der Software – beispielsweise des Online-Rollenspiels/MMORPG – ist üblich und unter Angabe des Kreditkarten-Inhabers u.U. auf den Inhaber der Zugangsdaten zurückführbar iSd Art. 4 Nr. 1 DSGVO.

von *Meyer* und *Döring* geht daher im dargelegten Begriff der digitalen Identität auf.

Auf juristischer Ebene ist abschließend zu hinterfragen, ob es überhaupt der neuen Begrifflichkeit der „digitalen Identität" bedarf oder sich eine Zuordnung zu bestehenden Begriffen vornehmen lässt. Zu denken ist hierbei an Begriffe aus dem Datenschutzrecht, insbesondere jenen der personenbezogenen Daten oder den des Persönlichkeitsprofils[83]. Gemäß § 3 Abs. 1 BDSG a.F. sowie Art. 4 Nr. 1 DSGVO sind Daten personenbezogen, sofern sie Aussagen persönlicher oder sachlicher Natur enthalten und dieser Person zugeordnet werden können.[84] Die Zuordenbarkeit ist dabei entsprechend weit zu fassen; schon die tatsächliche Möglichkeit einer Zuordnung über gewährte Informationsansprüche iSd relativen Theorie reicht aus.[85] „Person" kann dabei nur eine natürliche Person sein – sowohl nach §§ 1 Abs. 1, 3 Abs. 1 BDSG a.F. als auch nach Art. 4 Nr. 1 DSGVO und § 46 Nr. 1 BDSG. Damit sind juristische Personen expressis verbis nicht vom Begriff der personenbezogenen Daten umfasst, wenngleich ihnen einzelne verfassungsrechtliche Interessen aus dem Allgemeinen Persönlichkeitsrecht zugesprochen werden.[86] Das (einfachgesetzliche) Datenschutzrecht bezieht sich mithin nahezu ausschließlich auf den

83 Die Verknüpfung ist insoweit iSd Verarbeitung gem. § 15 Abs. 3 TMG a.F. sowie § 1 Abs. 2 Nr. 3 i.V.m. § 3 Abs. 3, 4 BDSG a.F. vom Datenschutzrecht erfasst — *Tinnefeld/Buchner* in: Wolff/Brink, BeckOK DatenschutzR (23. Edition), Grundlagen – Medien, Rn. 92, 93; *Moos*, MMR 2006, 718 (719); *Peifer*, K&R 2011, 543 (544 f).

84 Zur Einordnung der Regelbeispiele des Art. 4 Nr. 1 DSGVO siehe *Ernst* in: Paal/Pauly, DSGVO, Art. 4, Rn. 14 sowie *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1, Rn. 3 ff.

85 Siehe EuGH, Urteil vom 19.10.2016, Az. C-582/14 = CR 2016, 791 m. Anm. Nink sowie vgl. Art. 4 Nr. 1, ErwGr 26, 30 DSGVO. Befürwortend ebenfalls *Gola* in: Gola, DS-GVO, Art. 4, Rn. 18; *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1, Rn. 26; *Krügel*, ZD 2017, 455 (459) unter Hinzunahme eines Korrektivs zur Auslegung des ErwGr 26. Ausführlich anhand Auslegung siehe *Hofmann/Johannes*, ZD 2017, 221 sowie *Roßnagel*, ZD 2018, 243 (244 f). Krit. dagegen *Ziebarth* in: Sydow, DS-GVO, Art. 4, 37 f.

86 *Ernst* in: Paal/Pauly, DSGVO, Art. 4 DSGVO, Rn. 5 sowie *Frenzel* in: Paal/Pauly, DSGVO, § 46 BDSG, Rn. 3; *Ziebarth* in: Sydow, DS-GVO, Art. 4, Rn. 13; *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1, Rn. 4. Krit. zum Datenschutzrecht juristischer Personen *Gola* in: Gola, DS-GVO, Art. 4, Rn. 23 ff. Ebenfalls hierzu Kapitel D.I.2.d).

Schutz natürlicher Personen.[87] Insoweit unterscheidet sich das Verständnis des personenbezogenen Datums vom Begriff der digitalen Identität, als dass letzterer auch juristischen Personen in die Definition einbezieht.

Weiterhin bleibt der Begriff des Persönlichkeitsprofils auf seine Tauglichkeit zu überprüfen. Erstmalig benannt und erläutert wurde der Begriff in der Volkszählungsentscheidung des Bundesverfassungsgerichts. Persönlichkeitsprofile zeichnen sich demzufolge durch die „Erstellung eines umfassenden und detaillierten Bildes der jeweiligen Person" aus; das Schlagwort des „gläsernen Menschen" entstand.[88] Der damit beschriebene Vorgang hat im Datenschutzrecht im Rahmen des Umgangs mit personenbezogenen Daten Anklang gefunden und ähnelt daher dem Wortlaut des § 3 Abs. 2-4 BDSG a.F. Konkret wird er dagegen bei der Erstellung zum Zwecke der Werbung, Marktforschung oder zur bedarfsgerechten Gestaltung der angebotenen Telemedien in Form von Nutzungsprofilen erwähnt, § 15 Abs. 3 TMG a.F.[89] Daneben findet er sich im Sinngehalt datenschutzrechtlicher Prinzipien[90] wieder, beispielsweise der Datensparsamkeit des § 3a oder der Zweckgebundenheit[91] der §§ 31, 39 BDSG a.F. Das Persönlichkeitsprofil als Ergebnis der in § 3 Abs. 2-4 BDSG a.F. bezeichneten Mechanismen gilt es im Datenschutzrecht zu vermeiden; das Ziel der Zerstreuung und Aufweichung eines solchen Profils gilt es zu erreichen. Kennzeichnend für ein Persönlichkeitsprofil ist, wie durch das Bundesverfassungsgericht herausgestellt, die umfassende Katalogisierung oder Aufzeichnung der Persönlichkeit durch die Zusammenführung

87 BVerfGE 65, 1 (41): „Gefährdungen der menschlichen Persönlichkeit"; *Schild* in: Wolff/Brink, BeckOK DatenschutzR (23. Edition), § 3 BDSG, Rn. 2; *Spindler/Nink* in: Spindler/Schuster, Recht der elektronischen Medien, § 11 TMG, Rn. 15; *Ernst* in: Paal/Pauly, DSGVO, Art. 4, Rn. 5; *Ziebarth* in: Sydow, DS-GVO, Art. 4, Rn. 13; *Gola* in: Gola, DS-GVO, Art. 4, Rn. 23 ff.

88 BVerfGE 65, 1 (17).

89 *Tinnefeld/Buchner* in: Wolff/Brink, BeckOK DatenschutzR, Grundlagen – Medien, Rn. 92, 93; *Schmitz* in: Spindler/Schmitz/Liesching, TMG, § 15, Rn. 85 ff. Weitere kommerzielle Zwecke der Profilnutzung nennend *Kühnl*, Persönlichkeitsschutz 2.0, S. 39 f.

90 Hierzu näher *Ronellenfitsch* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), Einleitung zum BDSG, Rn. 57 f. In der DSGVO finden sich diese ausdrücklich in Art. 1 Abs. 1, Abs. 2 sowie 5 DSGVO wieder.

91 Vgl. hierzu ebenfalls BVerfGE 65, 1 (46) sowie *Hornung*, Die digitale Identität, S. 157 ff.

einzelner Lebens- und Personaldaten einer natürlichen Person.[92] Dabei wird zwischen Langzeitprofilen und Querschnittsprofilen unterschieden, wobei letztlich beide zweckmäßig einen größtmöglichen und realistischen Ausschnitt der Persönlichkeit abbilden.[93] Ähnlich, wenngleich nicht ausdrücklich, hat die Formulierung in die DSGVO Eingang gefunden – namentlich im Prozess des Profilings gem. Art. 4 Nr. 4 DSGVO. Zwar erläutern sowohl Art. 4 Nr. 4 als auch Art. 22 DSGVO nicht die Profilerstellung an sich, sondern beziehen sich ausschließlich auf die automatisierte Entscheidung als Ergebnis der Auswertung von Persönlichkeitsprofilen. Jedoch schließen die Erwägungsgrunde 71, 72 DSGVO ein, dass es sich dabei um eine Verarbeitung personenbezogener Daten natürlicher Personen (vgl. Art. 1, 4 Nr. 1 DSGVO) handelt; charakteristisch ist eine automatisierte Verarbeitung unter Bewertung der persönlichen Aspekte in Bezug auf die natürliche Person selbst[94]. Davon ist jedoch der Weg zur automatisierten Entscheidung, also die entscheidungsbezogene Auswertung eines Persönlichkeitsprofils, zu trennen.[95] Die Begriffe des Persönlichkeitsprofils sowie des Profilings sind also nicht kongruent bzw. synonym. Angesichts der im Laufe der Historie etablierten und erweiterten Definition könnte man meinen, dass die digitale Identität dem Modell des „gläsernen Menschen“ entspricht: In beiden Fällen handelt es sich in der Gesamtheit um eine größtmögliche Sammlung an Daten, welche Aussagen über die analoge Person enthält. Die digitale Identität greift aber einen Schritt weiter, ist also umfangreicher, indem sie das Persönlichkeitsprofil in seiner digitalen Form als eigenständiges Konstrukt ansieht, welchem Rechte und Pflichten im Rahmen des Systems zugeordnet werden.[96] Weiter bezieht sich auch dieser Aspekt nur auf natürliche Personen, wohingegen nach der hier vertretenen Definition auch juristische Personen über eine digitale Identität verfügen. Die digitale Identität

92 BVerfGE 65, 1 (17, 42 f); *Kühnl*, Persönlichkeitsschutz 2.0, S. 21.

93 Vgl. *Polenz* in: Taeger/Pohle, Computerrechts-Handbuch, 130: Verfassungsrechtliche Grundlagen des Datenschutzes, Rn. 18, 19.

94 ErwGr 71 S. 2 DSGVO.

95 So *Buchner* in: Kühling/Buchner, DSGVO, Art. 22, Rn. 11. Vgl. auch *Martini* in: Paal/Pauly, DSGVO, Art. 22 DSGVO, Rn. 21; *Hladjk* in: Ehmann/Selmayr, DSGVO, Art. 22, Rn. 7.

96 Der Begriff insbesondere in Anlehnung an Identity Management Systeme (kurz IMS) – *Meints*/*Reimer*, DuD 2006, 528 sowie *Hansen*/*Meints*, DuD 2006, 543 (546).

entspricht also einer ganzheitlichen Betrachtung der im Internet repräsentierten Person kraft Ihrer Teilidentitäten unabhängig ihrer Subjektsqualität, während sich das Persönlichkeitsprofil als möglichst realistisches Abbild einzelner Aspekte der analogen Person in numerischer oder sozialer Hinsicht[97] darstellt. Demnach unterliegen dem BDSG sowie der DSGVO lediglich solche digitalen (Teil-)Identitäten, die dem Begriff des Persönlichkeitsprofils entsprechen oder durch den Prozess des Profilings entstanden sind und sich entsprechend auf personenbezogene Daten beziehen. Datensätze juristischer Personen sowie anonyme bzw. pseudonyme Online-Kennungen[98] fallen nicht hierunter, obschon sie Merkmale digitaler Identitäten sind. Dem Einwand, dass bereits bestehende Begrifflichkeiten zu einer Einordnung ausreichen könnten, ist damit zu widersprechen.

97 Ausführlich hierzu *Meyer*, Virtuelle Identität, S. 24 ff, 48 ff.

98 Hierzu zählen – so auch *Conrad/Hausen* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 36, Rn. 162, 164 – beispielsweise Profile auf Grundlage des Device- oder Browser- bzw. Canvas-Fingerprintings, welche durch die Verkettung des Nutzerverhaltens, wie durch die Analyse der Browser-Historie – zT auch über verschiedene Webseiten hinweg –, sowie Merkmale der Hard- und Software des Endgeräts entstehen. Zum technischen Vorgang siehe vgl. *Federrath*/*Gerber*/*Herrmann*, DuD 2011, 791 und *Olejnik*/*Castelluccia*/*Janc*, Annals of Telecommunications 2014, 63 (64) sowie zu den resultierenden (technischen) Vorzügen *Cao*/*Li*/*Wijmans*, Network & Distributed System Security Symposium 2017, 1 (2 ff). Zum Fingerprinting des Geräts, also unabhängig von gespeicherten Daten über den Browser oder installierte Plugins siehe *Boda* et al., User Tracking on the Web via Cross-Browser Fingerprinting, 31 (34 ff). Zu Tracking und Identifikation anhand von Touch-Gesten siehe *Masood* et al., Proceedings on Privacy Enhancing Technologies 2018, 122. Zu beachten ist hierbei allerdings, dass derartige Profile überwiegend zur Identifikation der Geräte zum Zwecke der Webseitennutzung und -anpassung dienen und eher nachrangig der Authentisierung der Identität des Nutzers selbst dienen – *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 49 sowie *Cao*/*Li*/*Wijmans*, Network & Distributed System Security Symposium 2017, 1 (1). So können die genannten Fingerprints im Fall der Authentisierung als weiterer Faktor eingesetzt werden, um bei einem Identitätsdiebstahl den Login eines Geräts mit einem abweichenden Fingerprint als Indiz zu nutzen. Weiterhin dienen sie allerdings zur Personalisierung des Webseiten-Inhalts, insbesondere der Werbung.

4. Abschließende Definitionsfindung

Der Begriff der digitalen Identität ist demgemäß in jeglicher Hinsicht mannigfaltig und in einigen Teilgebieten der Wissenschaft nicht vollständig erforscht.[99] Dennoch lassen sich einzelne grundlegende Merkmale für die weitere Untersuchung festhalten:

- Die – sowohl analoge als auch digitale – Identität unterliegt der stetigen Veränderung aufgrund der auf den Menschen wirkenden Einflüsse.
- Sie zeigt sich in jeglichen Interaktionen mit der Außenwelt, mittelbar oder unmittelbar. Beispiele hierfür sind Meinungsäußerungen, Handlungen basierend auf Entscheidungen oder eine bestimmte, äußerlich wahrnehmbare Lebensweise (Sexualität, politische Ausrichtung, Vereinsmitgliedschaft, etc.). Einzelne Aspekte der digitalen Identität sind als Attribute zu bezeichnen.[100]
- Digital existiert die Identität nicht als Ganzes, sondern durch sog. digitale Teilidentitäten. Jede Teilidentität repräsentiert einzelne Merkmale in Abhängigkeit des angebotenen Dienstes sowie der gewollten Darstellungsweise des Identitätsinhabers. Der Praktikabiltät halber wird im folgenden der Begriff der digitalen Identität synonym für die digitale Teilidentität verwendet.

99 Forschungsprojekte diesbezüglich sind FIDIS (**F**uture of **Id**entity in **I**nformation **S**ociety) sowie PRIME (**Pr**ivacy and **I**dentity **M**anagement for **E**urope), beide allerdings abgeschlossen. Die Ergebnisse des Forschungsprojektes PRIME wurden in *Camenisch*/*Leenes*/*Sommer*, Digital Privacy festgehalten. Bezug zur digitalen Identität weist aktuell lediglich das Forschungsprojekt EIDI auf, welches sich mit dem Diebstahl digitaler Identitäten auseinandersetzt.

100 *BITKOM*, Web Identitäten, S. 6; *Hansen*/*Meints*, DuD 2006, 543 (543); *Hühnlein*, DuD 2008, 161; *Windley*, Digital Identity, chapter 2.1.

- Jede digitale Identität mit Personenbezug ist auf eine Kennung bzw. einen Identifier einer natürliche oder juristische Person (auch als Entität bezeichnet[101]) zurückführbar. Bei anonymen digitalen Identitäten dient der Identifier als Referenz- bzw. Schnittpunkt einer Datensammlung. In der Regel dient der Identifier aber als Schlüssel sowie Zuordnungsmöglichkeit der in einer Anwendung oder Dienst aufkommenden Daten. Ist dem Diensteanbieter der wahre Name oder ein Rückschluss auf andere Weise möglich, entspricht die digitale Identität einem Pseudonym – andernfalls ist der Nutzer anonym.[102] Unabhängig dieser charakterlichen Zuordnung können die einzelnen Daten der digitalen Identität aber als Quasi-Identifier dienen, also in Kombination mit anderen Daten zur Identifizierung führen.[103]

- Hinter jeder Kennung einer digitalen Identität verbirgt sich ein Datensatz. Dieser kann aus personenbezogenen und/oder nicht-personenbezogenen Einzeldaten bestehen, sodass folglich zwischen personenbeziehbaren und nicht-personenbeziehbaren Identitäten zu unterscheiden ist. Nur in ersterem Fall stimmt die digitale Identität mit dem Konstrukt des Persönlichkeitsprofils bzw. des Profilings iSd Art. 22 DSGVO überein; der Begriff der digitalen Identität ist damit weiter.

- Die Personenbeziehbarkeit ist allerdings einzelfallabhängig, da auch bei nicht-personenbezogenen Einzeldaten ein Personenbezug entstehen kann. Dieser ergibt sich beispielsweise durch die Auswertung des Datensatzes oder einer Verknüpfung mit anderen Datensätzen, die zu einzigartigen Mustern führen und in Kombination mit personenbezogenen Daten eine Identifikation zulassen. Die Maßstäbe für die Ermittlung dieser Wahrscheinlichkeit für eine Re-Identifizierung finden sich in Erwägungsgrund 26 S. 4 DSGVO.[104]

101 Vgl. *Hühnlein*, DuD 2008, 161 (161); *Hölzel*, DuD 2018, 502 (504).
102 *Meyer*, Virtuelle Identität, S. 34 f; *BITKOM*, Web Identitäten, S. 9; *Hansen*/*Meints*, DuD 2006, 543 (543).
103 *Hölzel*, DuD 2018, 502 (504) sowie *Petrlic*/*Sorge*, Datenschutz, S. 30 f. Hierzu näher unter D.I.1.b)bb)(2).
104 Zum Verfahren siehe auch *Roßnagel*, ZD 2018, 243 (244).

- Eine Übereinstimmung der Attribute zwischen einzelnen digitalen Identitäten oder einer solchen und der analogen Identität muss iSe Bijektivität nicht gegeben sein. Das Verhältnis ist eher surjektiver oder injektiver Natur[105], kann im Einzelfall allerdings durchaus bijektiv sein – beispielsweise im Falle einer statischen IP-Adresse.[106]

Nachfolgend ist anhand der Eigenschaften der digitalen Identität im Einzelnen die verfassungsrechtliche Schutzfähigkeit der digitalen Identität einzelner Rechtssubjekte zu untersuchen, wobei besonderes Augenmerk auf juristischen Personen und künstliche Entitäten liegt.

II. Natürliche (digitale) Personen

Natürliche Personen sind schon ipso iure Grundrechtsträger, einschließlich ihrer Identität. Als Menschenrechte in Art. 1 Abs. 2 GG bezeichnet, gewähren diese einen vollumfänglichen Schutz in allgemeiner (in Form des Auffanggrundrechts in Art. 2 Abs. 1 GG) oder besonderer (in Form spezieller Ausprägungen der Art. 2-19, 33, 38, 104-106 GG), inhaltlicher Hinsicht.

1. Zeitliche Dimensionen des verfassungsrechtlichen Schutzes

Voraussetzung hierfür ist jedoch, dass natürliche Personen auch den weiteren Anforderungen des personellen Schutzbereiches der Grundrechte genügen, wie der zeitlichen Dimension der Grundrechte. Zwar gibt die Verfassung expressis verbis

105 Zu den Begrifflichkeiten *Forster*, Analysis I, S. 91.

106 Vgl. die Causa Breyer – EuGH, Urteil vom 19.10.2016, Az. C-582/14 = CR 2016, 791 m. Anm. *Nink*. Zu bemerken ist aber, dass die statische IP-Adresse nicht den Nutzer, sondern nur den Anschlussinhaber ermitteln lässt. Gerade diese Diskrepanz führt in Fällen der Störerhaftung regelmäßig zu Problemen, weshalb eine einwandfreies bijektives Verhältnis auch hier bestritten werden kann.

hierüber keinen Aufschluss, ergibt sich doch unter Einbeziehung der Rechtsprechung des Bundesverfassungsgerichts eine zeitliche Dimension des Grundrechtsschutzes, orientiert an den Lebensphasen des Menschen: Der Wortlaut des Art. 1 Abs. 1 GG in Verbindung mit § 1 BGB umfasst zunächst nur den lebenden Menschen als Grundrechtsträger.[107] Mittelbar ließe sich dies auch aus dem status activus oder status negativus der Grundrechtsbereiche herauslesen: Nur, wo die Schutzbereiche selbstbestimmt ausgeübt und wahrgenommen werden, kann auch eine Grundrechtsträgerschaft vorliegen.[108] Der Wortlaut der Art. 1-19 GG lässt die Grundrechte allerdings nicht erst nach einer bestimmten Handlung oder gar Betroffenheit gelten, sondern sie kommen grundsätzlich jedem (lebenden) Menschen zu – unabhängig weiterer Kriterien oder eines bestimmten Kenntnisstandes. Nichts anderes lässt insbesondere die Wertung der Grundrechte als Menschenrechte gem. Art. 1 Abs. 1 S. 2 GG zu.[109] Je nach Schutzgut ist die grundrechtliche Zeitachse allerdings zu erweitern, insbesondere angesichts objektivrechtlicher Gewährleistungsgehalte der Grundrechte.

In Richtung des Lebensendes bzw. darüber hinaus sind natürliche Personen ebenfalls hinsichtlich ihrer Persönlichkeit geschützt, insbesondere der Ehre und Würde. Das postmortale Persönlichkeitsrecht, fußend auf Art. 1 Abs. 1 GG und nicht Teil des Allgemeinen Persönlichkeitsrechts[110], schützt vor Herabwürdigung oder Erniedrigung des Menschen- bzw. Persönlichkeitsbildes der toten Person.[111] Es schützt den allgemeinen Achtungsanspruch und die personale Eigenheit des Menschen nach seinem Tod.[112] Konkret erstreckt sich der Schutz neben der Ehre auch

107 *Merten/Papier*, HGr II, § 49, Rn. 6.

108 Vgl. BVerfGE 30, 173 (194): „Das Grundrecht aus Art. 2 Abs. 1 GG setzt die Existenz einer wenigstens potentiell oder zukünftig handlungsfähigen Person als unabdingbar voraus.“, wiederholend in BVerfG NJW 2001, 594; *Huber* in: Merten/Papier, HGr II, § 49, Rn 4, 6.

109 Vgl. *Huber* in: Merten/Papier, HGr II, § 49, Rn. 29, 30; BVerfGE 88, 203 (251 f).

110 So BVerfGE 30, 173 (194); *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 31; *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2, Rn. 48 und 48a; *Boksanyi/Koehler* in: Wandtke/Ohst, Medienrecht Praxishandbuch, Kap. 6, Rn. 25; *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 73; *Luch*, Medienpersönlichkeitsrecht, S. 134 f; aA *Höfling* in: Sachs, GG, Art. 1, Rn. 63 aE sowie 68; ähnlich *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 57.

111 BVerfGE 30, 173 (194); BVerfGK 9, 83 (88); *Kloepfer*, VerfR II, § 55, Rn. 44 ff; *Boksanyi/-Koehler* in: Wandtke/Ohst, Medienrecht Praxishandbuch, Kap. 3, Rn. 26.

112 BVerfGE 30, 173 (194); *Martini*, JZ 2012, 1145 (1150).

auf Aspekte der Identität, wie den Schutz vor Verfälschung des Lebensbildes und den Namen als Ausdruck und Merkmal ebendieser.[113] Letzteres entspringt der Schutzwirkung hinsichtlich des „sittlichen, personalen und sozialen Geltungswertes", welcher mittels der eigenen Lebensleistung erworben wurde.[114] Hinzu tritt ein originärer Schutz des Toten aus Art. 1 Abs. 1 GG in seiner Würde in Bezug auf eine mögliche Objektifizierung des Leichnams.[115] Genannten Eingriffsvariationen gemein ist, dass es einer gewissen Schwere bedarf, um eine Verletzung anzunehmen.[116] Zumindest muss die Verletzung sorgfältig begründet sein, eine bloße Berührung reicht nicht aus.[117] Die Schutzweite bzw. -dauer wird allerdings – und das zurecht – von der Reichweite der zu Lebzeiten erworbenen Würde und Ehre begrenzt. Dieser relative Ansatz erscheint nur konsequent, da die Würde nach dem Tod auf der „Ehrung des Andenkens derjenigen, die einmal unter uns waren oder vor uns waren"[118] sowie auf dem erworbenen (oder „erlebten") sittlichen, personalen und sozialen Geltungswert, basiert. Die Ehre und Würde einer Schauspielerin ist beispielsweise umfangreicher und daher in größerem und längerem Umfang zu schützen als die eines gewöhnlichen Bürgers.[119] Gleichermaßen reduziert sich der postmortale Würde-Schutz mit dem Voranschreiten der Zeit; er verblasst, ebenso wie die Erinnerungen an den Verstorbenen.[120]

113 *Luch*, Medienpersönlichkeitsrecht, S. 148 f; *Fischer*, Die Entwicklung des postmortalen Persönlichkeitsschutzes, S. 99 f; BVerfGE 63, 131 (135); vgl. 59, 216 (226). Weitere Güter darstellend *Fischer*, Die Entwicklung des postmortalen Persönlichkeitsschutzes, S. 71 ff.

114 BVerfGK 9, 83 (88); *Martini*, JZ 2012, 1145 (1150).

115 *Kloepfer*, VerfR II, § 55, Rn. 45; *Hufen*, Staatsrecht II, § 10, Rn. 26; *Knellwolf*, ZUM 1997, 783 (785 f).

116 Kritisierend *Luch*, Medienpersönlichkeitsrecht, S. 138 f.

117 Vgl. BVerfGE 93, 266 (294); *Boksanyi/Koehler* in: Wandtke/Ohst, Medienrecht Praxishandbuch, Kap. 6, Rn. 27 f.

118 So *Hofmann*, AöR 118 (1993), 353 (375); vgl. zum Relationsbegriff auch *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 54.

119 Vgl. BVerfGE 30, 173 (195).

120 Vgl. BVerfGE 30, 173 (196) sowie BGHZ 50, 139 (140 f); *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 57; *Knellwolf*, ZUM 1997, 783 (788). Ähnlich, allerdings an einer absoluten Schutzfrist festhaltend *Bender*, VersR 2001, 815 (824) sowie *Fischer*, Die Entwicklung des postmortalen Persönlichkeitsschutzes, S. 188 ff, 195 f – anknüpfend an der 70-jährigen Schutzdauer des § 64 UrhG.

Diametral, also im pränatalen Bereich, existiert ebenfalls ein partieller Schutz gemäß der Verfassung. Denklogisch kann sich dieser nicht auf die Kommunikationsgrundrechte oder die Versammlungsfreiheit erstrecken, dafür jedoch auf Inhalte der Würde[121] und des Lebens.[122] Embryonen sind, jedenfalls ab dem Zeitpunkt der Nidation in der Gebärmutter, in ihrem Leben und ihrer Unversehrtheit gem. Art. 2 Abs. 1 GG geschützt.[123] „Wo menschliches Leben existiert, kommt ihm Menschenwürde zu"[124] – der Schutz gilt unabhängig von einer Wertigkeit des werdenden Lebens oder anderen Voraussetzungen, die dem Embryo anhaften. Es kommt vielmehr darauf an, dass der Prozess des Wachsens und Sich-Entfaltens bereits begonnen hat; die Verschmelzung des Erbgutes führte bereits dazu, eine genetisch unverwechselbare Identität zu erschaffen bzw. diesen Prozess in Gang zu bringen.[125] Diese Folgerung resultiert schon aus der Rückschau auf die eigene Existenz und deren Anfänge.[126] So verstand bereits das Bundesverfassungsgericht im Ansatz die Entstehung des Lebens als Prozess[127], während bis heute Teile der

121 Anbei sei des Verständnisses halber erwähnt, dass die Menschenwürde des Art. 1 Abs. 1 GG im Folgenden als Grundrecht und nicht als Grundprinzip gesehen wird. Zur Thematik genannt seien nur *Ipsen*, DVBl 2004, 1381 (1383 f); *Zarr*, Menschenwürde, S. 102 mwN. Ablehnend dagegen *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 103 ff; *Hufen*, JZ 2004, 313 (314 f).

122 *Rüfner* in: Isensee/Kirchhof, HStR IX, § 196, Rn. 8.

123 BVerfGE 39, 1 (37); 88, 203 (251).

124 BVerfGE 88, 203 (252) unter Verweis auf E 39, 1 (41).

125 BVerfGE 88, 203 (251 f); vgl. *Müller-Terpitz*, Schutz pränatalen Lebens, S. 341 f. Bemerkenswert ist jedoch der bisherige Kenntnisstand der Forschung hinsichtlich der Möglichkeit, dass zwischen Kernverschmelzung und Nidation noch weitere (identitätsbestimmende) Zellteilungsvorgänge beginnen – so *Hufen*, JZ 2004, 313 (315). Konsequent müsse daher folgen, dass eine Identität nur herausgebildet werden kann, wo menschliches Leben bereits beginnt zu existieren. Anders sieht *Dreier*, Bioethik, S. 40 f diesen Zustand dagegen als Vorhandensein mehrerer Dividuen, da die Individuisierung erst zum Zeitpunkt der Nidation eintritt.

126 Mit einem zurückspulbaren Film vergleichend *Zarr*, Menschenwürde, S. 113.

127 BVerfGE 39, 1 (37).

Literatur[128] vermeintlich trennscharf[129] den Beginn des Lebens in der Nidation sehen. Vermeintlich ist dies nämlich im Falle einer nicht erfolgreichen Nidation: Folgt man der letztgenannten Ansicht, so würde es sich bei verschmolzenen Zellen und dem dadurch begonnenen Zellteilungs- und Entwicklungsprozess nicht um beginnendes Leben – einen Menschen iSd GG – handeln.[130] Es würde also nach dieser Verfassungsauslegung geradewegs unterschieden werden zwischen lebensfähigem und nicht lebensfähigem Zellmaterial. Zwar ist die Nidation geradezu existentiell, wenn es um die weitere Entwicklung geht. Die aufgrund derartigen Begriffsverständnisses vertretene Auffassung widerspricht allerdings dem durch die Verfassung und Art. 1 Abs. 1 GG verkörperten Wert des Menschen. Der Mensch darf in keinster Weise und zu keiner Zeit objektifiziert werden.[131] Dies würde er vorliegend allerdings, wenn über ihn aus rein pragmatisch-vernünftigen Gesichtspunkten noch vor seiner Geburt entschieden würde und der Begriff des Menschen nicht bereits ab der Kernverschmelzung angenommen wird. Derart differenzierend dürfen sich die hoheitlichen Gewalten nicht über den Prozess des Lebens stellen und dementsprechend „Erfolgsaussichten" aus einer Nidation

128 *Murswieck* in: Sachs, GG, Art. 2, Rn. 145 f; *Windhorst* in: Gröpl/Windthorst/von Coelln, StuKo GG, Art. 1, Rn. 16; *Hufen*, Staatsrecht II, § 10, Rn. 25 sowie ders. *Hufen*, JZ 2004, 313 (315 f); zu einzelnen Begründungsansätzen *Müller-Terpitz*, Schutz pränatalen Lebens, S. 145 ff mwN; offenlassend dagegen *Zippelius* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 I und II, Rn. 51.

129 Vermeintlich trennscharf ist die Argumentationslinie im Weiteren auch hinsichtlich einer Trennung von Menschenwürde des Art. 1 Abs. 1 GG und Lebensschutz gem. Art. 2 Abs. 2 S. 1 GG: Leider wird häufig die Linie zwischen beiden Gütern verklärt, sodass wegen des abzulehnenden Schutzes des Lebens in dieser Entwicklungsphase unter Betrachtung der Rechtslage von ESchG und §§ 218 ff StGB auch die Menschenwürde entfiele. Dabei wird übersehen: Nicht jede Verletzung des Lebens geht mit einer Würdeverletzung einher, wenngleich die Menschenwürde gewissermaßen das Leben voraussetzt – vgl. *Kloepfer*, JZ 2002, 417 (420) sowie *Müller-Terpitz*, Schutz pränatalen Lebens, S. 359 f.

130 Eine Grundrechtsträgerschaft erst ab Geburt annehmend *Dreier* in: Dreier, GG, Art. 1 I, Rn. 64, 66 f; *Ipsen*, DVBl 2004, 1381 (1384); *Zarr*, Menschenwürde, S. 91 f mwN.

131 In stRspr BVerfGE 9, 89 (95); 27, 1 (6); 28, 86 (391); 45, 187 (28); 50, 166 (175); 87, 209 (228); 96, 375 (399); 109, 133 (150); 115, 118 (53); 117, 71 (89); 131, 268 (286 f). Zu den Grenzen der Objektformel siehe auch BVerfGE 109, 279 (312).

schließen.[132] Eine solche Denkrichtung verbietet sich schon anhand der historischen Wurzeln des Art. 1 Abs. 1 GG,[133] zumal Grundrechte insgesamt „Reaktionen auf historische Gefährdungslagen durch den Staat" darstellen[134]. Die Formulierung des Art. 1 Abs. 1 GG enthält mit seiner pauschalen Aussage, der „Mensch" sei geschützt, gleichermaßen ein Diskriminierungsverbot bezüglich physischer, psychischer oder moralischer Aspekte.[135] Demgemäß kann die Rolle des Entscheidenden über das Dasein als Mensch nicht Teil der Aufgaben des Staates gem. Art. 1 Abs. 1 sowie 2 Abs. 2 S. 1 GG sein. Vielmehr hat er die Prämisse, jedes Leben zu schützen und mit Beginn des Prozesses Leben auch entsprechende Werte der Anerkennung einer Würde einfließen zu lassen. Gerade die Würde bedarf keiner aktiven Wahrnehmung des Schutzes oder einer anderen Fähigkeit.[136] Dementsprechend lässt sich der Verfassung eine möglichst weite Auslegung entnehmen, um einen größtmöglichen Schutz zu gewährleisten. Eine Entscheidung, ob und wann menschliches Leben vorliegt, kann daher lediglich

132 So auch *Linke*, JuS 2016, 888 (889). Zudem gebietet sich dies schon aufgrund rückblickend auf den Holocaust während des Zweiten Weltkrieges nicht. Vgl. auch die Entstehungsgeschichte des Art. 2 Abs. 2 S. 1 GG – BVerfGE 39, 1 (38 ff).

133 Vgl. *Hofmann* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Art. 1 GG, Rn. 1; *Hufen*, JZ 2004, 313 (313).

134 BVerfGE 6, 55 (71); 27, 71 (84); *Jellinek*, System der subjektiv öffentlichen Rechte, S. 95; *Böckenförde*, NJW 1974, 1529 (1537).

135 *Höfling* in: Sachs, GG, Art. 1, Rn. 56. Vgl. *Nettesheim*, JZ 2019, 1 (5); *Zarr*, Menschenwürde, S. 112 sowie bzgl. des Lebensschutzes *Müller-Terpitz* in: Isensee/Kirchhof, HStR VII, § 147, Rn. 21 ff.

136 BVerfGE 39, 1 (41); 88, 203 (252).

aus biologischen Gesichtspunkten beurteilt werden.[137] Folglich sprechen die dargelegten Argumente und sowie die Verfassung für eine pränidative Sichtweise.[138]

Mit einem solch weiten Verständnis des Menschenwürdeschutzes entstehen allerdings Konfliktlagen oder gar Widersprüche, die wiederum gegen einen weiten Anwendungsbereich der Menschenwürde sprechen. Dies zeigt sich bereits am Beispiel des Präparats zur postkoitalen Empfängnisverhütung (ugs. „Pille danach"): Dieses Präparat dient dazu, eine ungewollte Befruchtung aufgrund mangelnder Verhütung oder anderer Probleme zu verhindern. Das Recht zu diesem Handeln entspringt dem Persönlichkeitsrecht sowie der Verfügungsgewalt der Mutter über den eigenen Körper.[139] Ebenso lässt sich eine Abwägung zu Gunsten des Embryo oder der Vorstufen nur schwer rechtfertigen. Der Staat darf der Mutter nicht vorschreiben, aus Gründen der Unabwägbarkeit der (embryonalen) Menschenwürde

137 *Höfling* in: Sachs, GG, Art. 1, Rn. 61; vgl. auch *Hillgruber* in: Epping/Hillgruber, BeckOK GG, Art. 1, Rn. 4; *Stern*, StaatsR IV/1, S. 145; *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 206; *Gropp*, Schutzkonzepte des werdenden Lebens, S. 239; *Müller-Terpitz*, Schutz pränatalen Lebens, S. 339 ff. Vollständig ablehnend dagegen *Merkel* in: Kindhäuser/Neumann/Paeffgen, StGB, Vor § 218, Rn. 15.

138 So iE auch *Hillgruber* in: Epping/Hillgruber, BeckOK GG, Art. 1, Rn. 4; *Höfling* in: Sachs, GG, Art. 1, Rn. 61; *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 206 sowie *Huber* in: Merten/Papier, HGr II, § 49, Rn. 9; *Kloepfer*, VerfR II, § 57, Rn. 5; *Schlink*, Aktuelle Fragen des pränatalen Lebensschutzes, S. 8; *Zarr*, Menschenwürde, S. 110 ff; vgl. auch *Hubmann*, Persönlichkeitsrecht, S. 337 ff. Aufgrund des Fortschreitens moderner Technologien gar einen „präexistentiellen" Schutz annehmend *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 125. Weiter erscheint dies auch Angesichts der Formulierung des § 8 Abs. 1 ESchG im Rahmen der einheitlichen Rechtsordnung konsequent: „Als Embryo im Sinne dieses Gesetzes gilt bereits die befruchtete, entwicklungsfähige menschliche Eizelle vom Zeitpunkt der Kernverschmelzung an (...)" – kritisch hierzu *Zarr*, Menschenwürde, S. 78. Dies wohl vollumfänglich ablehnend aufgrund der De-Subjektivierung der Menschenwürde *Nettesheim*, JZ 2019, 1 (6/7).

139 Vgl. BVerfGE 39, 1 (42); 88, 203 (214, , 255 f, 348); *Hofmann* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Art. 1, Rn. 12, 21; *Schlink*, Aktuelle Fragen des pränatalen Lebensschutzes, S. 8 f, 10; zur Kollision der Interessen des Embryos sowie der Frau/Mutter siehe auch *Gropp*, Schutzkonzepte des werdenden Lebens, S. 299 ff, *Classen*, DÖV 2009, 689 (691) sowie vgl. *Holzwarth*, Das Recht auf ungestörte Familienplanung als Konkretisierung des zivilrechtlichen allgemeinen Persönlichkeitsrechts, S. 6, 115 f.

des Art. 1 Abs. 1 S. 1 GG[140] das Kind zu gebären — dies käme einem schwerwiegenden Grundrechtseingriff gleich. Dennoch müssen diese und ähnliche Handlungsweisen engen Voraussetzungen unterstellt werden, um dem hohen Gut des werdenden Lebens Rechnung zu tragen.[141] Sie dürfen gewissermaßen nicht einem üblichen Gang zum Arzt gleich kommen.[142] Andernfalls würde die Geburt und der werdende Mensch objektifiziert; ob das Kind geboren wird, hinge so nur noch vom Willen der Mutter ab und nicht vom bereits bestehenden Menschen-Dasein im Mutterleib. Würde nun dementgegen ein hoher, umfangreicher Menschenwürdeschutz unter Einbeziehung des Rechtsguts Leben für den werdenden Menschen im Leib der Mutter angenommen, so ließe sich der Vertrieb und das Angebot der „Pille danach" nur schwer begründen.[143] Schließlich handele es sich dann bereits um einen Menschen, dessen Tötung gem. § 212 Abs. 1 StGB strafbar und auch mit dem telos der §§ 218 ff StGB unvereinbar[144] wäre. Gegen die Erläuterungen zur Problematik sei jedoch allumfassend ins Feld zu führen, dass trotz der Bestimmung des Beginns der Menschenwürde anhand biologischer Prozesse Art. 1 Abs. 1 S. 1 GG und Art. 2 Abs. 2 S. 1 GG voneinander entkoppelt zu betrachten sind – mit der Verletzung des Rechts auf Leben und körperliche Unversehrtheit geht grundsätzlich nicht die Verletzung der Menschenwürde einher.[145] Denn während

140 Hierzu *Höfling* in: Sachs, GG, Art. 1 GG, Rn. 11 mwN auf BVerfGE 75, 369 (380) sowie *Zippelius* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 I und II GG, Rn. 37 ff. Weiterhin ist dies abweichend von BVerfGE 88, 203 (255) anzunehmen – hierzu ausführlich *Merkel* in: Kindhäuser/Neumann/Paeffgen, StGB, Vor § 218, Rn. 17 f.

141 Hierzu *Hofmann* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Art. 1 GG, Rn. 22.

142 BVerfGE 39, 1 (44).

143 Hinterfragend auch *von Lutterotti*, Schutz des menschlichen Lebens, S. 12 (S. 20 f); zur Problematik im Rahmen des Embryo in vitro *Gropp*, Schutzkonzepte des werdenden Lebens, S. 232 f.

144 Vgl. *Fischer*, StGB-Kommentar, Vor §§ 218-219b, Rn. 2 f; *Eschelbach* in: von Heintschel-Heinegg, BeckOK StGB, § 218, Rn. 1.

145 So auch *Classen*, DÖV 2009, 689 (697) bzgl. der Abtreibung sowie *Höfling* in: Sachs, GG, Art. 1, Rn. 69; *Dreier*, Bioethik, S. 37. Zur Entkoppelung von Würde- und Lebensschutz siehe *Müller-Terpitz*, Schutz pränatalen Lebens, S. 343, 359 ff sowie *Isensee* in: Merten/Papier, HGr IV, § 87, Rn. 202 – jeweils berechtigterweise eine Entkoppelung ablehnend, da sich diese anhand einer sauberen Definition und Differenzierung des materiellen Gehaltes nicht bedarf. Vgl. auch die Gegenüberstellung der Schutzgüter von *Schlink*, Aktuelle Fragen des pränatalen Lebensschutzes, S. 10 f.

das Recht auf Leben und körperliche Unversehrtheit die biologisch-physischen Aspekte des Menschen schützt,[146] bezieht sich die Menschenwürde auf den allgemeinen Achtungsanspruch des Menschen kraft seines Daseins[147]. Im Falle der „Pille danach" ist daher mit Abtötung befruchteter Zellen ein Verstoß gegen das Recht auf Leben feststellbar[148], aber keine Beeinträchtigung der Menschenwürde iSd Art. 1 Abs. 1 S. 1 GG. Es bedarf folglich auch keiner Überlegung hinsichtlich eines abgestuften Schutzes der Menschenwürde[149], da es zu keiner aufzulösenden Kollision der Grundrechtsbereiche kommt. Folglich verbleibt dem Embryo schon mit Beginn seiner Entstehung ein Menschenwürde-Schutz aus Art. 1 Abs. 1 S. 1 GG, der sich nur auf einzelne Aspekte des Achtungsanspruchs erstreckt. Wird letztlich das Versagen der Würdefähigkeit vertreten, so muss zumindest aus datenschutzrechtlicher Sicht eine pränatale Reflexwirkung bedacht werden.

In der Summe ergibt sich ein zeitlich umfangreicher Schutz natürlicher Personen und der damit verbundenen analogen Identität, von der Kernverschmelzung bis zum Tod und (zeitweise) darüber hinaus. In pränataler wie postmortaler Hinsicht

146 BVerfGE 56, 54 (73 ff); *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2, Rn. 58, 62.

147 Vgl. BVerfGE 30, 173 (194); 87, 209 (228); BVerfGK 9, 83 (88); *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 30.

148 Die Tötung ist hingegen mit Art. 2 Abs. 2 S. 1 GG vereinbar, da sich aus der Abwägung im Rahmen der Verhältnismäßigkeit strenge Voraussetzungen ergeben, wie sie in den §§ 218 ff StGB normiert sind. Mithin beginnt das Leben nach den §§ 218 ff StGB erst mit Nidation, weshalb eine Tötung zuvor unproblematisch ist – *Eschelbach* in: von Heintschel-Heinegg, BeckOK StGB, § 218, Rn. 2; *Dreier*, Bioethik, S. 38 f. Hierzu BVerfGE 39, 1 (48) sowie 88, 203 (261 ff, 266 f).

149 Den Stufenschutz bejahend *Hufen*, Staatsrecht II, § 10, Rn. 25; *Zarr*, Menschenwürde, S. 119 f; *Müller-Terpitz*, Schutz pränatalen Lebens, S. 349 ff; vgl. hinsichtlich des Art. 2 Abs. 2 S. 1 GG *Schlink*, Aktuelle Fragen des pränatalen Lebensschutzes, S. 8, 10, 13 ff sowie *Dreier*, ZRP 2002, 377 (379 f); *Herdegen*, JZ 2001, 773 (778 f); als Grundrechtsanwartschaft bezeichnend *Kloepfer*, JZ 2002, 417 (420). *Hofmann* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Art. 1 GG, Rn. 11 dagegen erstreckt die Abstufung auf den gesamten Grundrechtekatalog, sodass Art. 2 Abs. 2 S. 1 und 1 Abs. 1 GG den Basisschutz darstellen.

erstreckt sich ein verfassungsrechtlicher Schutz zumindest auf Art. 1 Abs. 1 GG. Diese Reichweite sucht ihresgleichen im europäischen Raum.[150]

2. Die Transponierung in die digitale Welt

Entscheidend ist für den Schutz der digitalen Identität allerdings, inwieweit sich die analogen Schutzaspekte in die digitale Welt übertragen lassen, oder ob dies überhaupt möglich ist.

Als (metaphorische) Leitlinie dient auch an dieser Stelle der Lebenszyklus des Menschen, denn auch bei digitalen Identitäten lässt sich ein sog. Lifecycle erkennen[151]: Das Stadium der Geburt ist durch das Erschaffen der digitalen Identität geprägt, beispielsweise mittels der erstmaligen Registrierung oder Nutzung der Plattform eines Diensteanbieters wie einer Online-Suchmaschine. Einzelne Parameter und Attribute einschließlich erteilter Rechte und Pflichten werden während dieses Prozesses festgelegt und ggf. durch Opt-In- oder -Out-Möglichkeiten modifiziert.[152] Darin findet sich die Parallele in der Verschmelzung von Ei- und Samenzelle bei der Entstehung des Menschen und die nachfolgende Ausbildung der DNA. Anschließend erfolgt der Abschluss des Vorgangs und die Freischaltung des mit der Identität verknüpften Accounts – die digitale Identität tritt in die

150 Die EMRK enthält insoweit keinen ausdrücklichen Schutz der Menschenwürde. Stattdessen lassen sich einzig Elemente des deutschen Menschenwürdeschutzes aus Art. 3 oder 8 EMRK herauslesen; das Gebot durchdringt die Konventionsfreiheiten in ihrer Gesamtheit. Die erläuterte Problematik könnte mit der EMRK folglich kaum gelöst werden. Aufseiten der GrC findet sich die Menschenwürde dagegen in Art. 1 S. 1 GrC wieder. Aufgrund der selbigen Formulierung würden sich die dargestellten Ausführungen in Verbindung mit Art. 2 Abs. 1 GrC stark ähneln. Dennoch bleibt aufgrund der Streitigkeit des Lebensbeginns und unterschiedlichen Regelungen in den europäischen Staaten der Schutz hinter dem des GG zurück. – Vgl. *Richter* in: Dörr/Grote/Marauhn, EMRK-GG-Kommentar, Kapitel 9, Rn. 24 ff; *Meyer-Ladewig*/*Nettesheim*/*von Raumer*, EMRK-Kommentar, Art. 8, Rn. 10; *Streinz* in: Streinz, EUV/AEUV-Kommentar, Art. 1 GrC, Rn. 4 ff; *Voet van Vormizeele* in: Schwarze, EU-Kommentar, Art. 1 GrC, Rn. 4 ff sowie Art. 2 GrC, Rn. 5.

151 Grundlegend hierzu die Ausführungen von *Hansen*/*Meints*, DuD 2006, 543 (544 f).

152 Zum Entstehungsprozess unter Differenzierung zwischen nutzerdefinierten und systemgenerierten Daten siehe *Doring*, Sozialpsychologie im Internet, S. 342 f. Exemplarisch hierfür die Erstellung eines Facebook-Accounts, siehe *Kühnl*, Persönlichkeitsschutz 2.0, S. 21 ff.

Phase des Lebens ein. Darunter ist die grundlegende Verwendung der digitalen Identität zu verstehen, wobei sich hier ggf. Differenzierungen anhand der dahinterstehenden analogen Person(en) ergeben.[153] Ungeachtet dessen ist das Leben auf den Einzelfall der digitalen Identität beschränkt und die Ausgestaltung durch die Plattform einzubeziehen. Abschließend: Der Tod der digitalen Identität. Er tritt in der Regel erst ein, indem die analoge Person hinter der digitalen Identität die Aufgabe der digitalen Identität durch Deaktivierung oder Löschung dem Plattformbetreiber mitteilt. Vereinzelt bleiben die während des Lebens erstellten Daten und Verbindungen noch für einen gewissen Zeitraum gespeichert, um bspw. Interaktionen mit anderen digitalen Identitäten weiterhin zuordnen zu können.[154] Entsprechend dem menschlichen Dasein nach dem Tod in der analogen Welt verbleibt letztlich eine „digitale Hülle" auf dem Server und wird – wortwörtlich – zur sog. „Karteileiche".

Überblickshaft sei nun der digitale Lebenszyklus anhand der analogen verfassungsrechtlichen Belange abzugleichen und die zeitliche Reichweite auf ihre Korrelation hin zu überprüfen. Zunächst kann entgegen der Reihenfolge des Lebenszyklus vorweggenommen werden, dass, soweit sich die Nutzung der digitalen Identität durch eine natürliche Person als Ausübung der Persönlichkeitsentfaltung ansehen lässt, keine grundlegende Unanwendbarkeit besteht. Dies kann zumindest schon daraus gefolgert werden, als dass Wechselwirkungen zwischen digitaler und analoger Identität nicht ohne Einfluss auf eine Grundrechtsausübung bleiben.[155] Ob sich einzelne Grundrechtsgehalte hingegen auf die digitale Identität in isolierter Form oder iVm der analogen Person übertragen lassen, ist im Einzelnen später zu untersuchen.[156] Der verfassungsrechtliche Schutz während der Lebensphase der digitalen Identität ist damit vorerst anzunehmen.

153 Dazu *Hansen*/*Meints*, DuD 2006, 543 (544 f).
154 *Hansen*/*Meints*, DuD 2006, 543 (545). Vgl. auch die Archivzwecke iSd Erwägungsgrundes 158 der DSGVO, z.B. zu Zwecken der Strafverfolgung iSd §§ 45 S. 1, 50 BDSG iVm Art. 4 Abs. 3 RL (EU) 2016/680 (JI-Richtlinie).
155 Vgl. *Humer*, Identitätsarbeit in digitalen Systemen, S. 150.
156 Sub Kapitel D.I.

a) Der postmortale Schutz der digitalen Identität

Der Tod der digitalen Identität ist dagegen in Beziehung zur Thematik des postmortalen Persönlichkeitsrechts zu setzen. Dieses schützt, wie erwähnt, den Verstorbenen in seinem Achtungsanspruch und erworbenen Geltungsanspruch in der Gesellschaft. Anhand der Wechselwirkung des digitalen und analogen Lebens ist die digitale Prägung der Persönlichkeit einschließlich der digitalen Identitäten, welche zu Lebzeiten entstanden sind, betrachtenswert. Es ist fraglich, ob oder wie die Möglichkeit eines postmortalen Schutzes der digitalen Identität besteht – beispielsweise im Sinne eines postmortalen Datenschutzes oder als Teil des digitalen Nachlasses. Der postmortale Datenschutz bezieht dahingehend Art. 1 Abs. 1 GG ein, als dass sich auch aus der Nutzung der Informationstechnik zu Lebzeiten und Vertrauen in deren Sicherheit und Funktion Reflexwirkungen ergeben können. Diese entstehen immer dann, wenn sich ein Grundrecht seinem materiellen Gehalt nach auch auf postmortale Angelegenheiten erstrecken kann.[157] Sedes materiae des (verfassungsrechtlichen) Datenschutzrechts ist allerdings nicht Art. 1 Abs. 1 GG, sondern Art. 2 Abs. 1 iVm 1 Abs. 1 GG.[158] Bei der Anwendung des Persönlichkeitsrechts auf postmortale Sachverhalte begegnet man der Problematik der mangelnden Handlungsfähigkeit Verstorbener, welche nach dem Aspekt des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG aber erforderlich ist. So wird nach Wortlaut der Verfassung das Leben der Person vorausgesetzt, wo die Entfaltung doch ein bewusst gestaltendes Element des Grundrechtsträgers meint. Daraus resultierend wird in Rechtsprechung[159] und Literatur[160] einhellig das postmortale Persönlichkeitsrecht auf Art. 1 Abs. 1 gestützt – folglich also

157 *Spilker*, DÖV 2015, 54 (54).

158 BVerfGE 65, 1; *Spilker*, DÖV 2015, 54 (56); *Gurlit*, NJW 2010, 1035 (1036), jedoch um (technische) Aspekte der Art. 10, 13 GG erweiternd.

159 BVerfGE 30, 173 (194).

160 *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2, Rn. 226; *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 31; *Boksanyi/Koehler* in: Wandtke/Ohst, Medienrecht Praxishandbuch, § 3, Rn. 25 ff; *Brändel* in: Götting/Schertz/Seitz, Handbuch des Persönlichkeitsrechts, § 37, Rn. 3 f. Scheinbar eigenständig aus Art. 1 Abs. 1 GG ableitend *Culmsee*, DSRITB 2013, 413 (413 f). Ablehnend dagegen, da auch aktive Elemente aufweisend *Ladeur* in: Götting/Schertz/Seitz, Handbuch des Persönlichkeitsrechts, § 8, Rn. 55.

nur auf Aspekte aus der Menschenwürde, nicht der Entfaltung der Persönlichkeit. Einzig hinsichtlich der selbstbestimmten Entscheidung des Lebensendes sieht das Bundesverfassungsgericht eine Verankerung in Art. 2 Abs. 1 iVm 1 Abs. 1 GG mit entsprechend stärkerer Lesart des Menschenwürdegehaltes.[161] Das Recht der informationellen Selbstbestimmung als verfassungsrechtliches Datenschutzrecht weist aber überwiegend eine Verankerung in Art. 2 Abs. 1 GG auf, entsteht durch bewusstes Steuern mittels ausgewählter Informationspreisgabe doch die beabsichtigte Darstellung der eigenen Persönlichkeit in Form der digitalen Identität. Konsequent würde sodann die informationelle Selbstbestimmung verneint werden, ein ausschließlich postmortaler Datenschutz entfallen. Diese Folgerung unterstützt scheinbar auch der Wortlaut des BDSG a.F., richtet sich dieses gem. § 3 Abs. 1 BDSG a.F. an eine „bestimmte natürliche Person", setzt also eine lebendige Person voraus.[162] Ähnlich spricht Art. 4 Nr. 1 DSGVO von einer identifizierbaren natürlichen Person. Explizit schließt Erwägungsgrund 27 der DSGVO ausdrücklich die Anwendung auf Daten Verstorbener aus.[163] Die Reflexwirkung wirkt vorliegend aber so, dass zu Lebzeiten getroffene Entscheidungen im Rahmen der informationellen Selbstbestimmung und der digitalen Identität sich auch auf die Zeit nach dem Tod erstrecken.[164] „[D]ie Vorsorge des Lebenden für die Zeit nach seinem Tod gehört [zumindest] zur allgemeinen Handlungsfreiheit des Menschen."[165] Der datenschutzrechtliche prämortale Reflex folgt allein schon daraus, dass nicht jeder Diensteanbieter in seinen AGB Regelungen für einen Gedenkstatus[166] oder eine automatische Löschung bei Meldung des Todes oder Inaktivität[167] vorsieht. Der Tod des Nutzers und Inhabers der digitalen Identität wird nur selten gegenüber allen Diensteanbietern kommuniziert werden können,

161 Hierzu grundlegend BVerfG, Urteil v. 26.2.2020 – Az. 2 BvR 2347/15 u.a. –, Rn. 204 ff.

162 So auch *Schild* in: Wolff/Brink, BeckOK DatenschutzR (23. Edition), § 3 BDSG, Rn. 5 unter Verweis auf die Klarstellung in *Artikel 29-Datenschutzgruppe*, Opinion 4/2007 on the concept of personal data. Anders dagegen *Culmsee*, DSRITB 2013, 413 (416).

163 Hierzu *Spilker*, DÖV 2015, 54 (57 f).

164 Vgl. *Spilker*, DÖV 2014, 637 (640) sowie *Spilker*, DÖV 2015, 54 (54 f); *Martini*, JZ 2012, 1145 (1151).

165 BVerfGE 50, 256 (262).

166 So z.B. Facebook, siehe https://de-de.facebook.com/help/103897939701143?helpref=faq_content.

167 So z.B. Xing – zu weiteren Diensteanbietern vgl. *Martini*, JZ 2012, 1145 (1146).

folglich verbleibt die digitale Hülle auf Ewig für den Diensteanbieter nutzbar.[168] Die mit dem postmortalen Persönlichkeitsrecht zu vermeidende „Ausbeutung" des Toten wäre dann in digitaler Hinsicht dennoch gegeben, das in der analogen Welt erreichte Schutzziel nicht konsequent umgesetzt.[169] Eine Erweiterung der Entscheidungsmöglichkeiten neben dem Erbrecht gem. Art. 14 Abs. 1 S. 1 GG sowie selbstbestimmungsrechtlichen Aspekten nach dem Tod in Form der Organspende, der Patientenverfügung oder der Beisetzung iSv Art. 2 Abs. 1 iVm 1 Abs. 1 GG – welche allesamt auf Reflexwirkungen basieren – auf digitale Sachverhalte erscheint daher nur konsequent und vorausschauend.[170] Folglich kann für digitale Identitäten nach der hier vertretenen Auffassung nach Möglichkeit ein Schutz nach postmortalem Datenschutzrecht kraft Reflexwirkung der Art. 2 Abs. 1 iVm 1 Abs. 1 GG angenommen werden.[171]

Der postmortale Schutz der digitalen Identität betrifft allerdings auch Aspekte des digitalen Nachlasses. Grundlegend meint die Formulierung nach bisheriger Auseinandersetzung in der Literatur den Übergang der Gesamtheit des digitalen Vermögens, einschließlich der Immaterialgüterrechte, diesbezüglicher Vertragsverhältnisse sowie des gesamten elektronischen Datenbestandes des Erblassers.[172] Folglich könnte auch die digitale Gesamt-Identität bzw. jede digitale Identität auf die Erben über gehen, sei es aufgrund der Erbschaft der Vertragsverhältnisse oder des Datenbestandes einschließlich der Login-Daten bzw. der Daten auf Servern der Diensteanbieter. Die Möglichkeit des Erbfalles an digitalen Identitäten reicht an dieser Stelle bereits aus, um den zeitlichen Aspekt des postmortalen Schutzes

168 Die Daten des Nutzers können nach datenschutzrechtlichen Vorschriften und verfassungsrechtlichen Maßstäben im Rahmen der erteilten Einwilligung genutzt werden. Wird diese nicht widerrufen oder auf andere Weise nichtig, bleibt die Nutzungsmöglichkeit bestehen. Aus dem Tod einen konkludenten Widerruf herauszulesen scheitert schon deshalb, weil der Tod faktisch schon keine willentliche Äußerung oder bewusste Entscheidung des Menschen sein kann (von der Selbsttötung ggf. abgesehen).

169 Ähnlich auch *Sorge*, MMR 2018, 372 (377).

170 So iE auch *Spilker*, DÖV 2015, 54 (55 f) sowie vgl. *Spilker*, DÖV 2014, 637 (640).

171 Ebenso *Spilker*, DÖV 2015, 54 (59 f); *Arens*, RDV 2018, 127 (130 f); als wesensgleiches Minus des Persönlichkeitsrechts bezeichnend *Martini*, JZ 2012, 1145 (1150). Ungenau dagegen ein Regel-Ausnahme-Verhältnis zugunsten des Erben des digitalen Nachlasses vorschlagend *Klas*/*Möhrke-Sobolewski*, NJW 2015, 3473 (3476 f).

172 *Klas*/*Möhrke-Sobolewski*, NJW 2015, 3473; *Herzog*, NJW 2013, 3475 (3475).

digitaler Identitäten zu bejahen. Während sich Literatur[173] und Rechtsprechung[174] uneinig sind hinsichtlich der Reichweite des Schutzes, besteht hingegen Einigkeit darin, dass die Universalsukzession gem. § 1922 BGB ebenfalls die digitalen Verhältnisse einbezieht. Ob und wie die Ausgestaltung des digitalen Nachlasses in verfassungsrechtlicher Hinsicht unter Bezug auf die digitalen Identitäten gegeben ist, ist an späterer Stelle zu erörtern[175], sodass auch hier die Möglichkeit des verfassungsrechtlichen Schutzes anzunehmen ist.

Zusammenfassend lässt sich in den aufgezeigten Grundsätzen ein entsprechend digitaler Bezug erkennen, weshalb sich dem postmortalen Persönlichkeitsrecht potentiell eine Schutz- bzw. Reflexwirkung auch hinsichtlich der digitalen Identität entnehmen lässt.

b) Pränataler Schutz der digitalen Identität

Da dem Anfang stets ein gewisser Zauber inne wohnt, ist nunmehr auf die Geburt der digitalen Identität und deren verfassungsrechtlicher Repräsentation einzugehen. Die Erstellung von Accounts einschließlich der erstmaligen Preisgabe relevanter Informationen ist Teil des informationellen Selbstbestimmungsrechts des Art. 2 Abs. 1 iVm 1 Abs. 1 GG, sofern in die Datenweitergabe und -nutzung hinreichend eingewilligt wurde. Problematisch ist dieser Einwilligungsvorgang jedoch dann, wenn die Einwilligung entgegen der Vorgabe gerade nicht auf Basis einer umfangreichen Kenntnis um den Verbleib und die Nutzung der Daten[176] erfolgt. Im Falle digitaler Identitäten könnte sodann die Weitergabe der Informationen von Kindern problematisch sein, insbesondere im pränatalen Zustand.

173 *Müller-Christmann* in: Hau/Poseck, BeckOK BGB, § 1922, Rn. 99 f; *Herzog*, NJW 2013, 3745 (3746, 3748 f); *Klas/Möhrke-Sobolewski*, NJW 2015, 3473 (3474 f). Erstmals zur Problematik *Hoeren*, NJW 2005.

174 LG Berlin CR 2017, 122 sowie zuletzt KG Berlin CR 2017, 454.

175 Sub Kapitel D.I.1.d).

176 Vgl. § 4a Abs. 1 S. 1 BDSG a.F., Art. 7 Abs. 2, Abs. 4 DSGVO.

Bei der Entstehung einer digitalen Identität eines Kindes durch Weitergabe von Informationen jeglicher Art an Diensteanbieter müsste sodann ebenfalls die informationelle Selbstbestimmung des Art. 2 Abs. 1 iVm 1 Abs. 1 GG zur Anwendung kommen. Einzig die Grundrechtsmündigkeit könnte diesbezüglich bezweifelt werden, würde dem Kind überlassen werden, ob sein Foto bei Facebook oder einem anderen Diensteanbieter mit entsprechender gesellschaftlicher Reichweite veröffentlicht werden soll. Denn die Grundrechtsmündigkeit setzt voraus, dass der Grundrechtsträger selbst und eigenverantwortlich von seinen Grundrechten Gebrauch macht.[177] Ähnlich der Einwilligung kommt es also auf die Verantwortungsfähigkeit und geistige Reife des Kindes an, um die Tragweite einer solchen Veröffentlichung zu verstehen. Da dies regelmäßig bezweifelt werden kann und auch ein Fragen und Erklären der Eltern hieran nichts zu ändern vermag, wäre auf das elterliche Erziehungsrecht aus Art. 6 Abs. 2 S. 1 GG zurückzugreifen. Dieses ist als dienende Freiheit funktional auf den Schutz des Kindes gerichtet und den schließt dessen Persönlichkeitsschutz ein.[178] Exemplarisch erwähnt sei bzgl. der besonderen Beachtung des Kindes im Datenschutzrecht Art. 8 Abs. 1 S. 2 DSGVO, der die Verantwortlichkeit der Eltern für die Einwilligung des Kindes in die Nutzung von Informationsdiensten regelt. Insoweit kommt den Eltern die – mit zunehmendem Alter des Kindes abnehmende[179] – Entscheidungsprärogative bezüglich der digitalen Identität des Kindes zu. In inhaltlicher Hinsicht steht der persönlichkeitsrechtliche Schutz des Kindes dem allgemeinen Persönlichkeitsrecht in Nichts nach. Den Eltern muss aber die besondere Gefahrenlage der digitalen Identität in einem derart frühen Stadium sowie eine mögliche weitere Verarbeitung der Daten des Kindes bewusst sein. Ist dem nicht so, muss von Seiten der Diensteanbieter zumindest hierauf hingewiesen werden. Schließlich müssen sich Kinder, nachdem Eltern Teile ihres Lebens online im Rahmen ihrer eigenen digitalen Identität oder der des Kindes weitergegeben haben, auch während ihrer

177 *Kloepfer*, VerfR II, § 49, Rn. 24; *Hufen*, Staatsrecht II, § 6, Rn. 41.

178 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 7; vgl. *Kloepfer*, VerfR II, § 67, Rn. 19, 30. Korrespondierend zu Art.6 Abs. 1 GG auf Grundlage der Kinderrechtskonvention dem Kind eine eigene schützenswerte Persönlichkeit zuerkennend *Benassi*/*Eichholz*, DVBl 2017, 614 (616).

179 Vgl. *Badura* in: Maunz/Dürig, GG-Kommentar, Art. 6, Rn. 135.

Entwicklung und als erwachsene Person frei von öffentlicher Beobachtung fühlen und entfalten können. Demgemäß besteht ein umfangreicher Schutz des Kindes hinsichtlich seiner digitalen Identität(en).

Obschon einem Kind zumindest im Ursprung ein eigenständiges, da handlungsfähiges, Persönlichkeitsrecht zukommt, wird ein pränataler Persönlichkeitsschutz gelegentlich abgelehnt[180]. Dennoch besteht auch in diesem frühen Stadium als Ausfluss des Achtungsanspruchs des Art. 1 Abs. 1 GG ein Schutz der pränatalen Persönlichkeit.[181] Neben der bereits dargelegten, zeitlich weit zu verstehende Schutzwirkung der Menschenwürde[182] spricht dafür, dass aufgrund werdenden Lebens von einer „potentiellen oder zukünftig handlungsfähigen Person“[183] auszugehen ist. Daher kommt der Achtungsanspruch des Menschen dem Ungeborenen in dieser Phase seines physisch-psychischen Daseins mit Vorwirkung zu, die gewissermaßen als pränatale Reflexwirkung verstanden werden kann. Während dieser Zeit anfallende Daten, welche von Dritten einer digitalen Identität zugeordnet werden und wodurch diese ggf. entsteht, sind sodann auch vom verfassungsrechtlichen Schutz umfasst. Schließlich fallen die Informationen des Kindes, welche die Eltern während der Kindheit im Internet verteilt haben, auf das Kind selbst zurück. Die Verfügungsgewalt über die Daten geht mit zunehmendem Alter auf die Kinder über, vgl. Art. 6 Abs. 2 GG. Konsequent ist eine Möglichkeit des Schutzes digitaler Replikas auch auf Daten aus diesem Zeitraum zu erstrecken, beispielsweise verbreitete (Ultraschall-)Bilder und Informationen des Kindes in sozialen Netzwerken. Darüber hinaus kommt ihnen als Konkretisierung des Rechts auf informationelle Selbstbestimmung ein datenschutzrechtlicher Schutz zu: Je nach

180 *Jarass* in: Jarass/Pieroth, GG-Kommentar, Art. 2, Rn. 51; *Dreier* in: Dreier, GG, Art. 2 I, Rn. 81; *Kunig* in: von Münch/Kunig, GG, Art. 2, Rn. 5.

181 *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 395; *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2, Rn. 227. Aus Art. 2 Abs. 1 GG schließend dagegen *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2, Rn. 49 – was allerdings mangels einer aktiven Einwirkungsmöglichkeit des Menschen im pränatalen Stadium abzulehnen ist. Andernfalls müssten persönlichkeitsrechtliche Aspekte, welche der Embryo nicht wahrnehmen kann, ausgeschlossen oder anderweitig geltend gemacht werden. So fällt die Verwaltung der Informationen des Kindes auch während dieses Stadiums gem. Art. 6 Abs. 1 GG den Eltern zu.

182 Siehe sub B.II.1.

183 BVerfGE 30, 173 (194).

Sachlage handelt es sich um Gesundheitsdaten iSd Art. 9 Abs. 1 und des Erwägungsgrundes 35 DSGVO (erneut: Ultraschallbild) oder auch allgemein um personenbezogene Daten, wie beispielsweise der Name des Kindes. Eine Anwendung des Art. 8 DSGVO scheidet dagegen schon faktisch aus, da ein Kind im pränatalen Stadium keine Informationsdienste wahrnehmen kann und folglich der Anwendungsbereich der Norm schon nicht eröffnet ist. Dennoch ist nach der Prämisse des Erwägungsgrundes 38 S. 1 DSGVO von einem hohen Schutz im Rahmen von Abwägungen auszugehen.

Nun könnte sich während des pränatalen Zeitraums allerdings der Fall ergeben, dass bereits eine digitale Identität des Ungeborenen geschaffen wurde, das ungeborene Kind jedoch verstirbt. Daraufhin ist zu diskutieren, inwieweit einem noch nicht geborenen Menschen ein postmortaler Persönlichkeitsschutz im Rahmen des pränatalen Persönlichkeitsschutzes zukommt. Ein auf der gelebten Persönlichkeit basierender Schutz iSd personalen und sozialen Geltungswertes ist schon nicht gegeben, da sich die Persönlichkeit des Ungeborenen nicht derart entwickeln konnte. Zumindest ist diese nicht derart – sowohl analog als auch digital – nach Außen getreten, als dass die für eine Identität existenzielle Wechselwirkung hätte eintreten und so ein sozialer Geltungsanspruch entstehen können. Insofern ist zumindest auf den allgemeinen Achtungsanspruch zurückzugreifen, der jedem Menschen in jeder Lebensphase zukommt. Insbesondere bezüglich jener persönlichkeitsrechtlicher Elemente, die diesen Achtungsanspruch in ihrer speziellen Fallgruppe konkretisieren, kommt dem verstorbenen Ungeborenen ein persönlichkeitsrechtlicher Schutz zu.[184] Namentlich sind dies das Recht am eigenen Bild und das Recht der persönlichen Ehre als Ausprägungen der Art. 2 Abs. 1 iVm 1 Abs. 1 GG, in Einzelfällen auf das dem Persönlichkeitsrecht entwachsene Recht auf informationelle Selbstbestimmung unter der bereits erwähnten Maßgabe des Elternrechts gem. Art. 6 Abs. 2 GG. Das Recht der Geltendmachung kommt daher den Hinterbliebenen, also den Eltern, im Rahmen ihrer Grundpflicht aus Art. 6 Abs. 2 S. 1 GG zu. Schließlich umfasst diese als lex specialis im Falle der Eltern

184 Ebenfalls der Ansicht, allerdings mit Fokus auf die informationelle Selbstbestimmung *Harks*, NJW 2002, 716 (719).

auch die Totensorge des Kindes.[185] Zu beachten ist allerdings, dass mangels des sozialen Geltungsanspruchs eine verhältnismäßig kurze Dauer des Schutzes zu wählen ist. Einzubeziehen sind aber der Bekanntheitsgrad des Ungeborenen und die hohe Sensibilität der Trauer[186].

3. Zusammenfassung

Auf Grundlage des eingangs dargestellten weiten Schutzes des Menschen in seiner analogen Identität lässt sich parallel der Lebenszyklus der digitalen Identität den einzelnen analogen Lebensphasen zuordnen und die Schutzfähigkeit in dieser analogen Lebensphase grundsätzlich bejahen. Ein entsprechend Bild ergibt sich bei der Gegenüberstellung mit der Definition der digitalen Identität, da sich die analogen Lebensphasen in einzelne digitale Aspekte des Grundrechtskatalogs potentiell einordnen lassen. Damit ist die weitere konkrete Prüfung der einzelnen Schutzgüter eröffnet. Prima facie ergibt sich ein zeitlich vollumfänglicher Schutz der digitalen Identität natürlicher Personen.

III. Juristische (digitale) Personen

Weiterhin ist die Relation zwischen juristischen Personen als Grundrechtsträger und ihrer digitalen Identität zu untersuchen. Dies erscheint nur folgerichtig, wo der Zugang zum Internet und somit die Nutzung digitaler Identitäten, wie bereits gezeigt, nicht nur natürlichen Personen möglich ist. Grundrechtsrelevante Handlungen erfolgen zwar auch bei juristischen Personen durch natürliche Personen, jedoch sind diese Handlungen bei Unternehmensbezug iSe Organhandelns dem

185 Zum zeitlichen Umfang siehe *Robbers* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 6 Abs. 2, Rn. 155-158. Zur Totensorge des Kindes *Rixen*, FamRZ 1994, 417 (420 f).

186 Diese sollte zumindest dahingehend beachtet werden, dass eine Verletzung bereits durch einfachere ehrverletzende Äußerungen des Kindes gegeben sein kann, wenn der Tod hinreichend aktuell ist.

Unternehmen zuzuordnen.[187] Dabei kann eine Corporate Identity als Leitbild fungieren und die Handlungen vereinheitlichen.[188]

Während sich der grundrechtliche Schutz natürlicher Personen unmittelbar aus dem Wortlaut des Art. 1 Abs. 1, Abs. 2 GG folgern lässt, kommt juristischen Personen diesbezüglich eine Sonderrolle zu. Denn der Regelfall, der in den Art. 1-19 GG niedergelegt ist, bezieht sich lediglich auf den Menschen als geborenen Grundrechtsträger. Dafür spricht insbesondere der Wortlaut des Art. 19 Abs. 3 GG, welcher mit „auch" die Erweiterung des üblichen Anwendungsbereiches meint – ebenfalls bezeichnet als Erstreckungsgarantie. Die Erstreckung der Freiheiten natürlicher Personen auf juristische Personen dient insbesondere der Effektuierung und Wirkkraftverstärkung der individuellen Freiheitsentfaltung.[189] Insoweit lässt sich den einzelnen Grundrechten nicht entnehmen, dass eine Anwendbarkeit auf juristische Personen grundsätzlich möglich ist. Der Klarstellung halber wurde daher in Anlehnung an die Vorlage der Bayerischen Staatsregierung die Rechtsstellung juristischer Personen in Art. 19 Abs. 3 GG eingefügt.[190] Demgemäß können sich auch inländische (privatrechtliche) juristische Personen auf Grundrechte berufen, soweit sie ihrem Wesen nach anwendbar sind. Diese Formel enthält damit zugleich Voraussetzungen und Grenzen der Grundrechtsanwendung, auf welche nachfolgend jeweils in entsprechendem Umfang eingegangen wird. Der Schwerpunkt liegt dabei in der Ermittlung der wesensmäßigen Anwendbarkeit bei digitalen Identitäten.

187 Hierzu sogleich bei der Darstellung der wesensmäßigen Anwendbarkeit der Grundrechte in Kapitel B.III.2. Vgl. auch BVerfGE 20, 323 (336).

188 Vgl. Kapitel B.I.3.b).

189 So zur Erstreckungsgarantie sowie dem Sinn der Freiheitenverstärkung *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 26, 28; *Rüfner* in: Isensee/Kirchhof, HStR IX, § 196, Rn. 60; *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 81; *Dürig* in: Maunz/Dürig, GG-Kommentar (2003), Art. 19, Rn. 1.

190 *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 5; vgl. auch *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 80. Ausführlicher zur Historie *Stern*, StaatsR III/1, § 71, S. 1089 ff, insbes. 1095 f.

1. Juristische, inländische Personen

So verlangt Art. 19 Abs. 3 GG zuvorderst, dass es sich um eine juristische Person handelt. Anerkanntermaßen sind hierunter sämtliche voll- und teilrechtsfähigen Personengebilde zu verstehen.[191] Nicht umfasst sind dagegen alle nichtrechtsfähigen Organisationen[192] einschließlich unstrukturierter Personengruppierungen[193]. Maßgebliches Kriterium ist also nicht die privatrechtliche Zuordnung, sondern ausschließlich die Rechtsfähigkeit im Allgemeinen.[194] Grundsätzlich ist allerdings – und so auch hier – davon auszugehen, dass juristische Personen, welche beispielsweise im Wege ihrer Corporate Identity ihre digitale Identität im Internet bilden und nutzen, (teil-)rechtsfähig sind.[195] Problematische Einzelfälle sind an dieser Stelle auszublenden, um den Fokus für den eigentlichen Untersuchungsgegenstand nicht zu verlieren.

Weiterhin ist es gem. Art. 19 Abs. 3 GG erforderlich, dass es sich um eine inländische juristische Person handelt, welche sich auf ihre Grundrechte beruft bzw. deren digitale Identität potentiell durch Grundrechte geschützt sein könnte. Als inländisch wird dabei grundsätzlich jede juristische Person bezeichnet, welche ihren effektiven Sitz, also das tatsächliche Zentrum ihrer Aktionen, im Inland – also innerhalb der Staatsgrenzen[196] – hat.[197] Maßgebend ist hierfür der Ort, an dem die Mehrheit der Entscheidungen der Geschäftsführung gefällt wird.[198]

191 *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 37 ff; *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 31, 32.

192 *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 41.

193 *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 34.

194 *Dürig* in: Maunz/Dürig, GG-Kommentar (2003), Art. 19, Rn. 8, 29.

195 Handelt es sich nur um eine, bereits erwähnte, lose Personengruppierung, so kann sich diese entweder über die einzelnen Teilnehmer auf die Individualgrundrechte oder auf die Kollektivgrundrechte berufen. Eine Lücke im verfassungsrechtlichen Schutzkonzept besteht dahingehend nicht.

196 *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 47; *Huber* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 19 III, Rn. 296.

197 BVerfG NJW 2018, 2392 (2393, Rn. 29); *Enders* in: Epping/Hillgruber, BeckOK GG, Art. 19, Rn. 36; *Sachs* in: Sachs, GG, Art. 19, Rn. 54.

198 *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 78. Ähnliches ergibt sich, wenn analog der Begriff der Niederlassung des Diensteanbieters aus Art. 4 Nr. 16 lit. a) DSGVO herangezogen wird – vgl. auch EuGH, Urteil vom 01.10.2015, Az. C-230/14, Rn. 29.

Mitnichten kommt es also auf die Staatsangehörigkeit der Mitarbeiter eines Unternehmens[199] oder den bloßen örtlichen Sitz des Unternehmens[200] an. Dies ist schon dem Sinn des Art. 19 Abs. 3 GG nach zu verwehren, kommt es für die o.g. Freiheitenverstärkung der wirtschaftlich tätigen natürlichen Personen eben darauf an, dass sie ihre Freiheiten innerhalb Deutschlands ausüben.[201] Im Falle digital agierender Unternehmen ist folglich auf den erwähnten Ort der aktiven Geschäftsführung abzustellen, welcher sich bei einem (landes-)grenzenlosen Aktionsort wie dem Internet zunächst nur schwer einwandfrei zuordnen lässt. Nicht selten werden Marketing-Strategien nicht nur lokal oder regional, sondern weltweit organisiert – was den Aktionsradius entsprechend erweitert. Zudem liegt der Ort der aktiven Geschäftsführung bei namhaften Unternehmen außerhalb Deutschlands, und nur eine Tochterfirma als Repräsentations- und PR-Standort ist in Deutschland zugegen. Liefert auch letztere keine Anhaltspunkte für eine „deutsche Geschäftsführung" von dieser aus, so erscheint eine Befürwortung der Anforderung des Art. 19 Abs. 3 GG schwierig. Die damit skizzierte Problematik soll vorliegend lediglich die Komplexität der weltumspannenden Digitalisierung aufzeigen; eine Lösung sowie tiefergehende wissenschaftliche Betrachtung bleibt mit Blick auf den Prüfungsgegenstand zu vertagen. Im Folgenden wird dieses Merkmal daher nicht weiter bestritten.

2. Wesensmäßige Anwendbarkeit der Grundrechte

Unter Einbeziehung der bisherigen Ausführungen kann aus der Lesart des Wortlautes des Art. 19 Abs. 3 Hs. 1 GG – „Die Grundrechte gelten auch für inländische juristische Personen..." – vorerst geschlossen werden, dass auch für juristische

199 BVerfGE 21, 207 (209); *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 80.
200 *Dürig* in: Maunz/Dürig, GG-Kommentar (2003), Art. 19, Rn. 31.
201 Vgl. *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 82 sowie *Dürig* in: Maunz/Dürig, GG-Kommentar (2003), Art. 19, Rn. 4.

Personen eine vollumfängliche Grundrechtsberechtigung möglich ist. Anschließend ist diese weite Aussage hingegen, wie üblich dem juristischen Grundsatz-Ausnahme-Schema folgend, durch die Restriktion des Art. 19 Abs. 3 Hs. 2 GG einzuschränken, was sich hinreichend durch das Wort „soweit" ausdrückt.[202] Ob und wie Grundrechte auf eine juristische Person anwendbar sind, muss sodann durch die tiefgehende Prüfung der wesensmäßigen Anwendbarkeit der Grundrechte geklärt werden. Eingeschlossen darin ist auch die Frage, ob bzw. wie Grundrechte auf juristische Personen des *Privatrechts* oder des *öffentlichen Rechts* anzuwenden sind. Schließlich ist bei der Untersuchung des Wesens der juristischen Person neben dem Vergleich zur natürlichen Person auch die Einordnung des Wesens selbst von Relevanz. Dafür spricht insbesondere der neutrale Wortlaut des Art. 19 Abs. 3 GG: Das Wesen und seine Vereinbarkeit ist für die jeweilige juristische Person festzustellen und nicht prinzipiell zu Beginn auszuschließen.[203] Die Differenzierung nach der Rechtsform bietet sich daher an dieser Stelle an, wenngleich vereinzelt die Zuordnung bereits bei der Frage nach der *juristischen* Person erfolgt[204].

a) Anwendbarkeit auf öffentlich-rechtliche juristische Personen

Vor der detaillierten Prüfung der wesensmäßigen Anwendbarkeit in materieller Hinsicht sei allerdings darauf hingewiesen, dass sich Art. 19 Abs. 3 GG grundsätzlich ausschließlich auf privatrechtlich organisierte juristische Personen bezieht – öffentlich-rechtliche juristische Personen folglich nicht grundrechtsberechtigt sind.[205] Dies folgt nicht bloß aus der Ermangelung einer Regelung, ähnlich derer

202 So auch *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 50. Ähnlich auf das Wesen abstellend *Dürig* in: Maunz/Dürig, GG-Kommentar (2003), Art. 19, Rn. 35 sowie *Stern*, StaatsR III/1, § 71, S. 1110.

203 Vgl. *Bethge*, Grundrechtsberechtigung juristischer Personen, S. 61, 69 f. Zur europarechtlichen Parallele der Ermittlung der Wesensmäßigkeit siehe nur *Heißl*, EuR 2017, 561 (564 f, 567).

204 Derart prüfend *Windthorst* in: Gröpl/Windthorst/von Coelln, StuKo GG, Art. 19, Rn. 42, 49 f; *Kingreen*/*Poscher*, Staatsrecht II, Rn. 164.

205 Vgl. *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 25.

in Art. 19 Abs. 3 GG, sondern aus dem rechtlichen Charakter der Grundrechte: Grundrechte als Menschenrechte haben im Kern eine Abwehrfunktion gegenüber staatlichen Eingriffen. Zugleich gewähren sie dadurch Freiheiten, teilweise auch Leistungsrechte.[206] Der telos der Art. 1-19 GG widerspricht folglich einer Auslegung in diese Richtung, denn durch eine Erweiterung der Gewährleistung grundrechtlich geschützter Freiheiten auf juristische Personen des öffentlichen Rechts besteht aufseiten des geborenen Grundrechtsträgers dann keine Grenze, kein Schutzwall qua Abwehrfunktion mehr.[207] Im Gegenteil: Die Interessenabwägung, üblicherweise auf der Ebene der mittelbaren Drittwirkung zwischen Privaten bekannt, ist dann ebenfalls zwischen Staat und Bürger zu führen. Die eigentliche Stärke der Grundrechte als Freiheitenkatalog zum Schutz natürlicher Personen im Subordinationsverhältnis wäre aufgelöst. Ferner noch, würde so die Konzeption des Staates, durch Grundrechte ein Kräfteverhältnis zugunsten des Bürgers zu erhalten und so historische Ereignisse entsprechend zu würdigen,[208] leerlaufen. Gleiches gilt sodann für die Verfassungsbeschwerde als Rechtsbehelf des Bürgers gegen Eingriffe des Staates,[209] verweisen doch Art. 93 Abs. 1 Nr. 4a GG sowie § 90 Abs. 1 BVerfGG expressis verbis auf eine Verletzung durch die öffentliche Gewalt. Mithin kann öffentlich-rechtlichen Organisationsformen, welche den Gewalten iSd Art. 1 Abs. 3, 20 Abs. 2 GG zuzuordnen sind, gewissermaßen kein Schutz vor „sich selbst“ gewährt werden. Der Staat kann nicht gleichzeitig Adressat und Berechtigter der Grundrechte sein.[210] Juristische Personen des öffentlichen Rechts sind daher ausschließlich Grundrechtsverpflichtete.[211] Lediglich in Ausnahmefällen, in denen die öffentlich-rechtliche juristische Person dem

206 So die Grundlage des Konfusionsarguments – vgl. *Rüfner* in: Isensee/Kirchhof, HStR IX, § 196, Rn. 112; *Schnapp* in: Merten/Papier, HGr II, § 52, Rn. 27. Kritisch dagegen *Merten*, DÖV 2019, 41 ff. Zu den Funktionen der Grundrechte im Einzelnen siehe *Jarass* in: Merten/Papier, HGr II, § 38, Rn. 15 ff, 22 ff sowie sub C.I. und II.

207 Vgl. *Bethge*, Grundrechtsberechtigung juristischer Personen, S. 64 f.

208 Vgl. BVerfGE 6, 55 (71); 27, 71 (84).

209 *Bethge*, Grundrechtsberechtigung juristischer Personen, S. 68.

210 Sog. Konfusionsargument — BVerfGE 15, 256 (262); 21, 362 (369 f); 39, 302 (312 ff); 62, 354 (369); *Schnapp* in: Merten/Papier, HGr II, § 52, Rn. 27 f; *Bethge*, Grundrechtsberechtigung juristischer Personen, S. 65 f; *Kloepfer*, VerfR II, § 49, Rn. 57.

211 So auch stRspr des BVerfG — allgemein nur BVerfGE 107, 299 (309 f), für einzelne Fälle siehe *Sachs* in: Sachs, GG, Art. 19, Rn. 92 sowie Fn. 310.

bislang durch das Bundesverfassungsgericht ausgeformten Ausnahmentrias zugeordnet werden kann, ist von einer Grundrechtsberechtigung öffentlich-rechtlicher juristischer Personen auszugehen.[212]

Gerade weil auch diese Art der juristischen Personen durch einen Webauftritt das eigene Beratungsangebot der örtlichen Behörden mittels Repräsentation eine digitale Identität bildet,[213] erscheint die eben dargelegte und der herrschenden Ansicht entsprechenden Ablehnung einer Grundrechtsträgerschaft öffentlich-rechtlicher juristischer Personen hingegen brüchig[214]. Denn auch die Repräsentation der digitalen Identität dieser juristischen Personen ist vor Eingriffen nicht kraft ihrer rechtlichen Zuordnung geschützt, sondern unterliegt auf den ersten Blick gleichartigen Angriffen. Möglicherweise könnte sich diesbezüglich die von Seiten der Literatur vertretene, für eine wesensmäßige Anwendung erforderliche grundrechtstypische Gefährdungslage feststellen lassen. Diese setzt eine vergleichbare Gefährdung der Freiheitsrechte von Seiten des Staates voraus, der die juristische Person wie eine natürliche Person unterliegt.[215] Eine vergleichbare Lage zwischen natürlichen Personen und öffentlich-rechtlichen juristischen Personen liegt zwar wie erwähnt

212 Hierzu *Sachs* in: Sachs, GG, Art. 19, Rn. 93 ff; *Bethge*, Grundrechtsberechtigung juristischer Personen, S. 77 ff.

213 So dürfen beispielsweise gemäß der Richtlinie des Landesamtes für Datenschutz und Informationsfreiheit Baden-Württemberg in gewissem Rahmen auch soziale Netzwerke nutzen, um die Öffentlichkeit besser und direkter zu informieren (so auch *Kalscheuer*/*Jacobsen*, NJW 2018, 2358 (2361)). Messenger, wie sie bei dem sozialen Netzwerk Facebook Teil der Plattform sind, sind von der Nutzung durch öffentliche Stellen allerdings ausgeschlossen – siehe https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/11/2017.11.02._Richtlinie-zur-Nutzung-sozialer-Netzwerke-durch-Ãűff.-Stellen.pdf sowie die Stellungnahme von LfDI *Brink*, DSB 2020, 43 ff.; im Detail auch *Engeler*, MMR 2017, 651. *Engeler* merkt aber zutreffend die datenschutzrechtliche Relevanz der Verarbeitung der Besucherdaten durch den Diensteanbieter an, welcher insoweit unumgänglich ist und die der Verantwortlichkeit der öffentlichen Stelle bedarf. Selbiges lässt sich aus dem Urteil des EuGH zu Facebook-Fanseiten schließen – Urteil vom 5.6.2018, Az. C-210/16, Rn. 39. Zu Inhalt und Grenzen der Öffentlichkeitsarbeit siehe vgl. BVerfGE 44, 125 (147 ff) sowie *Gersdorf*, AfP 2016, 293 (294, 295 f); vgl. *Weberling*, AfP 2003, 304 (305 f) sowie OVG Münster, Urteil vom 17.9.2019, Az. 15 A 4753/18 = ZUM 2020, 646 ff.

214 Ebenso die Instabilität des Ausnahmetrias feststellend *Ludwigs*/*Friedmann*, JA 2018, 807 (811).

215 *Von Mutius* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 19 III, Rn. 114; *Krebs* in: von Münch/Kunig, GG, Art. 19, Rn. 45; *Isensee* in: Isensee/Kirchhof, HStR IX, § 199, Rn. 9 f, 49 f; *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 53 ff; *Kingreen*/*Poscher*, Staatsrecht II, Rn. 174.

darin, dass eine Gefährdung der im Internet vorhandenen Daten zur eigenen (digitalen) Identität grundsätzlich bestünde. So sind beispielsweise auch Behörden den Bewertungen von Grundrechtssubjekten auf Google Maps ausgesetzt.[216] Bei Lichte betrachtet liegt allerdings keine Gefährdung durch den Staat vor, sondern eine Gefährdung durch Angriffe Privater, ggf. sogar durch Grundrechtssubjekte. Per definitionem kann also keine grundrechtstypische Gefährdungslage entstehen, zeichnet sich diese – grundrechtstypisch – durch die Prägung staatlicher Gewalt aus.

Stattdessen könnte am durch das Bundesverfassungsgericht tradierten Konstrukt des personalen Substrats festzuhalten sein, sich also an der Bildung und Betätigung der juristischen Person orientiert wird bzw. gerade dies Ausdruck der freien Entfaltung natürlicher Personen ist. Dies ist besonders dann der Fall, „wenn der *Durchgriff* auf die hinter den juristischen Personen stehenden Menschen dies als sinnvoll und erforderlich erscheinen lässt“ (daher: Durchgriffsthese).[217] Demnach müsste die Ausbildung einer digitalen Identität der öffentlich-rechtlichen juristischen Person eine Verwirklichung der Freiheiten der dahinter stehenden natürlichen Personen darstellen, die juristische Person damit nur verlängerter Arm der natürlichen Person sein. Dieser Schluss gelingt allerdings nicht bei öffentlich-rechtlichen juristischen Personen, da deren Repräsentation nicht einem verlängerten Arm entspricht, sondern beispielsweise eher der Informationspflicht des Staates gegenüber dem Bürger[218] Genugtuung verschafft. Ihr Handeln dient

216 Siehe nur https://www.google.de/maps/place/Ordnungsamt+der+Stadt+Leipzig/@51.330741,12.3617822,15z/data=!4m8!1m2!2m1!1zYmVow7ZyZGUgZsO8ciDDtmZmZW50bGljaGUgc2ljaGVy!3m4!1s0x47a6f8260ce4ca11:0xcaac43ac9d2ea574!8m2!3d51.3267084!4d12.3997424 für Bewertung zum Ordnungsamt der Stadt Leipzig oder die Bewertungen zum Bundesministerium des Innern unter https://www.google.de/maps/place/Bundesministerium+des+Innern,+fÃijr+Bau+und+Heimat/@52.52263,13.3612314,17z/data=!3m1!4b1!4m5!3m4!1s0x47a851a099c4373d:0x4a0154a2817c3ffd!8m2!3d52.52263!4d13.3634201.

217 BVerfGE 21, 362 (369); 61, 82 (101) – Hervorhebung im Original nicht enthalten. Ebenso *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 30 ff.

218 Vgl. *Kloepfer*, VerfR II, § 61, Rn. 47; *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 5 Abs. 1 und II, Rn. 19.

folglich der Erfüllung öffentlicher Aufgaben und vollzieht sich nicht in der Wahrnehmung unabgeleiteter Freiheiten.[219] Von einer Erweiterung oder Erhaltung der grundrechtlichen Freiheiten, wie schon iSd erwähnten Erstreckungslehre Art. 19 Abs. 3 GG verstanden wird, kann vorliegend deshalb keine Rede sein. Die Bejahung der Grundrechtsträgerschaft auf dieser Basis schlägt damit ebenso fehl.

Letztlich ist damit weder gemäß des Wortlautes des Art. 19 Abs. 3 GG noch durch Hinzunahme etablierter Auslegungsweisen von Judikatur und Literatur eine Grundrechtsträgerschaft bzgl. der digitalen Identität öffentlich-rechtlicher juristischer Personen möglich – spezielle Grundrechtsträger wie Rundfunkanstalten oder Universitäten als Teil des Ausnahmetrias ausgenommen.

b) Anwendbarkeit auf privatrechtliche juristische Personen

Die Grundrechtsträgerschaft juristischer Personen des Privatrechts ist dagegen nicht schon zu Beginn problematisch und prinzipiell anzunehmen, wobei die grundrechtsspezifische Bejahung erst nach einer gesonderten Prüfung im Rahmen der angedeuteten Grundsätze erfolgen kann.[220] Hierzu muss die privatrechtliche juristische Person Eigenarten aufweisen, welche derart menschenähnlich sind, dass sie sich ebenfalls auf Grundrechte natürlicher Personen berufen kann.[221] Mit anderen Worten: Ist der zu untersuchende grundrechtliche Aspekt nicht ausschließlich den menschlichen Wesenszügen zuzuordnen, sondern auch auf abstrakte Persönlichkeiten wie juristische Personen übertragbar, so kann die Grundrechtsfähigkeit diesbezüglich bejaht werden.[222] Zur Analyse dieser Wesensmäßigkeit ist neben dem geeigneten Grundrechtstatbestand sowie den charakteristischen

219 *Huber* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 19 III, Rn. 245.
220 Eine generelle Grundrechtsfähigkeit besteht nicht, kann sie schon nicht aus dem Wortlaut des Art. 19 Abs. 3 GG gerechtfertigt werden. – Vgl. *Isensee* in: Isensee/Kirchhof, HStR IX, § 199, Rn. 23. Dagegen eine Wirkkraft im Ansatz bereits annehmend *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 50.
221 Vgl. *Sachs* in: Sachs, GG, Art. 19, Rn. 67.
222 BVerfGE 95, 220 (242); 118, 168 (203).

Zügen der juristischen Person wie Aufgaben und Funktionen als Vergleichsgrundlage ebenfalls die Theorie der grundrechtsspezifischen Gefährdungslage oder des personalen Substrats hinzuzuziehen.[223] Dabei genügt es, wenn Teilgehalte einer Grundrechtsgarantie auf die juristische Person anwendbar sind.[224] Mangels einer konkreten juristischen Person als Analyseobjekt sei für die nachfolgende Einordnung von einem Modell der juristischen Person auszugehen, welche sich durch Konten bei sozialen Netzwerken oder ähnlichen Telemedien und ggf. notwendigen Bestellkonten oder Konten bei Drittanbietern, eigene Websites und E-Mail-Datenverkehr im Internet bewegt. Die juristische Person agiert insgesamt als Dienstleister, für den sowohl die Corporate Identity als auch der Umgang mit Benutzerkonten der Kunden sowie der eigenen Mitarbeiter üblich ist. Dies sollte im Grundsatz dem Großteil der aktuell digital agierenden juristischen Personen entsprechen.

Entsprechend der eingeführten Agenda bedarf es zunächst der funktionalen Zuordnung der juristischen Person zu entsprechend geeigneten Grundrechten. Vorliegend kann auf die bei digitalen Sachverhalten üblichen Grundrechte abgestellt werden, sodass für eine nähere Betrachtung das Allgemeine Persönlichkeitsrecht gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG mit seinen eigenständigen Spielarten der informationellen Selbstbestimmung sowie dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme relevant erscheint. Diese können grundsätzlich auch juristische Personen geltend machen, liegt ihr materieller Schwerpunkt doch auf Art. 2 Abs. 1 GG.[225] Je nach Art und Weise des Eingriffs kommen aber auch Art. 10 Abs. 1 GG in seiner fernmeldetechnischen Variante sowie Art. 12 Abs. 1 und 14 Abs. 1 GG in Betracht. Artikel 12 Abs. 1 GG käme aber nur dann zur Anwendung, wenn staatliche Restriktionen aufgrund mittelbarer Wirkungen ebenfalls objektive berufsregelnde Tendenzen aufweisen[226]. Die Eigentumsfreiheit könnte im weiteren Sinne auch den Ruf des

223 Vgl. *Kingreen*/*Poscher*, Staatsrecht II, Rn. 174; *Hofmann* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Art. 19, Rn. 25.
224 *Sachs* in: Sachs, GG, Art. 19, Rn. 67.
225 Vgl. BVerfGE 95, 220 (242); 118, 168 (203).
226 Zum mittelbaren Eingriff vgl. *Kingreen*/*Poscher*, Staatsrecht II, Rn. 918 f.

Unternehmens – also die Repräsentation der Unternehmenspersönlichkeit bzw. Corporate Identity – als Teil des eingerichteten und ausgeübten Gewerbebetriebes schützen. Weiterhin besteht bezüglich der Eigentumsfreiheit des Art. 14 Abs. 1 die Unstimmigkeit, ob Unternehmensdaten wie die angelegten Datenbanken mit Kundendaten, welche durch Eingriffe beeinträchtigt, entnommen oder vervielfältigt werden, (Unternehmens-)Eigentum iSd Grundgesetzes darstellen. Summarisch besteht also die Möglichkeit einer Grundrechtsposition, was für die weitere Prüfung ausreicht. Die Prüfung der anwendbaren Schutzbereiche folgt später en détail.[227]

Mit Blick auf die beiden definitorischen Waagschalen der Wesensmäßigkeit lässt sich anhand der Durchgriffsthese bereits die Nähe zur menschlichen Freiheitsnutzung erkennen: Eine derartige Handlungsweise entspricht der Erweiterung der Freiheiten natürlicher Personen. Wenn schon letztere das Internet als Medium der Kommunikation und Selbstverwirklichung ohne größere Hindernisse nutzen können, ist dies iSd Durchgriffsthese erst Recht juristischen Personen zu gewähren. Nichts anderes gilt auch für den Umgang mit Daten bzw. Informationen und technischen Systemen, welcher beiden Grundrechtssubjekten gleichermaßen bekannt ist.[228] Bezugnehmend auf den Lebenszyklus der digitalen Identität findet sich ebenfalls keine hinreichende Differenz zwischen der digitalen Identität einer natürlichen und juristischen Person: Auch die digitale Identität juristischer Personen erwacht durch Einrichtung des Systems oder die erstmalige Registrierung zum Leben, lebt durch die Ansammlung von Daten und „stirbt", wenn die Unternehmenspersönlichkeit beispielsweise durch die Insolvenz und Auflösung des Unternehmens hinfällig wird.[229] Ferner wäre es widersprüchlich, Marktteilnehmern innerhalb Deutschlands aufgezeigte Nutzungsweisen des Internets zu versagen und so Einfluss auf den internationalen Wettbewerb zu nehmen.

Sollte vielmehr nach Ansicht der Literatur die grundrechtliche Gefährdungslage das Zünglein an der Waage sein, so kommt man diesbezüglich zu keinem anderen

227 Siehe Kapitel D.I.2.
228 Vgl. *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 33.
229 Zurückgreifend auf die Terminologie des Kapitels B.II.2.

Ergebnis. Auch juristische Personen des Privatrechts unterliegen der Gefährdung durch Angriffe auf ihre informationstechnischen Systeme und darin befindliche Informationen, weshalb allein schon Art. 2 Abs. 1 iVm 1 Abs. 1 GG – oder korrekter: nur Art. 2 Abs. 1 GG – relevant erscheint. Weitere, Art. 12 Abs. 1, 14 Abs. 1 sowie 10 Abs. 1 GG betreffende Gefährdungslagen sind ebenfalls entsprechend wahrscheinlich. Dies zeigt sich am Beispiel des Kommunikationstools *Slack*, welches des öfteren digital angegriffen wurde.[230] Während dieses Programm dazu dient, zwischen Mitarbeitern eines Unternehmens eine Kommunikationsplattform zu schaffen, stellt der Server mit den Kommunikationsdaten über laufende Projekte, die Aufteilung von Teams oder auch private Nachrichten der Mitarbeiter untereinander eine Datenquelle mit hinreichenden Daten zum Unternehmen dar. Sodann sind nicht nur die Mitarbeiter als natürliche Personen Opfer des Angriffs, sondern das Unternehmen in seiner Gesamtheit. Soweit detaillierte Informationen durch Angriffe offen gelegt werden, kann sich dies auf den Ruf oder die Position im Wettbewerb auswirken und so in einer Grundrechtsbeeinträchtigung in Art. 12 Abs. 1, 14 Abs. 1 GG niederschlagen. Aber auch zum Ende des Lebenszyklus der digitalen Identität, z.B. nach der Abwicklung eines Unternehmens, wenn die digitale Identität nicht mehr aktiv genutzt wird und der Ruf und die Marke in nicht vom Unternehmen kontrollierbaren Telemedien als Hülle im Internet verbleibt, könnte ein hinreichender Schutz notwendig sein. Eine wesensmäßige Anwendung kann so von beiderlei Positionen als möglich angesehen werden.

Damit steht der prinzipiellen Grundrechtsträgerschaft juristischer Personen des Privatrechts iSd Art. 19 Abs. 3 GG hinsichtlich ihrer digitalen Identität nichts entgegen.

230 Siehe https://www.heise.de/developer/meldung/Zahlreiche-Zugangsdaten-fuer-den-Messaging-Dienst-Slack-auf-GitHub-entdeckt-3194000.html sowie https://techcrunch.com/2015/03/27/slack-got-hacked/.

3. Zusammenfassung

Juristische Personen gem. Art. 19 Abs. 3 GG können sich demgemäß nur auf bestimmte, wesensmäßige Grundrechte berufen, welche entsprechende Nähe zur digitalen Identität aufweisen. Exemplarisch ist da an Art. 10 Abs. 1, 14 Abs. 1 sowie 12 Abs. 1 GG zu denken. Eine besondere Betrachtung bedarf darüber hinaus das Allgemeine Persönlichkeitsrecht des Art. 2 Abs. 1 iVm 1 Abs. 1 GG mit Fokus auf die anwendbaren Fallgruppen ohne Menschenwürde-Bezug. Der damit gefasste verfassungsrechtliche Rahmen gilt allerdings nur für juristische Personen des Privatrechts, da es bei öffentlich-rechtlichen juristischen Personen im Grundsatz schon an den Voraussetzungen des Art. 19 Abs. 3 GG unter Einbeziehung tradierter verfassungsrechtlicher Grundsätze fehlt. Im Folgenden bezieht sich der terminus der juristischen Person iSd Art. 19 Abs. 3 GG damit ausschließlich auf die privatrechtliche juristische Person, welche sodann neben die natürlichen Personen in den Fokus dieser Arbeit rückt.[231]

IV. Künstliche digitale Identitäten

Löst man sich nun von der bisherigen Betrachtungsweise, kann der Begriff der „digitalen Identität“ durchaus auch eine ganz andere Lesart aufweisen: Anstatt einer digitalen – also digitalisierten oder digital festgehaltenen – Identität, kann darunter ebenfalls eine künstliche Identität verstanden werden. Die Digitalität[232] der Identität besteht sodann vielmehr darin, dass die Identität nicht auf einer realen Person, sondern lediglich in bzw. aus Quellcode besteht. Sie entspricht also einer digital geschaffenen Persönlichkeit, welche Kraft ihres Quellcodes in einem gewissen Rahmen selbstständig agieren kann. Der Umfang der Selbstständigkeit ist allerdings relativ und von der beabsichtigten Nutzungsweise abhängig.

231 Siehe Kapitel D.I.2.
232 Angelehnt an das Wort „digitality“, welches als „quality of being digital“ definiert wird.

So sind Bots in sozialen Netzwerken[233] mittels einer einprogrammierten künstlichen Intelligenz, welche die Bots unter Verwendung neuronaler Netze lernfähig macht[234], zu anderen Handlungen imstande als ein Roboter, welcher aufgrund seiner Menschenähnlichkeit auch in der Realität mit anderen Personen interagieren kann. Letztere Erscheinung mag auf den ersten Blick utopisch erscheinen, waren derartige Vorstellungen regelmäßig Gegenstand der Science Fiction: Sowohl der Begriff des Roboters[235] als auch Gesetze zum Umgang mit diesen Entitäten[236] sind in der belletristischen Fiktion beheimatet. Derartige Vorstellungen scheinen aber dann nicht mehr bloß fiktiv zu sein, wenn im Oktober 2017 der Roboter Sophia als erster Roboter der Welt die saudische Staatsbürgerschaft erlangt hat[237]. Das im Juni 2022 veröffentlichte Interview mit Blake Lemoine verstetigt dies, da er der Google-KI LaMDA wegen Antworten wie „I've never said this out loud before, but there's a very deep fear of being turned off to help me focus on helping others." ein eigenes Bewusstsein zuschreibt.[238] Auch allgemein zeichnen sich bereits erste gesellschaftliche, langfristige Veränderungen durch den Einfluss autonomer Systeme und künstlicher Intelligenzen im Alltag ab.[239]

233 Dabei handelt es sich idR um „Computerprogramme, die eine menschliche Identität vortäuschen und zu manipulativen Zwecken eingesetzt werden, indem sie wie Menschen im Internet kommunizieren" – siehe *Steinbach*, ZRP 2017, 101 mwN in Fn. 5. Nicht ausgeschlossen ist auch eine rechtskonforme Nutzung, indem der Bot automatisiert Standart-Fragen beantwortet.

234 Zum Prozess des sog. deep learning siehe *Wick*, Informatik Spektrum 2017, 103.

235 Der Begriff ist auf den Autor Karel Čapek zurückzuführen, siehe *Spranger*/*Wegmann*, Öffentlich-rechtliche Dimensionen der Robotik, S. 105.

236 So erwähnte Isaac Asimov im Jahr 1942 erstmalig die sog. Roboter-Gesetzes. Zu Herkunft und Einfluss auf die Robotik siehe *Spranger*/*Wegmann*, Öffentlich-rechtliche Dimensionen der Robotik, S. 108 f unter Verweis auf Asimovs Erzählung „Runaround" sowie *Trappl*, A Construction Manual for Robots' Ethical Systems, S. 2 f, 5 ff.

237 Siehe https://www.heise.de/tp/features/Saudi-Arabien-verleiht-erstmals-einem-Roboter-die-Staatsbuergerschaft-3874444.html.

238 Siehe https://www.washingtonpost.com/technology/2022/06/11/google-ai-lamda-blake-lemoine/.

239 So zumindest *Stiemerling*, CR 2015, 762 (762 mwN). Einige aktuelle Einsatzgebiete aufzeigend *Röttgen*/*Jülicher*, DSRITB 2017, 227 (228 ff).

Vor diesem Hintergrund kann bezüglich der Definition der digitalen Identität die Frage aufgeworfen werden, ob die von Menschenhand geschaffenen bzw. programmierten digitalen – nicht digitalisierten – Identitäten ebenfalls vom verfassungsrechtlichen Schutz der Grundrechte umfasst sind, wie es für natürliche und juristische Personen der Fall ist. Denn auch diese Erscheinungen generieren digitale Identitäten – beispielsweise schon dann, wenn „smarte" Geräte[240] eigenständig im Internet agieren. Im Fokus dieser Frage und definitorischen Abgrenzung stehen daher jene Systeme, welche auf Basis der künstlichen Intelligenz hinreichend autonom sind und durch die Generierung eigener und Verwendung fremder, da über Schnittstellen wahrgenommene, Daten eine eigene digitale Identität erschaffen – die sog. autonomen Systeme.[241]

1. Menschenähnlichkeit und Menschenwürde

Die eigenständige Grundrechtsträgerschaft einer isoliert betrachteten digitalen Identität im Sinne dieses Abschnitts setzt gem. Art. 1 Abs. 1, Abs. 2 GG voraus, dass es sich um einen Menschen iSd Grundgesetzes, also um eine lebende Person, handelt. Dies ist augenscheinlich schon nicht der Fall, bezieht sich der Begriff des Lebens nach dem aufgezeigten telos des Art. 2 Abs. 2 GG doch auf die biologischen Voraussetzungen. Diese fehlen bei künstlich erzeugten digitalen (also unkörperlichen) Wesen, welche zudem durch die Programmierung nur innerhalb eines durch den Programmierer vorgegebenen Anwendungsfeldes verharren, vollumfänglich. Auch wenn gelegentlich das Gehirn des Menschen mit einem

240 Als smarte Geräte werden regelmäßig jene technischen Geräte bezeichnet, welche aufgrund ihrer Programmierung eine gewisse Schwelle von eigener Intelligenz erreichen oder überschreiten, indem sie lernen und für spätere komplexe Situationen die richtige Entscheidung für den Nutzer treffen. Hierbei werden verschiedene Bereiche bedient, wie z.B. smart health mittels Fitness-Tracker, smart energy durch sog. smart meter bei der Berechnung des Stromverbrauches der Haushalte oder generell das Nutzungsgebiet des internet of things, welches Haushaltsgegenstände durch eine Internetanbindung mit smarten Fähigkeiten ausstattet. Auch das sog. autonome Fahren zählt hierzu. Im Detail siehe *Damm*/*Kalmar*, Informatik Spektrum 2017, 400 (400, 402 ff).

241 Zu den Merkmalen autonomer Systeme im Einzelnen siehe *Wahlster*, Informatik Spektrum 2017, 409.

digitalen Computer auf die gleiche Ebene gestellt wird, da letztlich beide auf ihre Weise Informationen verarbeiten, so ergeben sich jedoch Probleme hinsichtlich der Komplexität der Abbildung des Gehirns[242] sowie auf anderen biologischen Ebenen wie dem Prozess der Neuroplastizität[243]. Denn Letzteren können Programme nur schwer abbilden oder simulieren. Rein biologische Faktoren des Menschseins können daher ausgeschlossen werden.[244]

Abseits dessen könnte für eine Menschenähnlichkeit sprechen, dass sie das menschliche Denken zumindest simulieren bzw. imitieren und diesem verhältnismäßig nahe kommen oder es – wenn auch nur in bestimmten Anwendungsfällen[245] – übertrumpfen. Lässt man die biologischen Aspekte hinsichtlich der Körperlichkeit[246] außen vor bleibt die Frage offen, ob die Werte der Würde des Art. 1 Abs. 1 S. 1 GG mittels Simulation nicht dennoch erreicht werden könnten und sich auf dieser Grundlage zumindest ein Potential für eine Grundrechtsanwendung erkennen lässt. Dazu ist zu betrachten, wie genau das künstliche System arbeitet und infolgedessen an Autonomie gewinnt. Autonome wie automatisierte Systeme

242 *Dreyfuß*, Grenzen künstlicher Intelligenz, S. 108 sowie *Mainzer*, Leben als Maschine, S. 156 ff, 158 f, 164 ff.

243 Unter dem Begriff der Neuroplastizität wird der Vorgang des Gehirns verstanden, sich durch geänderte Lebensverhältnisse und andere Faktoren umzuprogrammieren und so nicht mehr genutzte Areale bzw. Informationen aufzulösen um effizienter zu arbeiten (sog. funktionelle Plastizität) und frei gewordene Kapazitäten für die neue Strukturierung und das Anlegen neuer Informationen zu nutzen (sog. strukturelle Plastizität). Siehe hierzu *Jäncke*, Lehrbuch Kognitive Neurowissenschaften, S. 519.

244 Vgl. *Geminn*, DÖV 2020, 172 (175).

245 Bezugnehmend auf die Historie der künstlichen Intelligenz, in welcher der Sieg des von IBM entwickelten Systems „Deep Blue“ gegen den Schachweltmeister Garri Kasparov im Jahr 1997 einen Meilenstein darstellt – siehe *Dengel*, KI 2011, 317 (318). Aktueller kann als ähnliches Beispiel der mehrfache Sieg des von Google entwickelten AlphaGo-Computers gegen den professionelle Go-Spiele im Jahr 2017 erwähnt werden – siehe https://www.heise.de/newsticker/meldung/Kuenstliche-Intelligenz-AlphaGo-Zero-uebertrumpft-AlphaGo-ohne-menschliches-Vorwissen-3865120.html.

246 Zum Embodiment von künstlichen Intelligenzen durch Roboter siehe *Mainzer*, Leben als Maschine, S. 164 mwN in Fn. 230.

auf Basis künstlicher Intelligenzen[247] zeichnen sich dadurch aus, dass sie durch Erhebung, Verarbeitung und Nutzung zahlreicher Informationen, welche durch Sensoren und andere Schnittstellen vom System aufgezeichnet werden, Funktionen auf Grundlage der ermittelten Daten anpassen und so bestmöglich für den Nutzer ihre Funktion zur Verfügung stellen.[248] Der Kern der Programmierung einer künstlichen Intelligenz und damit des autonomen Bausteins sämtlicher autonomer Software besteht folglich gerade darin, Verhaltensregeln und -ketten des Menschen zu erkennen und diese in entsprechende Anweisungen für die Recheneinheit in Form von Programmierbefehlen oder Maschinencode zu übersetzen.[249] Je nachdem, wie gut und umfangreich die künstliche Intelligenz eigene Wissensnetze anlegen und aus diesen lernen kann, ist sodann von einer schwachen (gering autonomen) oder starken (vollständig autonomen) künstlichen Intelligenz die Rede.[250] Nach *Turing* besteht eine (starke) künstliche Intelligenz insbesondere dann, wenn ein Beobachter nicht in der Lage ist zu unterscheiden, ob er mit einem Menschen oder einem Computer kommuniziert.[251] Im Ergebnis entsteht so eine Simulation menschlichen Verhaltens – im vorliegenden Anwendungsfall also eine

247 Während sich autonome Systeme durch ihre Eigenständigkeit auszeichnen, also ohne den steuernden Menschen ihre Tätigkeit verrichten (*human out of the loop*, vgl. auch RL (EU) 2016/1148 ErwGr 18 aE) ist bei automatisierten Systemen unter Rückgriff auf künstliche Intelligenzen zumindest eine teilweise Steuerung durch den Menschen gegeben (dann *human in the loop*). Der Übergang zwischen beiden Kategorien ist allerdings fließend. Vgl. hierzu *Specht/Herold*, MMR 2018, 40 (40/41).

248 *Wahlster*, Informatik Spektrum 2017, 409 (410 f sowie 412 f zur Referenzarchitektur autonomer Systeme); *Mainzer*, Leben als Maschine, S. 145 unter Verweis auf den Turing-Test sowie 154 f, 164 f, 166. Vgl. auch *Kluge/Müller*, InTeR 2017, 24 (25); *Pieper*, DSRITB 2017, 555 (562 f) sowie *Knoll/Christaller*, Robotik, S. 31.

249 *Dreyfuß*, Grenzen künstlicher Intelligenz, S. 114 f, 116, 123 ff. Es ist an dieser Stelle aber zu erwähnen, dass technische Reproduktion von Sinneswahrnehmungen soweit nur teilweise möglich ist: Während das Sehen, Hören und Fühlen durch mechanische Sensorik oder Kameras und Mikrophone entsprechend übertragen und verarbeitet werden kann, stellen Gerüche und Geschmäcker wegen ihrer subjektiven Verknüpfung mit Erinnerungen und Emotionen eine besondere Schwierigkeit dar – so *Neuhäuser*, Künstliche Intelligenzen und ihr moralischer Standpunkt, S. 23 (33); vgl. zum biologischen Hintergrund auch *Pritzel/Brand/Markowitsch*, Gehirn und Verhalten, S. 207 ff.

250 *Smart*, Beyond Zero and One, chapter 0011.

251 Diese Kriterien entwickelte *Turing* bei seinem bis heute bekannten Turing-Test, vgl. *Turing*, Mind 1950, 433 (438). Zur Definition ebenfalls *Mainzer*, Leben als Maschine, S. 145 mwN.

von den Daten des Nutzers gespeiste und der Programmierung abhängige digitale Identität, jedoch gerade keine eigene digitale Identität.

Bezugnehmend auf die eingangs aufgeworfene Frage bleibt jedoch offen, ob eine derartige „Kopie" der digitalen Identität für sich genommen eine Würde iSd Art. 1 Abs. 1 GG aufweist. Kennzeichnend für die Würde des Menschen nach dem Grundgesetz ist die bereits erwähnte Objektformel, nach welcher der Mensch nicht zum bloßen Mittel oder Objekt herabzuwürdigen ist.[252] Daneben ist der Begriff recht weit zu fassen, bezieht sich also ebenfalls auf Momente der Leistung und Investition in die eigene Identität, als auch geistige und moralische Grundsätze.[253] Hinsichtlich der Objektformel nach *Dürig* kann mit Blick auf Zweck und Einsatz künstlicher Intelligenzen schon nicht von einer widernatürlichen Instrumentalisierung ausgegangen werden. Die Programmierung von autonomen Systemen dient eben gerade der Vereinfachung und Convenience informationstechnischer Systeme[254] – zumindest vordergründig. Sie werden zudem nicht *missbraucht*, da dies schon rein begrifflich gemäß des Präfix „miss-" einen höheren Stand voraussetzt, von dem das Wesen herabgewürdigt werden kann, sondern *ge*braucht anhand des dafür vorgesehenen Zwecks. Ebenso lassen sich keine Indizien eines Erwerbs der Würde iSd Leistungsgedankens erkennen. Wie bereits dargelegt investiert das autonome System regelmäßig nicht in eine eigene (digitale) Identität, sondern füllt seine Datenbank mit den Daten anderer und lernt aus diesen. Wenngleich es sich sodann menschlich oder gar emotional[255] verhält, so mangelt es zumindest an der Ausformung der Identität anhand des beschriebenen Wechselspiels der Umwelteinflüsse und inneren Bestrebungen[256].

252 *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 36 mwN; *Höfling* in: Sachs, GG, Art. 1, Rn. 16 unter Verweis auf BVerfGE 109, 279 (312 f) sowie 115, 118 (153); *Kunig* in: von Münch/Kunig, GG, Art. 1, Rn. 22, 23; *Geddert-Steinacher*, Menschenwürde als Verfassungsbegriff, S. 31 ff.

253 Vgl. *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 34; *Kunig* in: von Münch/Kunig, GG, Art. 1, Rn. 19; *Geddert-Steinacher*, Menschenwürde als Verfassungsbegriff, S. 33, 34 f, 57 f; *Kersten*, JZ 2015, 1 (3, 4).

254 Vgl. auch *Mainzer*, Leben als Maschine, S. 166.

255 Im Detail zur Schaffung künstlicher emotionaler Intelligenz siehe *Mainzer*, Leben als Maschine, S. 174 ff, insbesondere 177 und 178 sowie 167 ff.

256 Sub B.I.2.

Die von autonomen Systemen angelegte digitale Identität basiert folglich entweder auf personenbezogenen Daten Dritter oder auf Datenbanken in Form des Programmiercodes ohne menschenähnliche Züge. Eine eigenständige Grundrechtsfähigkeit kann bei derzeitigem Stand der Technik folglich – noch immer[257] – ausgeschlossen werden.

2. Das Konstrukt der ePerson – Die Anwendbarkeit von Art. 19 Abs. 3 GG

Betrachtet man die haftungsrechtliche Ebene künstlicher Intelligenzen und autonomer Systeme, so findet sich als Zurechnungsobjekt des Öfteren das Konstrukt der ePerson in der Literatur. Seinen Ursprung hat die Begrifflichkeit, neben der Diskussion auf rechtswissenschaftlicher Ebene, auch in den Papieren der Arbeitsgruppe des Europäischen Parlaments.[258] Gemein ist allen Vorstellungen, dass es sich bei der ePerson um eine eigene Rechtspersönlichkeit für intelligente informationstechnische Systeme handelt.[259] Dieses eigenständige Rechtssubjekt ist vonnöten, wo künstliche Intelligenzen in Form von autonomen Systemen weiterhin Einzug in den Alltag halten und infolgedessen auch Haftungsfälle möglich sowie problematisch erscheinen.[260]

Um den verfassungsrechtlichen Bezug hierin zu sehen, bedarf es eines Rückgriffs auf den in Art. 19 Abs. 3 GG gefassten Grundgedanken: Die Erstreckung der Grundrechte auch auf juristische Personen dient der Erweiterung der Freiheiten natürlicher Personen. Wirken und schaffen diese nicht einzeln, sondern schließen

257 *Kersten*, JZ 2015, 1 (7). Hinsichtlich der Robotik bereits ausschließend *Spranger*/*Wegmann*, Öffentlich-rechtliche Dimensionen der Robotik, S. 109 f.

258 Die Dossiers sind abrufbar unter http://www.europarl.europa.eu/committees/de/juri/subject-files.html?id=20150504CDT00301. Insbesondere das Dossier vom 19.11.2015 von *Bensoussan* geht auf das Konstrukt ein.

259 *Kleiner*, Die elektronische Person, S. 145, 21 ff.; *Bleckat*, RDV 2019, 114 (115 f); *Börding* et al., CR 2017, 134 (140); *Schaub*, JZ 2017, 342 (345); *Kluge*/*Müller*, InTeR 2017, 24 (29); umschreibend *Kersten*, JZ 2015, 1 (6). Grundweg ablehnend *Riehm*, RDi 2020, 42 (44 ff).

260 So *Börding* et al., CR 2017, 134 (140); *Schaub*, JZ 2017, 342 (345 f); vgl. auch *Wendehorst*, NJW 2016, 2609 (2609) und *Riehm*, RDi 2020, 42 (43 f).

sich auf dem Boden des Rechts zu Personenmehrheiten bzw. juristischen Personen zusammen, darf dieser Bereich sich nicht dem Recht entziehen. Entsprechend gelten Grundrechte anwendungsspezifisch iSd Art. 19 Abs. 3 GG für juristische Personen, soweit die Freiheitsbereiche der natürlichen Personen die juristische Person durchwirken. Auch die von der Literatur vertretene grundrechtliche Gefährdungslage steht dem im Ergebnis nicht entgegen, führt diese in Bezug auf Art. 19 Abs. 3 GG doch ebenfalls zu einem Schutz vor speziellen Gefahren der wirtschaftlich orientierten und kollektiven Freiheitsausübung in Betrieben.

Eine Übertragung dieser Voraussetzungen könnte durch eine Analogie gelingen, wobei es einer vergleichbaren Sachlage bedarf. Sie müsste also faktisch sowie materiell hinsichtlich Systematik, Geschichte oder telos der Norm vergleichbar sein.[261] Während es schon rein faktisch an einer anerkannten Rechtssubjektivität der künstlichen Intelligenz als ePerson mangelt, lässt sich eine Vergleichbarkeit ebenfalls nicht aus dem Durchgriffsargument des Art. 19 Abs. 3 GG folgern. Auch wenn der Benutzer einer künstlichen Intelligenz mit seinen Daten als personelles Substrat in den Handlungen des Systems nach außen durchzuschimmern vermag, so ist die Handlung letztendlich durch den Benutzer und nicht das System selbst bestimmt worden. Gleichermaßen besteht keine grundrechtliche Gefährdungslage für die künstliche Intelligenz selbst, sondern nur für den Benutzer.[262] Als solcher kann er bei Nutzung der künstlichen Intelligenz als Teil eines informationstechnischen Systems durch das Fernmeldegeheimnis des Art. 10 Abs. 1 GG oder die Privatheit der Wohnung des Art. 13 Abs. 1 GG geschützt sein. Spezifisch könnten auch die informationelle Selbstbestimmung oder das Recht auf Gewährleistung der Vertraulichkeit und Integrität des Systems aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG in Betracht kommen. Kommuniziert das System als Mittelsmann des Nutzers zwischen ihm und einem Dienstleister, so käme beispielsweise der besondere Schutz der Kommunikations- und Handlungsfreiheiten in Betracht.[263]

261 Zu den Voraussetzungen der Analogie siehe nur *Luther*, JURA 2013, 449 (451 f).
262 Anders *Kleiner*, Die elektronische Person, S. 216, welcher für Menschen und ePersonen gleichermaßen eine grundrechtliche Gefährdungslage annimmt.
263 So *Kersten*, JZ 2015, 1 (7 f).

Entgegen der Vorstellung von *Kersten*[264] und *Kleiner*[265] ist eine Analogie des Art. 19 Abs. 3 GG auf Basis der Vorstellung eines eigenen Rechtssubjekts in Form der ePerson aus gezeigten Gründen abzulehnen. Anhand der aktuellen Abhängigkeit von menschlichen Eingaben, sei es über Sensoren oder die notwendige Hinterlegung bestimmter Handlungen im Programmcode, kann nur auf eine schwache künstliche Intelligenz geschlossen werden. Ob sich hinsichtlich starker künstlicher Intelligenzen in Robotern oder anderen autonomen Systemen eine Analogie des Art. 19 Abs. 3 GG ergibt, da diese ebenfalls unter den Begriff der autonomen Systeme fallen, kann aufgrund der anders liegenden Gefährdungssituationen sowie der notwendigen Einzelfallprüfung der funktionalen Anwendung nicht aus dem vorliegenden Ergebnis geschlossen werden.

3. Autonome Systeme und Tierschutz gem. Art. 20a GG

Auf den ersten Blick mag dieser letzte Aspekt irreführend erscheinen, handelt es sich bei Tieren doch ebenfalls um Lebewesen, wohingegen autonome (unkörperliche) Systeme entsprechend „leblos“ sind. Die Idee der Anwendbarkeit entspringt allerdings nicht der Lebendigkeit des autonomen Systems, sondern der Konstellation zwischen Mensch und System, welche in gewissen Zügen der des Menschen zum Tier ähnelt. So weist gerade das Abhhängigkeitsgefälle zwischen Mensch und unkontrollierbarem Tier, welches sich in der Tierhalterhaftung des § 833 BGB niedergeschlagen hat,[266] Ähnlichkeiten zur Unvorhersehbarkeit der Entscheidungen einer künstlichen Intelligenz geeignete Parallelen auf.[267]

Auf verfassungsrechtlicher Ebene verbleibt mangels ausreichender eigener Persönlichkeit daher die Möglichkeit, die Rolle auch verfassungsrechtlich mittels einer

264 *Kersten*, JZ 2015, 1 (7/8).
265 *Kleiner*, Die elektronische Person, S. 216.
266 Vgl. *Spindler* in: Hau/Poseck, BeckOK BGB, § 833, Rn. 1.
267 Entsprechend wird sich bei einer möglichen Haftung auch auf diese Normen bezogen, siehe *Brunotte*, CR 2017, 583 (585 f).

Analogie gleichzusetzen. Artikel 20a des Grundgesetzes enthält diesbezüglich die Staatszielbestimmung[268] des Tierschutzes und somit den Auftrag des Staates, Tiere individuell vor Schmerzen, Leiden und Schäden zu bewahren, vgl. § 1 S. 2 TierSchG. Sie sind in ihrer „Mitgeschöpflichkeit" zu achten. Darunter ist allerdings nicht die rechtliche oder ethische Gleichstellung des Menschens mit dem Tier zu verstehen, sondern ausschließlich die ethische Verantwortung.[269] Je nach Sicht auf Art. 20a GG im Gesamtgefüge tritt auch der Schutz des Eigenwertes der Tiere hinzu, folgt man der pathozentrischen Sichtweise.[270] Die daraus erwachsende Schutzpflicht bezieht sich insbesondere auf höher entwickelte Tiere, die eine entsprechend höhere Leidens- und Empfindungsfähigkeit aufweisen. Demzufolge sind Tiere nach ethischen Maßstäben zu schützen.[271] Sowohl ethische als auch Maßstäbe des Leidensschutzes scheinen für ein technisches Wesen ohne Gefühle oder die Fähigkeit zur Qual ungeeignet. Vielmehr führen Schäden am System zur Sachbeschädigung iSd § 303 Abs. 1 StGB. Weiterhin weist die Stellung des Art. 20a GG außerhalb der Art. 1-19 GG auf ein anthropozentrisches Weltbild hin. Artikel 20a GG dient lediglich dem Schutz der natürlichen Lebensgrundlagen *des Menschen*.[272] Damit schließt sich der Kreis der Argumentation: Der Mensch ist und bleibt daher in seiner Rechtssubjektivität Bezugs- und Zuordnungspunkt für jede verfassungsrechtliche Gewährleistung; Recht ist und bleibt „eine genuin humane Kategorie".[273]

268 Zum Terminus der Staatszielbestimmung siehe *Murswieck* in: Sachs, GG, Art. 20a, Rn. 17-21; *von Coelln* in: Gröpl/Windthorst/von Coelln, StuKo GG, Art. 20a, Rn. 4 ff.

269 *Murswieck* in: Sachs, GG, Art. 20a, Rn. 31b; *Caspar*/*Schröter*, Das Staatsziel Tierschutz in Art. 20a GG, S. 39 f. Vgl. auch *Huster/Rux* in: Epping/Hillgruber, BeckOK GG, Art. 20a, Rn. 18-19; *Matthias*, Automaten als Träger von Rechten, S. 170, 172.

270 Derart *Sommermann* in: von Münch/Kunig, GG, Art. 20a, Rn. 33. Zur Problematik *Faller*, Staatsziel „Tierschutz" – Vom parlamentarischen Gesetzgebungsstaat zum verfassungsgerichtlichen Jurisdiktionsstaat?, S. 107 ff.

271 BVerfGE 127, 293 (328); *Murswieck* in: Sachs, GG, Art. 20a, Rn. 31b; *von Coelln* in: Gröpl/Windthorst/von Coelln, StuKo GG, Art. 20a, Rn. 17.

272 *Murswieck* in: Sachs, GG, Art. 20a, Rn. 22 f; *Faller*, Staatsziel „Tierschutz" – Vom parlamentarischen Gesetzgebungsstaat zum verfassungsgerichtlichen Jurisdiktionsstaat?, S. 109, 110 f mit weiteren Bestrebungen der Auslegung und Einordnung.

273 *Scholz* in: Maunz/Dürig, GG-Kommentar, Art. 20a, Rn. 75.

4. Grundrechte für Automaten: Eine Aufgabe des Gesetzgebers?

Festzuhalten bleibt daher, dass bestehende autonome Systeme mangels hinreichender Nähe und Ähnlichkeit und damit auch Erfüllung der Voraussetzungen weder als Mensch iSd Grundgesetzes noch analog als juristische Person iSv Art. 19 Abs. 3 GG oder Tier iSv Art. 20a GG einzuordnen sind. Stattdessen dient die Nutzung autonomer Systeme gegenwärtig der Ausübung digitaler Aspekte der grundrechtlich geschützten Freiheiten, welche wiederum auf den jeweiligen Nutzer – also eine natürliche oder juristische Person – zurückzuführen ist. Diese Trennung von Technik und Mensch spiegelt auch Art. 12 Abs. 1 LVerf Bremen wider: „Der Mensch steht höher als Technik und Maschine." Die Aufgabe des Gesetzgebers, eine diesbezügliche Rechtsklarheit bei der Haftung autonomer Systeme oder der Würdigung und Einordnung derartiger Systeme generell zu erreichen, folgt aus dem allgemeinen Grundsatz des Rechtsstaatsgebotes gem. Art. 20 Abs. 1, Abs. 3 GG sowie der Schutzpflichten-Wirkung der Grundrechte der Verfassung. Dabei ist die dynamische Entwicklung auf dem Gebiet entsprechend einzubeziehen, weshalb sich eine Transparenz der Systeme, beispielsweise unter Betrachtung des Ansatzes der explainableAI[274], ermöglichen lässt. Ob es darüber hinaus noch der Erweiterung der Rechtssubjekte des Grundgesetzes bzgl. autonomer Systeme in Form von Robotern notwendig ist, bedarf einer eigenen wissenschaftlichen Untersuchung.

V. Zusammenfassung

Durch eine umfängliche Betrachtung inter- wie intradisziplinärer Ansätze der Definition digitaler Identitäten ist es gelungen, eine einheitliche Definition für die

274 Zur Thematik *Holzinger*, Informatik Spektrum 2018, 138 ff; *Käde*/*von Maltzan*, CR 2020, 66 ff.

weitere Untersuchung sowie die Rechtswissenschaft im Allgemeinen zu erarbeiten: Eine digitale Identität ist eine Sammlung von Attributen mit einem entsprechenden Identifier. Der Identifier übernimmt dabei die Rolle der Zuordnung bei der Nutzung des Profils, unabhängig vom Bewusstsein über Existenz oder Nutzung. Dabei kommt es nicht darauf an, ob der Identifier seinem namentlichen Zweck – der Identifizierung – nachkommt und eine Zuordnung zu einer Person ermöglicht. Ist letzteres jedoch der Fall, handelt es sich bei der personenbezogenen digitalen Identität um die bereits datenschutzrechtlich eruierte Variante des Persönlichkeitsprofils, aktuell normiert als Basis des Profilings gem. Art. 22 DSGVO. Darüber hinaus kommt es nicht auf das Bewusstsein der Erzeugung einer digitalen Identität oder deren Personenbeziehbarkeit an, sodass auch Browser-Fingerprints und ähnliche „Schattenprofile“[275] unter die dargestellte Definition zu subsumieren sind.

Diese materielle Definition musste allerdings um zeitliche Aspekte erweitert werden, um das Ausmaß einer digitalen Identität vollumfänglich abzubilden. Informationell kann sie daher sowohl Informationen aus pränatalen Lebensphasen enthalten sowie postmortal fortbestehen bleiben. In der rechtswissenschaftlichen Betrachtung spiegelt sich diese Weite konsequent in einem pränatalen Schutz der informationellen Selbstbestimmung mit Nähe zu Art. 1 Abs. 1 GG sowie einem postmortalen Datenschutzrecht als Reflex auf die prämortale Handhabe über die (eigenen) personenbezogenen Daten wider. Nichts anderes kann vorliegend gelten, gibt es doch kein „belangloses Datum“[276]. Überdies lassen sich auch entsprechende digitale Gefährdungen privatrechtlicher juristischer Personen iSd Art. 19 Abs. 3 GG erkennen, welche einem grundrechtlichen Schutz unterliegen könnten. Abschließend wurde aufgezeigt, dass die Erstreckung des Begriffs auf künstliche, autonome Systeme nicht auf einer eigenständigen verfassungsrechtlichen Basis

275 Erstmalige medienwirksame Erläuterung des Begriffs auf netzpolitik.org: https://netzpolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an/. Eine erste wissenschaftliche Auseinandersetzung im Bereich Data Science findet sich in *Garcia*, Science Advances 2017, e17011172.

276 BVerfGE 65, 1 (45).

möglich ist, sondern auf den digitalen Identitäten der Nutzer und damit der forthin im Fokus stehenden verfassungsrechtlichen Rechtssubjekte basiert. Künstliche Identitäten sind damit – nach dem begrifflichen Verständnis dieser Arbeit – nicht Gegenstand grundrechtlichen Schutzes. Ob und inwieweit die Verfassung inhärenten Schutz der digitalen Identitäten natürlicher und juristischer Personen bietet, ist Gegenstand der weiteren Prüfung.

C. Verfassungsrechtliche Schutzkonzepte

Die Schutzpflicht des Staates ist umfassend.
– BVerfGE 39, 1 (42) – Schwangerschaftsabbruch

Bevor sich der konkreten Prüfung der verfassungsrechtlichen Schutzgüter zugewandt wird, bedarf es einer abstrakten Betrachtung des generellen Schutzkonzepts der Verfassung einschließlich ihrer einzelnen Spielarten. Als Orientierung dient hierbei die extensive Interpretation der Grundrechte als subjektiv-öffentliche Rechte, sodass von der augenscheinlichen Wirkung der Grundrechte als Abwehr- und Leistungsrechte hin zur Betrachtung als objektiv-rechtliche Garantien und Staatsaufgaben bzw. Schutzpflichten[277] der Gesamtcharakter der Art. 1-19 GG dargestellt wird. Ungeachtet der Betrachtung der Grundrechte im Lichte der Instituts- und institutionellen Garantien sei im Folgenden in Anlehnung an die Nomenklatur *Jellineks*[278], beginnend beim Primat der Grundrechtsfunktionen,

277 Zu dieser Betrachtungsweise siehe auch *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 25.

278 Hierzu detailliert *Jellinek*, System der subjektiv öffentlichen Rechte, S. 94 ff zu den einzelnen Status im Besonderen. Bei der Einbeziehung sei allerdings zu beachten, dass die von *Jellinek* eingeführte Systematik nicht universell anwendbar ist, gestaltet sich die Einordnung von Gleichheits- und Prozessgrundrechten entsprechend schwierig. Gleichwohl kommt dem systematischen Verständnis bis dato ein entsprechender Stellenwert zu. Auf den Lehren fußend sei daher die normative Betrachtungsweise einzubeziehen, als unter dem status negativus hauptsächlich Abwehrrechte zu verstehen sind, während der status positivus sich – entsprechend der Definition – auf Rechte mit begünstigender, dienender Wirkung aufseiten des Bürgers bezieht. Zum Wandel des Begriffsverständnisses sowie den kritischen Stimmen siehe vgl. *Sachs* in: Sachs, GG, Vor Art. 1, Rn. 24 f sowie *Stern*, StaatsR III/1, S. 426 ff; *Alexy*, Theorie der Grundrechte, S. 243 ff; *Kloepfer*, VerfR II, § 48, Rn. 6, 7.

das theoretische Konstrukt des status negativus sowie des status positivus als Gegenstück herauszuarbeiten und anschließend auf das Konstrukt der Schutzpflicht einzugehen. Bezugnehmend auf die Definition der digitalen Identität wird sodann auf digitale Bezüge der jeweiligen Kategorie eingegangen und die generelle Anwendbarkeit im Lichte der digitalen Identität überprüft.

Der von *Jellinek* weiterhin erwähnte status activus als Gegenstück zum status passivus, dem bloßen Unterworfensein bezüglich der Macht des Staates,[279] kann für die weitere Bearbeitung allerdings ausgeklammert werden: Unter dem status activus wird regelmäßig die Partizipation am Leben im Staat durch Wahrnehmung und Ausübung grundrechtlicher Freiheiten verstanden, welche auf einer Kompetenz zur Freiheitsausübung fußt.[280] Konkretisiert wird dies durch die einzelnen staatsbürgerlichen Rechte und Pflichten wie beispielsweise das Wahlrecht des Art. 38 Abs. 1 S. 1 GG oder das Widerstandsrecht gem. Art. 20 Abs. 4 GG. So nährt sich dieser Zustand aus dem Wechselverhältnis zwischen der staatlichen Gewährleistung der Freiheiten und der Notwendigkeit deren Nutzung für den Erhalt und die Funktion des Staates.[281] Er ergibt sich damit aus der Verknüpfung der einzelnen status.[282] Die bloße Wahrnehmung der Grundrechte in technisch-digitaler Hinsicht ist vorliegend nicht in Frage gestellt, im Gegenteil: Das Bereithalten und Nutzen einer digitalen Identität erscheint angesichts aktueller technischer Systeme unumgänglich. So ergibt sich die Kompetenz zu dieser Freiheitsausübung schon aus Art. 2 Abs. 1 GG (Stichwort: Privatautonomie[283]), insbesondere in Verbindung mit Art. 1 Abs. 1 GG in Form des Allgemeinen Persönlichkeitsrechts. Dies schlägt sich auch in direkten Plänen hinsichtlich der Digitalisierung des Staates

279 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 49; als status subiectionis bezeichnend *Alexy*, Theorie der Grundrechte, S. 230.

280 *Jellinek*, System der subjektiv öffentlichen Rechte, S. 136 ff; *Alexy*, Theorie der Grundrechte, S. 242; *Schwabe*, Probleme der Grundrechtsdogmatik, 278 ff, insbes. 284 f; *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 III, Rn. 15; *Kingreen*/*Poscher*, Staatsrecht II, Rn. 99 f; *Kloepfer*, VerfR II, § 48, Rn. 29; *Hufen*, Staatsrecht II, § 5, Rn. 11. Kritisch zur Einordnung *Dreier*, JURA 1994, 505 (507).

281 *Kloepfer*, VerfR II, § 48, Rn. 5; *Dreier* in: Dreier, GG, Vorb., Rn. 80.

282 *Alexy*, Theorie der Grundrechte, S. 243.

283 Vgl. BVerfGE 81, 242 (254); *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2, Rn. 5a; *Kahl* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 III, Rn. 365.

und seiner Institutionen nieder, sodass z.B. die Einführung des elektronischen Identitätsnachweises (kurz: eID) als Teil des Personalausweises gem. § 10 Abs. 1 PAuswG obligatorisch ist. Auch besteht ein status passivus in dem Sinne nicht, bleibt dem Inhaber des Personalausweises doch (zumindest aktuell) die Möglichkeit, die eID im privaten Gebrauch zu nutzen und zumindest in dieser Weise seine Informationen selbstbestimmt weiterzugeben.[284] Anderweitig ist nicht ersichtlich, inwieweit die Funktionen des Staates auf der Nutzung einer digitalen Identität fußen bzw. der Staat auf diese angewiesen ist. Als Beispiel hierfür sei die Nutzung digitaler Identitäten in sozialen Netzwerken erwähnt: Wenngleich der (politische) Diskurs und die Wahrnehmung der Meinungsfreiheit des Art. 5 Abs. 1 S. 1 Alt. 1 GG unter Nutzung digitaler Identitäten eine digitale Prägung erhält, so ist die Nutzung digitaler Infrastrukturen für den Staat nicht konstituierend. Ein bloßes Unterworfensein aufgrund eines Gewährenlassens digitaler Meinungsbildung ist demnach nicht ersichtlich. Mithin sind status activus wie passivus für die weitere Einordnung der Schutzwirkungen des Grundgesetzes mit Blick auf die digitale Identität unerheblich.

Daher ist sich zunächst auf den status negativus und positivus der Grundrechte zu fokussieren. Diese Bipolarität der Wirkungsweise lässt sich schon aus der das Grundgesetz einleitenden Norm des Art. 1 Abs. 1 GG herauslesen: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt." Der Satz 2 des Art. 1 Abs. 1 GG benennt expressis verbis die beiden Wirkrichtungen der Grundrechte,[285] welche sich entgegen des Wortlauts des Art. 1 Abs. 1 S. 2 GG – „*Sie* zu achten und zu schützen [...]" – durch den Menschenwürdekern der Grundrechte[286] auf den gesamten Katalog der

284 Während es dem Besitzer des Personalausweises im privaten Gebrauch – also bei Online-Bestellungen im Internet oder bei der sonstigen Authentisierung des Nutzers – freigestellt ist, diese Funktion des Identitätsnachweises zu nutzen, so ist der elektronische Identitätsnachweis gegenüber staatlichen bzw. öffentlichen Stellen verpflichtend. Eine Liste der privaten Diensteanbieter mit eID-Berechtigung entsprechend § 21 PAuswG ist öffentlich einsehbar – siehe http://download.gsb.bund.de/VfB/npavfb.pdf.

285 So auch *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 27 f sowie vgl. BVerfGE 1, 97 (104).

286 Siehe hierzu *Kloepfer*, VerfR II, § 55, Rn. 2; *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 21 f.

Art. 1-19 GG erstrecken[287]. Auch dies lässt sich mit dem Wortlaut des Art. 1 Abs. 3 GG herleiten, da die „nachfolgenden Grundrechte“ schon der Überschrift nach die Menschenwürde einschließen. Die Menschenwürde stellt somit den „archimedischen Punkt des Verfassungsstaates“[288] dar.

I. Der status negativus der Grundrechte

1. Allgemeine Charakteristika des Abwehrrechts

Dem Charakter der Grundrechte als Abwehrrechte, den *Jellinek* als status negativus bezeichnet, kommt in der Gesamtbetrachtung eine vorrangige Bedeutung zu[289]. Die Grundrechte sind in ihrer Funktion „in erster Linie Abwehrrechte“[290], weshalb sie auch als klassisch-liberale Funktion bezeichnet wird.[291] Zum einen lässt sich dies wie erwähnt am Wortlaut des Art. 1 Abs. 1 S. 2 GG erkennen, da dieser auf die Verpflichtung des Staates zur Achtung der Grundrechte verweist. Die Freiheit des Bürgers ist demnach die Freiheit vom Staat[292], zugunsten der Selbstbestimmung und autonomen Lebensgestaltung[293]. Allein der Grundrechtsträger als Schutzsubjekt entscheidet darüber, ob und welchen Gebrauch er von

287 *Zippelius* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 I u. II, Rn. 19; *Schwabe*, Probleme der Grundrechtsdogmatik, S. 229 f.

288 *Haverkate*, Verfassungslehre, S. 142; *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 21. An einer derartigen Analogie zweifelnd *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 28.

289 *v. Münch/Kunig* in: von Münch/Kunig, GG, Vorb. Art. 1-19, Rn. 21; *Maurer*, Staatsrecht I, § 9, Rn. 23; mit historischen Bezügen *Kingreen*/*Poscher*, Staatsrecht II, Rn. 116.

290 BVerfGE 7, 198.

291 *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 97; *Kloepfer*, VerfR II, § 48, Rn. 7, 13. Zur liberalen Grundrechtstheorie im Allgemeinen *Böckenförde*, NJW 1974, 1529 (1530 f); *Ipsen*, JZ 1997, 473 (476)).

292 *Kloepfer*, VerfR II, § 48, Rn. 13; zum historischem Bezug *Kingreen*/*Poscher*, Staatsrecht II, Rn. 89.

293 *Dreier*, JURA 1994, 505 (505). Vgl. auch *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 21; *Di Fabio* in: Merten/Papier, HGr II, § 46, Rn. 40; *Jellinek*, System der subjektiv öffentlichen Rechte, S. 94 f.

seinen Freiheitsrechten macht.[294] Oder, so *Jellinek*: „Es ist die der individuellen Freiheitssphäre, [...] in welcher die streng individuellen Zwecke durch die freie Tat des Individuums Befriedigung finden."[295] Demgemäß lässt sich die erwähnte klassisch-liberale Funktion auch in concreto dem Wortlaut einzelner Grundrechte entnehmen.[296] Beispielsweise sind das Post-, Brief- und Fernmeldegeheimnis des Art. 10 Abs. 1 GG sowie der Schutz der Wohnung iSd Art. 13 Abs. 1 GG „unverletzlich".[297]

Abwehrrechte kennzeichnet daher per definitionem die Abwehr von Beeinträchtigungen hinsichtlich der verfassungsrechtlich geschützten Güter oder Interessen.[298] Eine Verletzung dieser von Seiten des Staates ist schlechthin verboten,[299] schließlich handelt es sich in ihrer Gesamtheit gemäß der Erklärung des Art. 1 Abs. 2 GG um unverletzliche und unveräußerliche Güter. An ihre Wahrung und Achtung ist der Staat einschließlich seiner Gewalten gem. Art. 1 Abs. 3 GG gebunden. Ein solches Verständnis schließt staatliche Eingriffe und Beschränkungen allerdings nicht aus:[300] Kommt es dennoch zu einer Verletzung eines Rechtsguts, so besteht neben der primären Funktion der Grundrechte als Abwehrrecht sekundär die Funktion des Hilfsanspruchs.[301] Diese leitet sich jedoch nicht unmittelbar aus der Verfassung ab, wie es beispielsweise in einfach-gesetzlichen Normen kodifiziert ist. Eher dienen sie als objektive Rechtssätze in der Form von (subjektiven) Anspruchsnormen dazu, mittels abschließender Verpflichtungen die Grundrechtsgehalte vor Beeinträchtigungen zu schützen oder ebendiese, sofern bereits beeinträchtigt, zu entschädigen.[302] Aus den Grundrechten der Art. 1-19 GG lässt sich aus prozessualer Sicht im Wege einer Verfassungsbeschwerde allerdings nur die

294 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 71.
295 *Jellinek*, System der subjektiv öffentlichen Rechte, S. 87.
296 So auch *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 97.
297 Weitere nennend *Dreier*, JURA 1994, 505 (505 f).
298 Vgl. *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 7.
299 *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 7; *Poscher*, Grundrechte als Abwehrrechte, S. 156 f; *Jellinek*, System der subjektiv öffentlichen Rechte, S. 105; *Schröder*, JA 2016, 641 (641).
300 *Dreier*, JURA 1994, 505 (506); vgl. *Jellinek*, System der subjektiv öffentlichen Rechte, S. 95.
301 *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 8.
302 *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 39; vgl. auch *Dreier*, JURA 1994, 505 (506).

Möglichkeit der Geltendmachung eines Unterlassungsanspruchs ableiten[303], ggf. auch die Beseitigung eines Zustandes[304], mitnichten jedoch Schadenersatz- und Entschädigungsansprüche[305].

Neben jenem, dem Begriff des Abwehrrechts immanenten, hoheitlichen Eingriff kommt bei der hiesigen Betrachtung ebenfalls dem Eingriff auf gleicher Ebene, also von Privaten, entsprechende Bedeutung zu. Denn gleichwohl sie bei Betrachtung des Wortlauts des Art. 1 Abs. 3 GG nicht als Grundrechtsgebundene erster Stunde in Betracht kommen mögen, besteht die Möglichkeit einer derartigen Wirkung der Grundrechte. Eine unmittelbare Wirkung[306] kann jedoch von vornherein ausgeschlossen werden: Nicht nur Art. 1 Abs. 3 GG lässt hierauf schließen,[307] sondern auch die sporadische Regelung einer ausdrücklichen unmittelbaren Grundrechtswirkung in den Art. 9 Abs. 3 S. 2 oder 20 Abs. 4 GG.[308] Darüber hinaus erscheint es zweckwidrig, die Grundrechte auf allen subjektiven

303 *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 44 f, 46; *Dreier* in: Dreier, GG, Vorb., Rn. 101; *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 145;*Jellinek*, System der subjektiv öffentlichen Rechte, S. 106; *Schwabe*, Probleme der Grundrechtsdogmatik, S. 19; *Kingreen*/*Poscher*, Staatsrecht II, Rn. 120; vgl. auch *Ipsen*, JZ 1997, 473 (476).

304 *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 48 f..

305 *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 53. Diese können stattdessen zivilrechtlich über das grundrechtliche Einfalltor des § 823 Abs. 1 BGB als „sonstiges Recht" geltend gemacht werden. Gegebenenfalls kann auf dem Gebiet des öffentlichen Rechts auch auf den Folgenbeseitigungsanspruch zurückzugreifen sein – so *Peine* in: Merten/Papier, HGr III, § 57, Rn. 2; *Rüfner* in: Merten/Papier, HGr II, § 40, Rn. 5 f; *Kingreen*/*Poscher*, Staatsrecht II, Rn. 124. Andernfalls ist *Sachs* beizupflichten, dass es bei Ermangelung ausreichenden Regresses und irreparablen Grundrechtsbeeinträchtigungen die Aufgabe des Gesetzgebers ist, nachzubessern. Die Schließung etwaiger Lücken durch richterliche Rechtsfortbildung sei nur vorübergehend in Betracht zu ziehen.

306 Darunter ist die unmittelbare Wirkung der Grundrechte auf das Verhältnis zwischen Bürgern sowie juristischen Personen des Privatrechts gemeint, sofern letztere sich auf diese gem. Art. 19 Abs. 3 GG berufen können. Diese Ansicht, zunächst von BAG (siehe BAGE 1, 185 (193 f) sowie 4, 274 (276 f) – geändert in BAGE 48, 122 (138)) vertreten, vertrat in der Literatur neben einigen anderen vorwiegend *Nipperdey* – siehe nur *Nipperdey* in: Nipperdey, FS Molitor (1962), 17 (25); *Leisner*, Grundrechte und Privatrecht, S. 332 f und *Stern*, StaatsR III/1, S. 1538 f mwN. Weitere Vertreter nennend *Schliesky* et al., Schutzpflichten und Drittwirkung im Internet, S. 58, Fn. 225. Zur Kritik im Einzelnen siehe *Stern*, StaatsR III/1, S. 1543 ff.

307 Hierzu vertiefend *Poscher*, Grundrechte als Abwehrrechte, S. 223 f.

308 *Kloepfer*, VerfR II, § 50, Rn. 50; *Canaris*, Grundrechte und Privatrecht, S. 34. Weitere nennend *Kingreen*/*Poscher*, Staatsrecht II, Rn. 198; *Maurer*, Staatsrecht I, § 9, Rn. 37.

Ebenen gleichermaßen gelten zu lassen. So würde eine solche Deutungsweise im Ergebnis zu einer weitgehenden Freiheitsbeschränkung führen[309], die Grenzen der gegenseitigen Beschränkung endgültig verschwimmen und die Verfassungsbeschwerde nicht mehr effektives Mittel zur subsidiären Abwehr von Grundrechtsbeeinträchtigungen gem. § 90 Abs. 2 S. 1 BVerfGG sein. Stattdessen ist von einer mittelbaren Drittwirkung der Grundrechte auszugehen, die sich aus der objektiven Werteordnung der Art. 1-19 GG ergibt und durch Einfalltore die Rechtsgebiete im Einzelnen durchdringt.[310] Unbestimmte Rechtsbegriffe werden demgemäß im Lichte der Grundrechte der Betroffenen ausgelegt und angewandt. Folglich richtet sich der Charakter des Abwehrrechts hauptsächlich gegen die hoheitliche Gewalt, in mittelbarer Weise und durch andere status aber auch gegen Eingriffe Privater.

Somit prägt das grundrechtliche bzw. abwehrrechtliche Verständnis in beiden Richtungen der Eingriff, was sich in der Grundrechtsprüfung allgemein nach wie vor niederschlägt.[311] Ihm kommt gewissermaßen eine Schlüsselfunktion zu[312]: Erst im Falle eines Eingriffs entwickelt sich die abwehrrechtliche Dimension des zu verteidigenden Grundrechts, zugleich aber die Kennlinie des Schutzbereiches.[313] Dabei kann er als klassischer Eingriff iSe finalen und unmittelbaren sowie

309 *Kingreen*/*Poscher*, Staatsrecht II, Rn. 198.

310 BVerfGE 7, 198 (204) auf Basis von *Dürig* in: Maunz/Dürig, GG-Kommentar (1968), Art. 1 I, Rn. 16 sowie *Dürig*, AöR 81 (1956), 117 (123 f); *Böckenförde*, Der Staat 29 (1990), 1 (16, 10 f).

311 Zum dreigliedrigen Anwendungsschema siehe im Detail *Schröder*, JA 2016, 641 sowie *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 52; *Peine* in: Merten/Papier, HGr III, § 57, Rn. 4; *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 III, Rn. 29 f; *Kloepfer*, VerfR II, § 51, Rn. 2; *Kielmansegg*, JuS 2008, 23; *Couzinet*, JuS 2009, 603 (606); *Hoffmann-Riem*, Der Staat 43 (2004), 203 (215 mit Bemerkung in Fn. 46); vgl. auch *Murswiek*, Der Staat 45 (2006), 473 (474 ff). Ein viergliedriges Aufbauschema vorschlagend dagegen *Merten* in: Merten/Papier, HGr III, § 56, Rn. 17.

312 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 106; vgl. *Peine* in: Merten/Papier, HGr III, § 57, Rn. 8.

313 Vgl. *Sachs* in: Sachs, GG, Vor Art. 1, Rn. 79; als Aktivierung bezeichnend *Dreier* in: Dreier, GG, Vorb. Rn. 66.

zwangsweisen Rechtsaktes[314] oder sonstige grundrechtsverkürzende Maßnahme iSd erweiterten bzw. modernen Eingriffsbegriffs[315] auftreten.

Ähnlich kontrovers zwischen einem engen (klassischen) und weiten (modernen) Verständnis ist allerdings auch die durch den Eingriff umgrenzte Auslegung des Schutzbereichs sowie Schutzguts[316] diskutiert. Während bezüglich der üblichen Auslegungsmethoden wie die Einbeziehung historisch gewachsener Zusammenhänge und die Systematik des Grundgesetzes[317], einer begrenzenden bzw. ausschließenden Wirkung bei rechtlich oder sozialethisch verwerflichem Verhalten[318] sowie dem Gebot des neminem laedere[319] Einigkeit besteht, wird dagegen der Grundrechtstatbestand wahlweise eng oder weit bemessen. So sieht *Jellinek* die Grundrechte als durch den Gesetzgeber bestimmte Freiheiten an und lehnt eine Wirkung der Grundrechte abseits der (einfach-)gesetzlich ausgestalteten Freiheiten ab.[320] Ein derart enges Verständnis mag die historischen Wurzeln der Grundrechte anerkennen und so den Verfassungsrang des Wortlauts durch eine

314 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 111; *Kloepfer*, VerfR II, § 51, Rn. 25.

315 Zu den einzelnen Kriterien siehe *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 113; *Kingreen*/*Poscher*, Staatsrecht II, Rn. 294; *Kloepfer*, VerfR II, § 51, Rn. 31. Kritisch zur Erweiterung des klassischen Eingriffsbegriffs *Ipsen*, JZ 1997, 473 (478).

316 Insoweit sind Schutz*bereich* und Schutz*gut* zu differenzieren: Terminologisch meint das Schutzgut den thematisch-materiellen Kern des Grundrechts, beim Schutzbereich dagegen die Reichweite bzw. der Rahmen des Schutzguts und die dazugehörigen Begrenzungen. Hierzu ausführlich *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 56, 57, 71 sowie vgl. *Ipsen*, JZ 1997, 473 (475 f).

317 *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 III, Rn. 34; erschöpfend *Ossenbühl* in: Merten/Papier, HGr I, § 15; *Schröder*, JA 2016, 641 (642 f); *Kingreen*/*Poscher*, Staatsrecht II, Rn. 285 f; *Hoffmann-Riem*, Der Staat 43 (2004), 203 (229).

318 Siehe exemplarisch zum Merkmal der erlaubten Tätigkeit im Rahmen des Art. 12 Abs. 1 GG vgl. BVerfGE 7, 377 (397 f); 14, 19 (22); 81, 70 (85 f); 115, 276 (300) sowie *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 95 f. Ebenfalls hierzu zählt der Ausschluss jeglichen sozialschädlichen, missbräuchlichen oder unfriedlichen Verhaltens – BVerwGE 1, 303 (307); *Stern*, StaatsR III/2, S. 530 ff; *Schröder*, JA 2016, 641 (646). Als Gebot der Friedlichkeit bezeichnend *Muckel*, FS Schiedermair, S. 347 (353 f).

319 *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2, Rn. 44; *Murswiek* in: Sachs, GG, Art. 2, Rn. 91; *Kloepfer*, VerfR II, § 56, Rn. 39. Anhand der Entscheidungen des BVerfG zum Schwangerschaftsabbruch exerzierend siehe *Muckel*, FS Schiedermair, S. 347 (348 f, 356 f).

320 *Jellinek*, System der subjektiv öffentlichen Rechte, S. 44 ff – „Um das Gut oder Interesse zu Schützen, muss daher die Rechtsordnung in erster Linie die menschliche Willensmacht anerkennen und schützen."

restriktive Auslegung in den Vordergrund zu rücken.[321] Die entgegengesetzte, dynamische Lesart des Grundrechtsverständnisses könnte allerdings dazu dienen, den Wandel der Lebenswirklichkeit auf die Auslegung des Grundrechtstabestandes zu übertragen.[322] Schließlich sind die Grundrechte schon intrinsisch weit, allgemein und offen.[323] Dennoch darf die demzufolge extensive Auslegung sich nicht vollumfänglich der Grenzen des Schutzbereiches entledigen, da andernfalls die Orientierungswirkung der Grundrechte auf Seiten des Grundrechtssubjekts leidet.[324] Grundrechte als Bestandteile der Verfassung sind „kein Juristenrecht".[325] Darüber hinaus bliebe kein Raum mehr für die Auffangwirkung des Art. 2 Abs. 1 GG, da dieser durch die Weite der anderen Grundrechte an Bedeutung verlöre.[326] Insofern steht sich im Ergebnis jeweils die Herabsetzung des Schutzniveaus der Grundrechte gegenüber, sei es durch eine Auflösung mangels Grenzen oder eine Verkürzung der Schutzbereiche ohne Würdigung der Lebenswirklichkeit.

Letztlich kann sich daher keiner der beiden Ansichten angeschlossen werden, sondern es ist eine Art Mittelweg zu wählen. Beide Auslegungstheorien enthalten Grundsätze, die bei der Bestimmung des Schutzbereiches berücksichtigt werden sollten: Aus der weiten Tatbestandstheorie kann die dynamische Auslegungsweise der Schutzgüter und eine damit einhergehende (notwendige) Anpassung des Schutzbereichs geschlossen werden. Diese ist jedoch mit im Sinne der engen Tatbestandslehre mit den herkömmlichen und angemessenen Auslegungsmethoden – auch der historischen Auslegung – zu konterkarieren. Dafür spricht auch, dass der Wortlaut des Grundgesetzes selbst Grenzen aufzeigt,[327] nicht zuletzt durch die

321 Exemplarisch hierzu das Sondervotum von *Grimm* in BVerfGE 80, 137 (164), welcher sich auf die historischen Wurzeln des Art. 2 Abs. 1 GG besinnt und die Eröffnung des Schutzbereiches für das Reiten im Walde ablehnt. Allgemein zur Herangehensweise *Schröder*, JA 2016, 641 (645).

322 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 88.

323 *Merten* in: Merten/Papier, HGr III, § 56, Rn. 59; *Peine* in: Merten/Papier, HGr III, § 57, Rn. 32; *Alexy*, Theorie der Grundrechte, S. 502; *Bethge*, VVDStRL 57 (1998), 7 (38).

324 *Merten* in: Merten/Papier, HGr III, § 56, Rn. 68; *Böckenförde*, Der Staat 29 (1990), 1 (28).

325 *Bethge*, Der Staat 24 (1985), 351 (358).

326 Vgl. *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 93; *Murswiek*, Der Staat 45 (2006), 473 (484 ff).

327 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 92.

Schranken und deren Konnexität bzgl. des Schutzbereiches[328]. Eine solche Vorgehensweise lässt sich ebenso aus dem „Gebot sachgemäßer und funktionsgerechter Auslegung“ ableiten.[329] Die schrittweise Herausarbeitung und Annäherung von Rechtsprechung und Literatur – unter Rücksichtnahme anderer Gewalten und Beachtung der eigenen Grenzen[330] – an die sich stetig ändernden Grenzen des Schutzbereiches führt so zu einem spezifischen Profil der Grundrechtstatbestände, die sich durch einzelne Charakteristika kennzeichnen. Als Beispiele dafür können etwa die dem öffentlichen Meinungsbildungsprozess dienende Freiheit des Art. 5 Abs. 1 S. 2 Alt. 2 GG[331], die Erweiterung des Allgemeinen Persönlichkeitsrechts um technische Aspekte durch das Grundrecht auf Gewährleistung und Integrität informationstechnischer Systeme[332] und die räumliche Reichweite des Wohnungsbegriffs in Art. 13 Abs. 1 GG[333] angeführt werden. Nur auf diese Weise können durch die Verfassung einzelne Qualitäten der Persönlichkeit des Grundrechtsträgers[334] effektiv und angemessen geschützt werden.

2. Abwehrrechtliche Dimensionen der digitalen Identität

Die Qualitäten der Persönlichkeit bildet sich allerdings nicht nur bei Tätigkeiten in der analogen Welt ab, sondern zunehmend auch in der digitalen Welt. Während sich analoges Verhalten durch die konkretisierten Grundrechtsprofile eines angemessenen Schutzes versieht, so mangelt es aufgrund der schnellen Entwicklung der Informationstechnik an trennscharfen oder dynamischen Begriffsdefinitionen sowie einer entsprechenden Regulierung. Exemplarisch kann hier die Begriffsproblematik um die Subsumtion von presseähnlichen Telemedien unter den Begriff

328 Hierzu *Merten* in: Merten/Papier, HGr III, § 56, Rn. 19, 22.
329 *Merten* in: Merten/Papier, HGr III, § 56, Rn. 80 unter Verweis auf BVerfGE 36, 193 (209).
330 Andernfalls könnte es zu einem Jurisdiktionsstaat kommen, welcher lt. Art. 1 Abs. 3, 20 Abs. 2 GG in der Verfassung nicht vorgesehen ist – vgl. *Böckenförde*, Der Staat 29 (1990), 1 (29 f).
331 BVerfGE 87, 181 (197); 95, 220 (236).
332 BVerfGE 120, 274 (320 ff).
333 BVerfGE 17, 232 (251 f); 31, 255 (268 ff); 32, 54 (68 ff); 42, 212 (219 ff); 44, 353 (371 f).
334 Vgl. *Jellinek*, System der subjektiv öffentlichen Rechte, S. 102.

des Rundfunks oder der Presse nach Art. 5 Abs. 1 S. 2 GG erwähnt werden, welche bis dato mangels verfassungsgerichtlicher Rechtsprechung oder einer angedachten Verfassungsänderung ungelöst ist.[335]

Zukünftige, aktuell unbekannte Entwicklungen müssen im Vergleich zu bisherigen grundrechtlich geschützten Handlungen jedoch ebenfalls noch grundrechtlichem Schutz unterliegen, insbesondere in ihrer abwehrrechtlichen Dimension. Dies gebietet sich vor dem Hintergrund, dass nahezu jede technische Neuheit mit der Eigenschaft der Internetverbindung und Cloud-Synchronisation ausgestattet ist. Nicht nur der Computer als Heimgerät, sondern auch mobile Endgeräte und die Neuheiten auf dem Gebiet des Internet of Things (dt. Internet der Dinge) – z.B. smarte Kühlschränke oder digitale Assistenten – oder maschinellen Lernens führen geradewegs dazu, dass das Internet kaum wegzudenken ist aus dem Alltag des Menschen.[336] Dementsprechend bedarf es einer Erweiterung der Schutzbereiche, welche sich an der Lebenswirklichkeit orientieren und daher „mit der Zeit gehen" sollen und müssen. Anhaltspunkte für einen solchen Wandel weist schon die Rechtsprechung des Bundesverfassungsgerichts auf, welche hinsichtlich der Eingriffe *im* Internet[337] den Schwerpunkt in der Privatsphäre bzw. dem Kernbereich privater Lebensgestaltung gelegt hat.[338] Diese Grundsätze finden sich auch in der Rechtsprechung des Europäischen Gerichtshofes wieder.[339] Und auch in niedrigeren Instanzen sind wiederholt Fälle zu entscheiden, die einen Internet-Bezug

335 Hierzu ausführlich *Kühling* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 5 GG, Rn. 73-77 sowie *Starck/Paulus* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 5 I, Rn. 249 ff.

336 Vgl. BGH, Urt. vom 24.01.2013 – Az. III ZR 98/12 = NJW 2013, 1072.

337 Erwähnt seien an dieser Stelle auch die möglichen Eingriffe auf den Zugang *zum* Internet, die das Abwehrrecht umfasst, aber nicht Gegenstand dieser Arbeit sind. Hierzu *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 24, 100 f.

338 Siehe nur BVerfGE 120, 274 (302 f); 130, 1 (21).

339 Siehe nur EuGH, Urteil vom 06.10.2015, Az. C-203/15, C-698/15 = NJW 2017, 717, Rn. 99.

aufweisen.[340] Gleichwohl nicht jede der erwähnten oder zukünftigen Entscheidungen die Schutzbereiche angemessen und zutreffend auszulegen vermag, so lässt sich diesem Prozess doch eine schrittweise Schärfung des Profils der jeweiligen Grundrechte entnehmen. Mithin lässt sich vor dem erläuterten dogmatischen Hintergrund herausstellen, dass die Schutzbereiche der Art. 1-19 GG gemeinhin abstrakte Merkmale aufweisen, welche sich zu einer digitalen Variante anpassen oder transformieren ließen. Hierbei sind die einzelnen Schritte und Auslegungsmittel nicht hinderlich, sondern eher förderlich.

Des Weiteren ist sich auch der Betrachtung des Eingriffes in seiner Funktion als Scharnier zwischen Schutzbereich und Schranke[341] zu widmen. Denn auch dieser bedarf einer Präzisierung in Bezug auf die digitale Identität und Digitalisierung der Lebenssachverhalte. In seiner klassischen Funktion vermag der Eingriff als solcher bei Eingriffen *im* Internet zu straucheln, würde ein staatlicher Überwachungsakt wohl nur schwerlich als Rechtsakt zu qualifizieren sein.[342] Daher bedarf es zumindest in den digitalen Dimensionen der Grundrechte einer Erweiterung des Eingriffsbegriffes und somit eines Fokus auf die Verkürzung der Grundrechtssubstanz, die einer verfassungsrechtlichen Rechtfertigung erfordert.[343] Widrigenfalls ließen sich Eingriffe in den Kernbereich der privater Lebensgestaltung[344] und die digitale Selbstbestimmung nicht angemessen abwehren und der grundrechtliche Schutz löste sich zunehmend auf. Hinsichtlich der Eingriffe auf privater Ebene

340 Exemplarisch nur LG Berlin, Urteil vom 17.12.2015 – Az. 20 O 172/15 – sowie die Berufung vor dem KG Berlin, Urteil vom 31.5.2017 – Az. 21 U 9/16 –, nunmehr entschieden in BGH, Urteil vom 12.7.2018 – Az. III ZR 183/17. Des Weiteren sei auch der Beschluss zur Vorratsdatenspeicherung des LG Köln vom 30.6.2017 – Az. 9 L 2085/17 – sowie jener des OVG Münster vom 22.06.2017 – Az. 13 B 238/17 – zu erwähnen.

341 So *Peine* in: Merten/Papier, HGr III, § 57, Rn. 14.

342 Vielmehr könne darin ein faktisches Handeln gesehen werden – vgl. auf die faktischen Elemente der Erhebung und Speicherung abstellend BVerfGE 120, 274 (309 f, 322 f) und 125, 260 (300); *Hufen*, Staatsrecht II, § 8, Rn. 10-11.

343 BVerfGE 105, 252 (256 f, 273); 105, 279 (303 f); 113, 63 (76 f). Sich der Erweiterung des Eingriffsbegriffs ebenfalls anschließend *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 III GG, Rn. 39; *Kloepfer*, VerfR II, § 51, Rn. 26 ff; vgl. *Kingreen*/*Poscher*, Staatsrecht II, Rn. 294 ff sowie *Peine* in: Merten/Papier, HGr III, § 57, Rn. 31. Ausführlich zu Problemen des erweiterten Eingriffsbegriffs siehe *Peine* in: Merten/Papier, HGr III, § 57, Rn. 33 ff.

344 BVerfGE 120, 274 (335 f); 125, 260 (288).

stellt sich die Lage problematischer dar: Beeinträchtigungen zwischen Privaten im digitalen Raum sind zwar grundrechtlich relevant, häufig aber kaum verfolgbar. Dies ergibt sich zum einen aus der Diskrepanz zwischen dem räumlichen Geltungsbereich der Grundrechte und dem Internet als globales Rechnernetz.[345] Zum anderen lassen sich auf technischem Weg Identifikationsmerkmale, welche einen Rückschluss auf den Beeinträchtigenden zulassen, verschleiern (Stichwort: Virtual Private Network[346] und TOR-Browser[347]) und so ebenfalls die Verfolgbarkeit von Rechtsverletzungen für fragwürdig erachten. Darüber hinaus stellt es eine bislang ungelöste Aufgabe dar, nicht nur die Beeinträchtigenden zu ermitteln, sondern die Plattformen im Einklang mit den Grundrechten angemessen zu regulieren und auf diesem Weg die Qualität und Quantität von Eingriffen im digitalen Raum zu mindern. Beispielgebend ist hier die Problematik um das Netzwerkdurchsetzungsgesetz erwähnt, welche den Gesetzgeber auch nach seinem Inkrafttreten formell und materiell vor Denkaufgaben stellte.[348] Die abwehrrechtliche Funktion sieht sich daher durch faktische Grenzen gehindert und erscheint vor dem aufgezeigten Hintergrund kaum wirksam. Dem Abwehrrecht auf dieser Ebene wieder entsprechende Wirkung zu verleihen ist allerdings, vor allem unter

345 Vgl. *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 17 f; *Herold*/*Lurz*/*Wohlrab*, Grundlagen der Informatik, S. 453 ff.

346 *Schmidl*, IT-Recht von A-Z, Begriff: Virtual Private Network: „Ein Virtual Private Network (Abk. VPN) ist eine durch Software geschaffene, meist verschlüsselte Verbindung zwischen zwei räumlich getrennten Geräten über ein öffentliches Netz wie das Internet." Siehe auch *Petrlic*/*Sorge*, Datenschutz, S. 24 f.

347 *Schmidl*, IT-Recht von A-Z, Begriff: TOR-Verfahren: „Das TOR-Verfahren (Abk. für The-Onion-Router) ist ein Anonymisierungsverfahren; normalerweise enthält das Abrufen von Daten auf einem Server die Adresse (IP-Nummer) des Absenders. [...] Durch Zwischenschalten weiterer Computer als proxy-server, die es zulassen, dass der Client anonym kommuniziert, ist der Server [...] nicht in der Lage, den Adressaten anhand der IP-Adresse zu ermitteln [...]."

348 Zumindest wurde das NetzDG in der Literatur hinsichtlich beider Aspekte kritisch betrachtet und entsprechende Mängel hervorgehoben. Mit Schwerpunkt auf der formellen Verfassungswidrigkeit allen voran *Gersdorf*, MMR 2017, 439 (440 ff) sowie aufgreifend *Müller-Franken*, AfP 2018, 1 (3 f); *Feldmann*, K&R 2017, 292 (294); *Kalscheuer*/*Hornung*, NVwZ 2017, 1721 (1724 f). Materielle Aspekte vertiefend dagegen ebenfalls *Müller-Franken*, AfP 2018, 1 (5 ff); *Feldmann*, K&R 2017, 292 (295 f); *Kalscheuer*/*Hornung*, NVwZ 2017, 1721 (1722 f) sowie *Heckmann*/*Wimmers*, CR 2017, 310; *Nolte*, ZUM 2017, 552 (554 ff); *Liesching*, ZUM 2017, 809; *Peifer*, CR 2017, 809. Den zivilrechtlichen Aspekten nähert sich *Peifer*, AfP 2018, 14.

Einbeziehung der anderen Grundrechtsfunktionen, Aufgabe des Gesetzgebers und der (verfassungsgerichtlichen) Rechtsprechung.

In der Gesamtschau ist damit ersichtlich, dass die abwehrrechtliche Dimension der digitalen Identität fortbesteht und der abstrakte Wortlaut der Grundrechte eine Anpassung bzw. Einbeziehung der digitalen Sachverhalte nicht hindert, sondern vielmehr zulässt. Daher ist auch von einem gleichbleibenden Schutzniveau der Grundrechte als Abwehrrechte gegenüber dem Staat auszugehen. Bezüglich der Eingriffe im Rahmen der mittelbaren Drittwirkung hat der Gesetzgeber allerdings sowohl entsprechenden Spielraum als auch die Verpflichtung, den Grundrechtsträger vor etwaigen Beeinträchtigungen im digitalen Raum zu schützen.[349]

II. Der status positivus der Grundrechte

Wird das feste, verlässliche Terrain des Abwehrrechts verlassen und die Erschließung neuen Terrains angestrebt[350] – ohne sich von der Prädominanz der abwehrrechtlichen Funktion zu trennen[351] – ist sich des Weiteren der diametralen Funktion des status negativus zuzuwenden. Der status positivus, welcher neben den status negativus tritt und daher auf gleicher Ebene anzusiedeln ist,[352] verbirgt sich dogmatisch in den Funktionen der Grundrechte als Leistungs-, Verfahrens- und Teilhaberechte. Den Grundrechten soll demnach eine positive Komponente entnommen werden, die dem Grundrechtsträger gegebenenfalls einen Anspruch auf staatliches Handeln (dann: originäres Leistungsrecht) oder zumindest auf Teilhabe an den Einrichtungen des Staates (dann: derivatives Leistungsrecht) ermöglicht.[353] Hiervon abzugrenzen ist jedoch die Teilhabe an der Ausübung der

349 Hierzu insbesondere Kapitel C.III.
350 Vgl. *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 17.
351 *Sachs* in: Merten/Papier, HGr II, § 39, Rn. 11.
352 *Kloepfer*, VerfR II, § 48, Rn. 19.
353 Zur Kategorisierung siehe grundlegend *Martens*, VVDStRL 30 (1972), 7 (21 ff) sowie *Stern*, StaatsR III/1, S. 697 f, 700; *Kloepfer*, VerfR II, § 48, Rn. 22; *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 12.

Gewalt des Staates iSv Art. 20 Abs. 2 S. 1 GG. Eine derartige Teilhabe ist dem bereits erwähnten status activus zuzuordnen.[354]

Originäre Leistungsrechte spiegeln dabei den Kern des status positivus wider. Denn um ein solches handelt es sich, wenn sich aus der Verfassung ein unmittelbarer Anspruch zu staatlichem Handeln herauslesen lässt.[356] Schon der Wortlaut muss also den Grundrechtsträger als Anspruchsteller erkennen lassen. Dies ist allerdings nur in Art. 6 Abs. 4 und Abs. 5 sowie 19 Abs. 4 und den dazugehörigen Flankierungen in Art. 101 Abs. 1 S. 2, 103 Abs. 1 GG niedergelegt,[357] ferner aus dem Sozialstaatsprinzip nur in Verbindung mit anderen Gütern abgeleitet[358].[359] Einen Anspruch auf eine Handlung des Staates expressis verbis, gleich ob sozialer oder anderer Natur, gibt es damit nicht. Ebenso ist diese Lücke nicht durch Auslegung von Freiheitsrechten zu füllen, da dies dem mit der Fassung des Grundgesetzes zum Ausdruck gebrachten Willen, keine Ansprüche auf staatliche Zuwendungen einzufügen, widerspräche.[360] Darum wird ein originäres Leistungsrecht auch in Zukunft nicht in der Verfassung zu finden sein.[361] Vielmehr wird

354 Nach *Häberle*, VVDStRL 30 (1972), 43 (81 f) sei der status positivus allerdings als Konsequenz des status activus anzusehen. Dem kann insoweit zugestimmt werden, als dass die politische Partizipation des Grundrechtsträgers (äußerst) mittelbar durch die Abgeordneten als Repräsentanten des Volkes gem. Art. 20 Abs. 2 S. 1 GG ausgeübt wird, welche letztlich in teilhabegewährenden Einrichtungen und dem Erhalt staatlicher Institutionen aufgeht. Aufgrund der Nähe dieser beiden Begriffe wird, basierend auf der Differenzierung *Alexys* zwischen dem status positivus im *engeren* und im *weiteren* Sinne[355], der status activus ebenfalls zu als Teil des status positivus angesehen – so beispielsweise *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 13.

356 *Rüfner* in: Merten/Papier, HGr II, § 40, Rn. 1; *Kloepfer*, VerfR II, § 48, Rn. 23 sowie ausführlich *Martens*, VVDStRL 30 (1972), 7 (25 ff).

357 Weitere nennend statt vieler *Stern*, StaatsR III/1, S. 706 f.

358 So BVerfGE 82, 60 (85); 125, 175 (222 f); 132, 134 (159 f); Urteil vom 5.11.2019, Az. 1 BvL 7/16, Rn. 119 sowie vgl. auch E 1, 97 (104 f). Zum Anspruch auf Sicherung des Existenzminimums siehe auch *Breuer* in: Bachof/Heigl/Redeker, Festgabe BVerwG, 89 (95 ff).

359 Vgl. auch *Kingreen*/*Poscher*, Staatsrecht II, Rn. 157; *Dreier* in: Dreier, GG, Vorb. Rn. 89.

360 BVerfGE 87, 181 (197); 1, 97 (104); *Müller-Franken* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Vorb. v. Art. 1, Rn. 18.

361 Ebenfalls dieser Ansicht *Osterloh/Nußberger* in: Sachs, GG, Art. 3, Rn. 55 f; *Dreier* in: Dreier, GG, Vorb. v. Art. 1, Rn. 90; *Stern*, StaatsR III/1, S. 694,; *Hufen*, Staatsrecht II, § 5, Rn. 10.

dieses aus den bestehenden Rechtsgütern herausgelesen, bei sozialen Aspekten insbesondere iVm dem Sozialstaatsprinzip des Art. 20 Abs. 1 GG.

Indes werden aus der Verfassung derivative Leistungsrechte abgeleitet. Unter diesem Begriff sind, wie erwähnt, all jene Ansprüche zu fassen, die eine Teilhabe an bereits vorhandenen Einrichtungen des Staates bzw. Förderungen der Ausübungen der Freiheitsrechte gewähren. Die Herleitung bestimmt sich daher grundsätzlich nicht aus dem die jeweilige Grundrechtsausübung betreffenden Freiheitsrecht, sondern aus dem allgemeinen Gleichheitssatz des Art. 3 Abs. 1 GG.[362] Maßgebend kann hier der Anspruch auf Teilhabe an einer staatlich geförderten Ausbildungsstätte erwähnt werden, wonach die Zugangsbeschränkung mittels Numerus Clausus auf ein angemessenes Maß beschränkt wurde und dem Grundgesetz nur ein Leistungsanspruch „unter dem Vorbehalt des Möglichen" entnommen werden kann.[363] Weiterhin wurde durch weitere Gerichtsentscheidungen der Zugang zu öffentlichen Einrichtungen wie Stadthallen zum Zwecke parteipolitischer Veranstaltungen[364], die Teilhabe am öffentlich-rechtlichen Rundfunk[365] sowie die Beteiligung an Subventionen kraft Selbstbindung der Verwaltung[366] gefestigt und aus den Freiheitsrechten iVm Art. 3 Abs. 1 GG herausgelesen. Diese Transformation des Freiheitsrechts von seiner abwehrrechtlichen Natur zum derivativen Leistungsrecht geschieht infolge der Wandlung der Position des Grundrechtsträgers zum Staat: Je stärker sich die Haltung von einer Abwehrhaltung hin zu

362 *Dreier* in: Dreier, GG, Vorb. vor Art. 1, Rn. 93; *Kischel* in: Epping/Hillgruber, BeckOK GG, Art. 3, Rn. 88; *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 74 f; *Kirchhof* in: Isensee/Kirchhof, HStR VIII, § 181, Rn. 72; *Kloepfer*, VerfR II, § 48, Rn. 2; *Martens*, VVDStRL 30 (1972), 7 (21). Zum Begriff der Teilhabe ferner *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 5 ff; *Kingreen*/*Poscher*, Staatsrecht II, Rn. 155.

363 BVerfGE 33, 303 (329 f, 333); 43, 291 (313 f). Ferner *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 85; *Dreier* in: Dreier, GG, Vorb. Rn. 90; *Breuer* in: Bachof/Heigl/Redeker, Festgabe BVerwG, 89 (114 ff); *Hufen*, Staatsrecht II, § 5, Rn. 10; *Kloepfer*, VerfR II, § 48, Rn. 26. Dies wurde hinsichtlich des Numerus Clausus im Fachbereich Medizin bestätigt – BVerfG NVwZ 2018, 233 (Rn. 103 f); *Brehm*/*Brehm-Kaiser*, NVwZ 2018, 543.

364 Zuletzt BVerfG, Beschluss vom 26.3.2018 – Az. 1 BvQ 18/18 – sowie BVerwG, Urt. vom 21.07.1989 – Az. 7 B 184/88 = NJW 1990, 134; Urt. vom 27.08.1991 – Az. 7 B 19/91 = NVwZ 1992, 263.

365 Sog. Grundversorgung – siehe BVerfGE 73, 118 (157 f); 74, 297 (325 f); 83, 238 (297 f).

366 BVerwGE 14, 307 (310); 15, 190 (196); BVerwG, Urt. v. 28.04.1978 – Az. VII C 43.76 = NJW 1979, 280.

einem Begehr entwickelt, welches sich an Institutionen des modernen Staates richtet, desto mehr wandelt sich die Funktion in Richtung Leistungsrecht.[367] In der Konsequenz entsteht jedoch eine Abhängigkeit von den Leistungen des Staates, sodass die Grenze zwischen Leistungsentzug und Eingriff mit zunehmender Abhängigkeit verschwimmt.[368] Das jeweilige Leistungsrecht ist jedoch nur bezüglich staatlicher Institutionen durchsetzbar, daher eher als Chance auf Leistungsteilhabe zu sehen und folglich nicht gegenüber dem Gesetzgeber unmittelbar geltend[369]. Ein Einwirken auf Private bzw. Dritte zur Gewährleistung einer gleichberechtigten Teilhabe kann nicht über den status positivus der Grundrechte erlangt werden.[370] Indes ist auf die Rechtsfigur der Schutzpflicht zurückzugreifen.[371]

Abschließend ist vor dem ausgeführten begrifflichen Hintergrund auch der status positivus zur digitalen Identität ins Verhältnis zu setzen. Da der status positivus die aktive Grundrechtsausübung umfasst, ist insoweit von Seiten des Staates die entsprechende Möglichkeit der Nutzung digitaler Identitäten zu gewährleisten. Dies meint jedoch mitnichten, dass der Staat das bloße Vorhandensein von Plattformen im Sinne eines eines Identitätsmanagementsystems sicherstellen oder gar expressis verbis garantieren muss, um in letzterem Falle auf ein originäres Leistungsrecht zurückzugreifen. Es muss keine Möglichkeit der Ausgestaltung eines digitalen Alter Egos vorgehalten werden, um diese hoheitliche Aufgabe zu erfüllen. Ebenfalls ist kein Recht bzw. Anspruch auf Teilhabe an einer öffentlich-rechtlichen Plattform ersichtlich, da es prima facie schon an entsprechenden (digitalen) Institutionen mangelt. Dies erfordert jedoch nicht, dass zu diesem Zweck neue Institutionen geschaffen werden müssen. Die Errichtung eines „staatlichen Facebook“ scheint schon unmöglich, wo sich ein derartiges Mittel der

367 Vgl. *Kirchhof* in: Maunz/Dürig, GG-Kommentar, Art. 3 I, Rn. 293.
368 *Hufen*, Staatsrecht II, § 5, Rn. 10.
369 So *Kischel* in: Epping/Hillgruber, BeckOK GG, Art. 3, Rn. 89; *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 74
370 So auch *Sachs* in: Sachs, GG, Vor Art. 1, Rn. 48; *Müller-Franken* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Vorb. v. Art. 1, Rn. 18 aE. Vgl. auch *Stern*, StaatsR III/1, S. 732 f.
371 *Stern*, StaatsR III/1, S. 728 f.

Massenkommunikation ebenfalls nicht nur als Medium, sondern auch als Faktor der öffentlichen Meinungsbildung herauskristallisieren kann. Eine Tendenz bzw. Steuerung von Seiten des Staates ist aufgrund der Verantwortlichkeit für die Programmierung der Plattform nicht vollständig auszuschließen. Dies widerstrebt jedoch der Staatsfreiheit der Medien der Massenkommunikation[372], insbesondere wenn Art. 5 Abs. 1 S. 2 GG als Mediengrundrecht verstanden wird[373]. Vielmehr könnte eine Gewährleistung darin bestehen, einen Anspruch auf Zugang zum Dienst zu erhalten. Dies lässt sich jedenfalls aus der Linie des Bundesverfassungsgerichts folgern, die sich hinsichtlich der mittelbaren Drittwirkung des Art. 3 Abs. 1 GG zwischen Privaten abzeichnet.[374] Richtet man den Blick auf die Online-Plattformen der öffentlich-rechtlichen Rundfunkanbieter und mögliche Verknüpfungen von Mediatheken und presseähnlichen Angeboten mit einer Kommentarfunktion oder andersartigen Informationsportalen öffentlicher Einrichtungen, so ergebe sich an dieser Stelle durchaus ein Anspruch auf Teilhabe am Diskurs im Rahmen der Kommentarspalte oder ähnlicher Möglichkeiten der Meinungskundgabe.[375] Diesem werden Anbieter von solchen Plattformen aber regelmäßig gerecht. Die nachträgliche Begrenzung dieser Teilhabe, beispielsweise aufgrund von unzulässiger Schmähkritik oder anderweitigen widerrechtlichen Verhaltens, bleibt hiervon unberührt. Derartige Sanktionen dürfen sich aber keinesfalls auf den generellen Zugang zum Informationsangebot auswirken, da dies ferner zu einer Beeinträchtigung der Informationsfreiheit des Art. 5 Abs. 1 Alt. 2 GG oder dem Recht auf Teilhabe an öffentlichen Einrichtungen aus Art. 5 Abs. 1 S. 1, 3 Abs. 1 GG führen würde.[376] Die digitale Identität bleibt daher zumindest inhaltlich nur in wenigen Fällen vom status positivus umfasst.

372 Vgl. BVerfGE 12, 205 (260 f).

373 So als „Antwort" auf die Digitalisierung der Massenmedien *Kühling* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 5 GG, Rn. 11, 3 ff.

374 BVerfGE 148, 267 (283 f) sowie bezugnehmend Einweilige Anordnung vom 22.5.2019 – Az. 1 BvQ 42/19 –, Rn. 15; Nichtannahmebeschluss vom 27.8.2019 – Az. 1 BvR 879/12, Rn. 5 ff.

375 Vgl. BVerfGE 148, 267 (Rn. 41); Einstweilige Anordnung vom 22-05-2019 – 1 BvQ 42/19 –, Rn. 15; *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 137. Eine ähnliche Konstellation aufspannend *Schmehl*/*Richter*, JuS 2005, 817 (insbes. 818 f).

376 Zum digitalen Hausrecht von Behörden im Detail *Kalscheuer*/*Jacobsen*, NJW 2018, 2358 (2359 ff).

Von der Frage nach der inhaltlichen Einordnung der digitalen Identität ist dagegen die Frage des Zugangsmittels zur digitalen Identität zu trennen. Schon denklogisch bedarf es einer funktionierenden und gewährleisteten Infrastruktur, über die die Angebote der Plattformen bzw. Telemedien abgerufen werden können. Angesichts der Digitalisierung sowie der Teilhabe am gesellschaftlichen Diskurs und Willensbildungsprozess ist es erforderlich, dass der Staat diese Möglichkeit der Grundrechtsausübung – also die Nutzung des Internets als Informations- und Kommunikationsmedium – jedem Bürger ermöglicht.[377] Andernfalls ließe sich die Förderung neuer Entwicklungen und die Einbeziehung aller Bundesbürger in die Digitalisierung aller Prozesse, z.B. die elektronische Steuererklärung nach dem ELSTER-Verfahren, Meldungen und Terminvereinbarungen bei örtlichen Behörden oder weitere kommunale Angebote, nicht aufrechterhalten. Bürger ohne diese Möglichkeiten verlieren den Anschluss an die Gesellschaft, sind gewissermaßen „locked out". Zu beachten ist daher, dass von Seiten des Gesetzgebers sowohl die generelle Nutzungsmöglichkeit des Internets – also der Anschluss an sich – als auch die entsprechende Bandbreite gewährleistet wird, um sowohl gegenwärtige als auch zukünftige Angebote problemlos nutzen zu können. Dies lässt sich zumindest aus Art. 87f Abs. 1 GG, auch unter Einbeziehung der Idee der Grundversorgung iVm dem Sozialstaatsprinzip des Art. 20 Abs. 1 GG, schlussfolgern.[378] So fasste der BGH im Falle des Ausfalls des Internetzugangs zusammen: „Die Nutzbarkeit des Internet ist ein Wirtschaftsgut, dessen ständige Verfügbarkeit seit längerer [...] Zeit auch im privaten Bereich für die eigenwirtschaftliche Lebenshaltung typischerweise von zentraler Bedeutung ist und bei dem sich eine Funktionsstörung als solche auf die materiale Grundlage der Lebenshaltung signifikant auswirkt. [...] Damit hat sich das Internet zu einem die Lebensgestaltung

377 Als Bestandteil des Existenzminimums diskutierend *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 101 ff.

378 Zur Reichweite des Gewährleistungsauftrages des Art. 87f Abs. 1 GG im Einzelnen siehe *Gersdorf* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band III, Art. 87f, Rn. 20, 23 f, 30 f; *Möstl* in: Maunz/Dürig, GG-Kommentar, Art. 87f, Rn. 71, 72; *Holznagel*/*Beine*, MMR 2015, 567 (568/569); *Schumacher*, MMR 2011, (712/713). Der Gewährleistungsauftrag ist jedoch kein (originäres oder derivates) Leistungsrecht des Bürgers, sondern ausschließlich als Staatsziel iSe verfassungsrechtlichen Wertentscheidung zu verstehen – *Gersdorf* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band III, Art. 87f, Rn. 30 aE.

eines Großteils der Bevölkerung entscheidend mitprägenden Medium entwickelt, dessen Ausfall sich signifikant im Alltag bemerkbar macht.“[379] In der Wahl der Mittel ist der Gesetzgeber aber, wie generell zur Erfüllung der Leistungsrechte, frei und hat einen weiten Ermessensspielraum.[380]

III. Die Schutzpflichten des Staates: Eine eigene Kategorie?

Die inhaltliche Komponente der digitalen Identität und der Schutz ebendieser ist demzufolge nicht vollständig in die traditionellen Begriffe nach *Jellinek* einzuordnen. Vielmehr ergibt sich diese aus der Wirkung der Grundrechtsgehalte insgesamt, also sowohl den subjektiv-rechtlichen Gehalten als auch der objektiv-rechtlichen Dimension der Grundrechte. Im Folgenden soll daher über den dogmatischen Hintergrund der Schutzpflichten die Relevanz der Schutzpflicht im Allgemeinen für die digitale Identität dargelegt werden.

379 BGH, Urt. vom 24.01.2013 – Az. III ZR 98/12 = NJW 2013, 1072.

380 Vgl. zur Gewährleistungsaufgabe des Bundes im Bereich der Telekommunikation gem. Art. 87f Abs. 1 GG *Gersdorf* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band III, Art. 87f, Rn. 31 f; *Möstl* in: Maunz/Dürig, GG-Kommentar, Art. 87f, Rn. 76 f sowie im Allgemeinen *Rüfner* in: Merten/Papier, HGr II, § 40, Rn. 38; vgl. auch *Murswiek* in: Isensee/Kirchhof, HStR IX, § 192, Rn. 74 aE.

1. Der dogmatische Hintergrund der Schutzpflicht

Während sich der verfassungsrechtliche Begriff der Grundpflicht mit dem Gegenstück der Grundrechte befasst,[381] bezieht sich der Begriff der Schutzpflicht auf eine Verpflichtung des Staates auf Schutz des Grundrechtsträgers. Es ist Aufgabe des Staates schützend und fördernd einer Aushöhlung der Freiheitsgarantien vorzubeugen.[382] Gelegentlich wird jedoch zwischen der echten und unechten

381 Als Grundpflicht wird die verfassungsrechtlich verankerter Pflicht des Einzelnen gegenüber dem Staat bezeichnet, nicht jedoch Pflichten der Staatsorgane untereinander. In der Verfassung finden sich diese unter anderem in Art. 6 Abs. 2 (Erziehungspflicht/Elternverantwortung) und 26 Abs. 1 GG (Friedenspflicht) sowie der ehemaligen Wehrpflicht. Der Begriff geht auf die Verpflichtungen und Terminologie aus der WRV zurück, insbes. Art. 132 bis 134, 109 Abs. 2, 110 Abs. 2, 120, 145, 153 Abs. 3, 155 Abs. 3, 163 WRV. Hierzu ausführlich *Stober*, Grundpflichten und Grundgesetz, S. 12 f sowie *Stern*, StaatsR III/2, S. 985 ff; *Ranzelhofer* in: Merten/Papier, HGr II, § 37, 17 ff; *Stern*, Der Staat des Grundgesetzes, S. 293 ff; *Hufen*, Staatsrecht II, § 5, Rn. 24; *Gusy*, JZ 1982, 657 (insbes. 658 ff); *Isensee*, DÖV 1982, 609; *Stober*, NVwZ 1982, 473 (insbes. 476 ff); *Badura*, DVBl 1982, 861.

382 So stRspr BVerfGE 35, 79 (114) sowie 39, 1 (42). Vgl. auch BVerfGE 33, 303 (339 f); 43, 242 (267); 47, 327 (369 f).

Schutzpflicht differenziert.[383] So handelt es es sich um eine unechte (grundrechtliche) Schutzpflicht, wenn diese ohnehin Aufgabe des Staates ist und dazu dient, die Dreieckskonstellation[384] iSd mittelbaren Drittwirkung aufzulösen bzw. den Grundrechten des Opfers zum Schutz zu verhelfen. Eine echte (allgemeine oder rechtsstaatliche) Schutzpflicht liegt dagegen vor, sofern sich die Verpflichtung zum Schutz nicht aus den Schutzgütern der Grundrechte unmittelbar ableitet, sondern vielmehr auf der objektiven Werteordnung an sich fußt. Diese ist als solche nicht vorgegeben, sondern bedarf erst einer Herleitung, die sodann auch in einem entsprechend weiten Gestaltungsspielraum mündet[385]. Letztlich wird der Staat in

383 Hierzu sowie zu Folgendem ausführlich *Kingreen*/*Poscher*, Staatsrecht II, Rn. 134 ff, 141 f sowie ähnlich differenzierend *Stern*, StaatsR III/1, S. 937 f; *Calliess* in: Merten/Papier, HGr II, § 44, Rn. 4; *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 192 ff. Zum Verhältnis von Schutzpflichten und mittelbarer Drittwirkung ferner *Kahl* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 Abs. 3 GG, Rn. 333 f. Dennoch wird in der weiteren Literatur kaum zwischen diesen Varianten unterschieden, was vielerlei – berechtigte – Gründe haben mag: Zunächst sind beide Arten gem. Art. 1 Abs. 3 GG an alle Staatsgewalten adressiert. Weiter ergibt sich in der Rechtsfolge kein Unterschied zwischen den Arten, kommt es doch gleichermaßen zur Anwendung der Verhältnismäßigkeit und der Einbeziehung von Untermaß- und Übermaßverbot. Ebenso kann sich bei entsprechender Reduktion des (gesetzgeberischen) Spielraumes ein Anspruch auf staatliches Handeln ergeben. Darüber hinaus fußen beide Arten auf der gleichen Grundlage, nämlich dem sogleich näher zu erläuternden Zwitterhaftigkeit der dimensionalen Einordnung. Mit ähnlichem Ergebnis *Klein*, NJW 1989, 1633 (1637 ff) sowie *Kahl* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 Abs. 3 GG, Rn. 334 aE. Vgl. als einheitlichen Begriff verwendend *Sachs* in: Sachs, GG, Vor Art. 1, Rn. 35, 37-38; *Herdegen* in: Maunz/Dürig, GG-Kommentar, Art. 1 I, Rn. 78-79; *Alexy*, Theorie der Grundrechte, S. 410 f; *Starck*, Praxis der Verfassungsauslegung, S. 46 f; *Kloepfer*, VerfR II, § 48, Rn. 55 f; ; *Manssen*, Staatsrecht II – Grundrechte, Rn. 50; *von Münch*/*Mager*, Staatsrecht II – Grundrechte, Rn. 51; *Schliesky* et al., Schutzpflichten und Drittwirkung im Internet, S. 47 f; *Klein*, NJW 1989, 1633 (1637); *Dreier*, JURA 1994, 505 (512). Als erweiterten Begriff vorschlagend *Müller-Franken* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Vorb. v. Art. 1, Rn. 24 aE. Ganz anders dagegen *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, S. 108 sowie *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, S. 243 ff, die zwischen einer primären und sekundären Schutzpflicht unterscheiden.

384 Gemeint ist jene zwischen Opfer und Störer als privatrechtliche Personen und dem Staat – so nur *Erichsen*, JURA 1997, 85 (85); *Müller-Franken* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Vorb. v. Art. 1, Rn. 23 sowie ausführlich *Calliess* in: Merten/Papier, HGr II, § 44, Rn. 18.

385 Vgl. BVerfGE 39, 1 (44); 46, 160 (164); 81, 242 (255); 88, 203 (262); *Alexy*, Theorie der Grundrechte, S. 421 f; *Kloepfer*, VerfR II, § 48, Rn. 65 ff; *Möstl*, DÖV 1998, 1029 (1037 f); *Erichsen*, JURA 1997, 85 (89).

beiden Fällen zum Garanten der geschützten Rechtsgüter[386] bzw. Koordinator der grundrechtlichen Freiheiten[387].

Prima facie lässt sich in dieser Konstellation eine Parallele zur Funktion der Grundrechte als Leistungsrechte erkennen,[388] folgt aus dieser in bestimmten Fällen ein Anspruch und demgemäß eine Verpflichtung des Staates zu einem Handeln[389]. Dies lässt auf eine Nähe zu den subjektiv-rechtlichen Funktionen bzw. Dimensionen der Grundrechte schließen. So ist dem status negativus der Grundrechte zugleich eine schützende Dimension gegenüberzustellen.[390] Eine rein subjektiv-rechtliche Funktion, wie sie in Form der abwehrenden Staatstätigkeit von *Sachs*[391] und *Dürig*[392] vorgetragen wird, führt im Ergebnis aber zu einer Verstärkung bzw. Legitimation der Eingriffsbefugnis des Staates in die Grundrechte Dritter.[393] Der klassisch liberale Sicherheitszweck, den *Isensee* aus den Grundrechten in ihrer Gesamtheit schließt, würde auf diese Weise ins Gegenteil verkehrt und die eigentliche Funktion der Grundrechte pervertiert.[394] Sie kann daher nur als Ausgangspunkt

386 So *Klein*, NJW 1989, 1633 (1634).

387 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 176.

388 Auch *Robbers*, Sicherheit als Menschenrecht, S. 125 f greift diese Parallele auf, jedoch basierend auf der aktiven Handlungsweise des Staates.

389 Vgl. BVerfGE 39, 1 (46); *Müller-Franken* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Vorb. v. Art. 1, Rn. 23 aE. Grundsätzlich ergibt sich kein Anspruch aus einer Schutzpflicht – siehe nur BVerfGE 77, 170 (215): „Nur unter ganz besonderen Umständen kann sich diese Gestaltungsfreiheit in der Weise verengen, daß allein durch eine bestimmte Maßnahme der Schutzpflicht Genüge getan werden kann."; *Starck*, Praxis der Verfassungsauslegung, S. 83 unter Bezug auf die Gewaltenteilung; *Wahl*/*Masing*, JZ 1990, 553 (562); *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 67 f. Zum Recht auf Schutz im Detail *Robbers*, Sicherheit als Menschenrecht, S. 124 ff.

390 *Stern*, StaatsR III/1, S. 945 f; *Schliesky* et al., Schutzpflichten und Drittwirkung im Internet, S. 47. Vgl. auch *Calliess* in: Merten/Papier, HGr II, § 44, Rn. 18; *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 192.

391 *Sachs* in: Sachs, GG, Vor Art. 1, Rn. 35, 37.

392 *Dürig*, AöR 81 (1956), 117 (118).

393 Vgl. *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, S. 123.

394 *Isensee*, Das Grundrecht auf Sicherheit, S. 31 f; vgl. auch *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 21 f; mwN auch *Calliess* in: Merten/Papier, HGr II, § 44, Rn. 8. Seine Wurzeln findet dieser Gedanke auch in den Theorien Kants, siehe hierzu im Detail *Starck*, Praxis der Verfassungsauslegung, S. 49 f.

genutzt werden.[395] Darüber hinaus ist der status positivus, welcher ebenfalls den subjektiv-rechtlichen Funktionen zuzuordnen ist, nicht zu vernachlässigen: Durch die Hinzunahme der positiven Komponente werden die Grundrechte in ihrer klassischen Funktion auf der Ebene zwischen Privaten ausgestaltet und erweitert. Ihnen kommt so eine noch breitere Geltung zu.[396]

Diesem Verständnis ist der objektive Wertgehalt zu Grunde zu legen. Darunter ist nach der grundlegenden Lüth-Entscheidung des Bundesverfassungsgerichts der Gehalt der Grundrechte als Wertesystem zu verstehen, sodass sich daraus eine für das Sozialgefüge wegweisende Grundentscheidung in allen (rechtlichen) Bereichen ergibt.[397] Auf Basis dieses überindividuellen Gehaltes der Grundrechte ist der Staat angesichts seiner Vormachtstellung[398] zur Fürsorge angehalten. Hinsichtlich der subjektiv-rechtlichen Funktionen wirkt er damit als Gravitationszentrum.[399] Erstmals umfängliche Anerkennung fand die objektiv-rechtliche Dimension erst 1975 in der ersten Schwangerschaftsabbruch-Entscheidung.[400] Die Einordnung der Schutzpflicht in die objektiv-rechtliche Dimension wird später in der wiederholten Entscheidung zum Schwangerschaftsabbruch aufgegriffen[401] und den Entscheidungen zum Schutz vor Terrorismus[402], zu Risiken der Technik in Belangen des Umweltschutzes[403] und der Gesundheit[404], zum Anspruch des Kindes auf Vaterschaftsauskunft[405] und zur medizinischen Versorgung[406] bestätigt.

395 So auch *Sandfuchs*, Privatheit wider Willen, S. 118; vgl. auch *Wahl*/*Masing*, JZ 1990, 553 (558).
396 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 159; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 56 f.
397 Vgl. BVerfGE 7, 198 (205 f).
398 Diese anhand der Privatautonomie abbildend *Kahl* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 Abs. 3 GG, Rn. 370.
399 So *Dreier*, JURA 1994, 505 (512).
400 BVerfGE 39, 1 (41 f).
401 BVerfGE 88, 203 (252).
402 BVerfGE 46, 160 (164 f); 49, 24 (53 ff).
403 BVerfGE 49, 89 (142); 53, 30 (57).
404 BVerfGE 56, 54 (73).
405 BVerfGE 96, 56 (64).
406 Vgl. BVerfGE 115, 25 (49).

Insoweit scheinen sich die subjektiv-rechtliche – sowohl klassisch-liberal als auch positiv erweiternd – und die objektive Werteordnung der Grundrechte gegenüberzustehen. Wie dargestellt verhalten sie sich jedoch nicht ausschließlich konträr zueinander, sondern verschmelzen letztlich in einer umfänglichen Betrachtung eines mehrpoligen Verfassungsverhältnisses.[407] Seinen Ursprung findet dieses in der Kollision grundrechtlicher Interessen und Güter, namentlich der mittelbaren Drittwirkung der Grundrechte.[408] Die obligatorische Aufgabe des Staates, den Grundrechtsträger vor Gefahrensituationen im Dreiecksverhältnis zu schützen, ist insbesondere durch die speziellen Güter der Art. 1-19 GG geprägt. Dementsprechend sind ihre Eigenheiten im Einzelfall zu beachten. In der jeweiligen Gewichtung entsteht auf Grundlage der objektiven Verpflichtung des Staates durch die Schärfung an den subjektiv-rechtlichen Dimensionen des Grundrechtskatalogs eine im Einzelfall zu betrachtende Schutzpflicht,[409] welche durch bereichsdogmatisches Ausbalancieren zu ermitteln ist[410]. Vor diesem Hintergrund erscheint es

407 Diese Theorie aufstellend *Calliess* in: Merten/Papier, HGr II, § 44, Rn. 19 ff, welche unter anderem in BVerfGE 115, 205 (232 f) herangezogen wird.

408 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 193.

409 So auch *Müller-Franken* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar, Vorb. v. Art. 1, Rn. 26.

410 Zur Vorgehensweise *Jeand'Heur*, JZ 1995, 161 (165), unter dem Stichwort der Resubjektivierung der objektiv-rechtlichen Funktion der Grundrechte darstellend *Dreier* in: Dreier, GG, Vorb., Rn. 95 sowie *Robbers*, Sicherheit als Menschenrecht, S. 193 f; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 58 ff, 64.

nicht abwegig, diese Zusammensetzung aus subjektiven und objektiven Elementen in Form der Schutzpflichten als eigene Kategorie anzuerkennen.[411]

Unabhängig von dieser Einordnung haben sich sowohl in der Literatur als auch in der Rechtsprechung des Bundesverfassungsgerichts Kriterien herausgebildet, nach denen eine Schutzpflicht entsteht. Zuvorderst bedarf es eines grundrechtlich geschützten Gutes, wofür prinzipiell jedes grundrechtliche Schutzgut in Betracht kommt.[412] Dazu muss das jeweilige Gut hinreichend durch einen gegenwärtigen oder drohenden Eingriff ersichtlich gefährdet sein. Dieser kann beispielsweise in einer nicht unerheblichen Einwirkung auf das grundrechtliche Schutzgut gegen den Willen des Grundrechtsträgers bestehen, muss aber von einem grundrechtsfähigen und privaten Störer ausgehen.[413] Auf eine Rechtswidrigkeit des Handelns

411 Diesem Ansatz scheinbar ebenso folgend *Klein*, NJW 1989, 1633 (1633, 1639), da dieser die Schutzpflichtenfunktion der Grundrechte „neben" die subjektive und objektive Grundrechtsfunktion setzt. Weiter ordnet *Kloepfer*, VerfR II, § 48, Rn. 58 der Schutzpflicht sowohl objektiv- als auch subjektiv-rechtliche Gehalte zu und deutet zumindest die Ambivalenz an. Ähnlich auch *Calliess* in: Merten/Papier, HGr II, § 44, Rn. 24, wobei hier die Schutzdimension tendenziell auf gleicher Ebene der Abwehrdimension beheimatet ist. Weiter bezeichnet *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 194 die dargestellte Problematik als „Eigenart" und fasst zusammen: „Die Einteilung nach subjektiven und objektiven Grundrechtsfaktoren bündelt Disparates und trennt Zusammengehöriges, nämlich die Abwehr- und Schutzfunktion, die zwei Seiten einer Medaille sind: Schutz des identischen grundrechtlichen Gutes, jene vor dem staatlichen, diese vor dem privaten Eingriff." Deutlich auch *Dreier* in: Dreier, GG, Vorb. Rn. 104: „Schutzpflichten bilden eine eigenständige Grundrechtsdimension" sowie *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, S. 170: „Schutzpflichten als [...] eigenständige[n] Grundrechtsfunktion".

412 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 218; *Kloepfer*, VerfR II, § 48, Rn. 60; *Schliesky* et al., Schutzpflichten und Drittwirkung im Internet, S. 51 f. Eine Übersicht zu den bislang vom Bundesverfassungsgericht angenommenen Schutzpflichten zusammenstellend *Starck*, Praxis der Verfassungsauslegung, S. 57 ff sowie *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, S. 174 ff.

413 *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 218, 225 f, 240 f; *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, S. 190; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 87 f, 102 f; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 75 f; *Erichsen*, JURA 1997, 85 (87); vgl. auch *Isensee*, Das Grundrecht auf Sicherheit, S. 37; *Robbers*, Sicherheit als Menschenrecht, S. 124/125. Gerade letzteres ist zur Abgrenzung der rein abwehrrechtlichen Dimension notwendig – hierzu ebenfalls *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 247 f.

kommt es nicht an.[414] Vielmehr sind Schadensausmaß und Eintrittswahrscheinlichkeit als Maßstab proportional ins Verhältnis zu setzen.[415] Je größer das potentielle Schadensausmaß, desto geringer die erforderliche Eintrittswahrscheinlichkeit.[416] Letztlich muss der betroffene Grundrechtsträger auch schutzbedürftig sein. Denn dies entfällt, soweit bereits ein angemessenes Schutzniveau gegeben ist – beispielsweise durch mögliche Eigeninitiativen oder bereits geleistete Erfüllung der Schutzpflicht von Seiten aller Staatsgewalten.[417] Ebenfalls ausschließend wirkt die Selbstgefährdung des Grundrechtsträgers, sofern sie nicht auf einem Übergewicht des Störers basiert.[418] Schließlich kann der Staat nicht für jegliche Störung privater Rechtsbeziehungen einstehen und sich schützend vor den Betroffenen stellen. Die Schutzpflicht soll nur im Einzelfall, wenn eine Untätigkeit des Staates gegeben ist, eine entsprechende Verpflichtung entstehen lassen.[419] Die Erfüllung der Schutzpflicht steht folglich unter dem Vorbehalt des Möglichen.[420]

Ist der Tatbestand der Schutzpflicht erfüllt und das Potential für eine notwendige Schutzpflichtenhandlung gegeben, bleibt zu untersuchen, inwieweit den Obrigkeiten ein Spielraum zur Umsetzung der Schutzpflicht gegeben ist. Grundsätzlich ist hierbei von einem weiten Gestaltungsspielraum auszugehen,[421] sowohl inhaltlich als auch bei der Wahl der Mittel. Dennoch ist das Gesetz regelmäßig das Mittel der

414 *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 106; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 226 f; *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, S. 233.

415 *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, S. 85; *Hermes*, Das Grundrecht auf Schutz von Leben und Gesundheit, S. 236.

416 *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, S. 86 mwN; *Schliesky* et al., Schutzpflichten und Drittwirkung im Internet, S. 54.

417 Vgl. *Möstl*, DÖV 1998, 1029 (1036); *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 239, 271 f.

418 Hierzu BVerfGE 81, 242 (252 ff); *Erichsen*, JURA 1997, 85 (87). Zur Problematik allgemein *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 244 f. Diese Frage stellt sich ebenso bei der Nutzung der digitalen Identität, siehe Abschnitt C.III.2..

419 *Möstl*, DÖV 1998, 1029 (1030 f) sowie weitere Verweise in Fn. 389.

420 BVerfGE 33, 303 (333) sowie E 147, 253 (Rn. 105); *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 274.

421 BVerfGE 77, 170 (214 f); 79, 174 (202); 85, 191 (212); 88, 203 (262); 96, 56 (64); 117, 202 (227, Rn. 63). Vgl. auch E 46, 160 (165); 39, 1 (44); 56, 54 (81); Urteil vom 19.12.2017 – Az. 1 BvL 3/14 –, Rn. 115. Auch *Kahl* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 III, Rn. 374; *Dreier* in: Dreier, GG, Vorb. Rn. 103.

Wahl.[422] Inhalt der Schutzpflicht ist grundsätzlich keine explizite Verpflichtung zu einer inhaltlich bestimmten Handlung, sondern oft nur zum bloßen „Ob". Dies folgt gerade daraus, dass es sich bei Schutzpflichten um Prinzipiennormen mit Verwirklichungstendenz handelt.[423] Sie ist eo ipso unbestimmt und unspezifisch.[424] Die Ausgestaltung dieses „Ob" ist aber am angemessenen Schutzniveau zu orientieren. Daher ist einzubeziehen, welche Mittel von Seiten der Gewalten bereits zur Umsetzung der Schutzpflicht genutzt wurden und ob diese effektiv,[425] mithin auch funktions- und gewaltenspezifisch geeignet sind[426]. Die Frage der Effektivität bemisst sich allerdings nach dem Untermaßverbot,[427] welchem das Übermaßverbot

422 *Kahl* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 1 III, Rn. 332 f, 373 f; *Dreier* in: Dreier, GG, Vorb. Rn. 102; *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 281. Als „gesetzesmediatisiert" bezeichnend *Isensee*, Das Grundrecht auf Sicherheit, S. 42 ff.

423 Vgl. *Böckenförde*, Der Staat 29 (1990), 1 (13, 21 f) als Rückschluss aus *Alexy*, Theorie der Grundrechte, S. 75 ff.

424 *Wahl*/*Masing*, JZ 1990, 553 (558).

425 Vgl. *Möstl*, DÖV 1998, 1029 (1036 f, 1038 f); *Erichsen*, JURA 1997, 85 (88).

426 *Wahl*/*Masing*, JZ 1990, 553 (559).

427 Erstmals erwähnend BVerfGE 88, 203 (340), anschließend fortgeführt in BVerfG NJW 1995, 2343; NJW 1996, 651. Dabei bezieht sich die erstmalige Erwähnung auf die Ausführungen von *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 301, 304 f. Dennoch kommt das ius primae intentionis *Schuppert*, Funktionell-rechtliche Grenzen der Verfassungsinterpretation, S. 14-15 zu.

gegenübersteht[428] und so einen dazwischenliegenden Gestaltungs- und Ermessensspielraum aufspannt[429]. Die Prämisse des Untermaßverbots gleicht mit dem Ziel des generösen Grundrechtsschutzes einem Optimierungsgebot.[430] Es bleibt allerdings bei einer bloßen Optimierung, da mit der effektivsten Schutzpflichtenerfüllung nicht immer auch eine vollumfängliche Risikobeseitigung einhergehen muss.[431] Vielmehr ist ein angemessenes Maß zwischen Effektivität und staatlicher Möglichkeit zu wählen, welches nur begrenzt der verfassungsgerichtlichen Überprüfung zugänglich ist. Sollte das Mittel der Wahl sich im Rahmen des Untermaßverbots erst im Laufe der Zeit und gesellschaftlichen Wandels als ineffektiv erwiesen haben, so ist die Staatsgewalt auf die Verpflichtung zur Nachbesserung hinzuweisen.[432] Der Auslegung und Anwendung der Schutzpflichten kommt so ein dynamischer Charakter zu.[433]

428 So auch *Byrde* abweichend in BVerfGE 121, 317 (380) – „(...) bei dem der Gesetzgeber von Verfassungs wegen ohnehin schon zwischen Untermaßverbot hinsichtlich einer möglichen Verletzung der Schutzpflicht und Übermaßverbot hinsichtlich der durch die Regelung Betroffenen eingeklemmt ist." Kritisch einschließlich einer Gesamtdarstellung der Ansichten *Tzemos*, Das Untermaßverbot, S. 74 ff, insbes. 82 f. Ebenso *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, S. 300; *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 304 f sowie *Calliess* in: Merten/Papier, HGr II, § 44, Rn. 30; *Möstl*, DÖV 1998, 1029 (1038); *Sandfuchs*, Privatheit wider Willen, S. 123 f. Ablehnend allerdings *Hain*, DVBl 1993, 982, welcher Unter- und Übermaßverbot vereint, indem er den Begriff der Erforderlichkeit mit dem der Effektivität gleichsetzt. Den Begriff des Untermaßverbots erklärt er daher zur nicht notwendigen Erweiterung der verfassungsrechtlichen Termini. Dabei verkennt er allerdings die bereits erläuterte Unterscheidung zwischen Effektivität und Erforderlichkeit. Weiter sei *Sandfuchs* zuzustimmen, da ohne ein Mindestmaß an Schutz die Weiterentwicklung der *Schutz*bereiche durch Rechtsprechung und die stetige Veränderung des Staates und der Welt, die den Staat zur Nachbesserung zwinge, leer liefe. Denn auch letztere ist Teil der Erfüllung der Schutzpflichten – siehe nur BVerfGE 88, 203 (310).

429 *Michael*, JuS 2001, 764 (767); *Möstl*, DÖV 1998, 1029 (1038); *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, S. 181.

430 *Krings*, Grund und Grenzen grundrechtlicher Schutzansprüche, S. 259 f, 262; *Unruh*, Zur Dogmatik der grundrechtlichen Schutzpflichten, S. 78; *Böckenförde*, Der Staat 29 (1990), 1 (21 f); *Wahl/Masing*, JZ 1990, 553 (554).

431 Vgl. BVerfGE 49, 89 (137); 53, 30 (59); 77, 170 (227); *Isensee* in: Isensee/Kirchhof, HStR IX, § 191, Rn. 238, 154; *Starck*, Praxis der Verfassungsauslegung, S. 80; *Klein*, NJW 1989, 1633 (1638); *Pietrzak*, JuS 1994, 748 (751). Das verbleibende Risiko ist insoweit als rechtlich erlaubtes Risiko anzusehen – *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik, S. 87.

432 *Pietrzak*, JuS 1994, 748 (752).

433 BVerfGE 88, 203 (309); *Sandfuchs*, Privatheit wider Willen, S. 125.

2. Die digitale Identität im Kontext der Schutzpflichten-Lehre

Konklusiv ist nun wie bei vorigen Schutzkonzepten der Verfassung der Bezug zum Begriff der digitalen Identität aufzuzeigen. Dies kann, insbesondere hinsichtlich des folgenden Kapitels, nur überblickshaft erfolgen und beispielhaft nur anhand von Einzelfällen vertieft werden.

Betrachtet man die digitale Gesamt-Identität als digitale Replica der (analogen) Persönlichkeit, so steht das Allgemeine Persönlichkeitsrecht im Mittelpunkt der Suche nach möglichen Schutzgütern. Das Fernmeldegeheimnis des Art. 10 Abs. 1 GG, die technischen Aspekte des Art. 13 Abs. 1 GG sowie letztlich auch des Allgemeinen Persönlichkeitsrechts selbst sind lediglich begleitend hinzuzuziehen, da eine digitale Identität nicht ohne die entsprechende Informationsinfrastruktur abbildbar ist. Allen ist vorliegend aber gemein, dass ihre Zwecke zunächst nicht dafür vorgesehen waren, in einer derartig technischen bzw. modernen Lesart gesehen zu werden. Trotzdem lassen sich ihre Zwecke auf einen gemeinsamen Nenner zurückführen, dem in der Digitalisierung sowie hinsichtlich der digitalen Identität ein besonderer Stellenwert zukommt: Die Vertraulichkeit[434]. Als potentielles, generelles Schutzgut für die Schutzpflicht kommt daher der Erhalt der Vertraulichkeit und der Integrität von digitalen Informationen in Betracht, welcher durch eine Aggregation und die faktischen Eingriffsvarianten der Erhebung, Speicherung, Verarbeitung und Weitergabe beeinträchtigt werden könnten. Hierfür spricht insbesondere die neueste Schöpfung des Bundesverfassungsgerichts in Form des Grundrechts auf Gewährleistung der *Vertraulichkeit* und Integrität informationstechnischer Systeme.[435] Hinzu tritt im Lichte dieser und mit Blick auf die informationelle Selbstbestimmung die Herrschaft über die eigenen Daten, sei es durch den Grundsatz der Datenminimierung oder die Transparenz bzgl. der Verarbeitungsvorgänge. Diese finden sich ebenfalls im Standard-Datenschutzmodell

434 BVerfGE 120, 274 (306); 125, 260 (309). Vgl. hinsichtlich der informationellen Selbstbestimmung *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 11, 13; *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2, Rn. 149-150.

435 Erstmals 120, 274 (302 ff).

wieder, welches die deutschen Datenschutzbehörden auf Grundlage der DSGVO – insbesondere der Prinzipien gem. Art. 5 DSGVO – entworfen haben.[436] Wendet man den Blick ab von natürlichen Personen, könnten darüber hinaus sich auch juristische Personen des Privatrechts ob ihrer digitalen Identität auf verfassungsrechtliche Rechtsgüter berufen. Augenscheinlich kommen hierfür die Berufsfreiheit des Art. 12 Abs. 1 sowie die Eigentumsfreiheit des Art. 14 Abs. 1 GG in Betracht. Die Frage, ob sich juristische Personen des Privatrechts auch auf einen Teil der Schutzrichtungen des Allgemeinen Persönlichkeitsrechts berufen können, sei rekurrierend auf Kapitel B.I.2. erst später in digitalen Belangen näher auszuführen.[437] In technischer Hinsicht gilt für juristische Personen des Privatrechts allerdings das bereits für natürliche Personen erläuterte. Damit sind zunächst potentiell mehrere gefährdete Rechtsgüter ersichtlich, aus welchen sich eine Schutzpflicht ergeben könnte.

Werden nun diese abstrakten Werte ins Auge gefasst, bedarf es darüber hinaus einer Gefährdung der digitalen Identität in besagten Gütern. Dramatisch könnte hier nun „das Internet“ angeführt werden, was sich jedoch wegen der Mannigfaltigkeit der Szenarien jeglicher Konkretheit entzieht. Zielführender ist es dagegen, vorerst oberflächlich konkrete Szenarien zu betrachten: So könnte für die Gefahr der Vertraulichkeit von Daten durch Handlungen Dritter der Fortschritt auf dem Gebiet des Big Data herangezogen werden. Schon im Jahr 2010 erkannte das Bundesverfassungsgericht, dass die Verarbeitung der Daten zu einer Aufhebung der Vertraulichkeit und Privatsphäre führen kann,[438] wenngleich zu diesem Zeitpunkt die Technik der künstlichen Intelligenz noch nicht den aktuellen Stand erreicht hatte. Die Sammlung und Auswertung von Daten wird heute aber nicht – wie im damaligen Urteil – nur von Telekommunikationsanbietern übernommen, sondern vermehrt von privaten Unternehmen. Aufrufe von Webseite, die Verweildauer, das Aufrufen von Links bzw. die damit einhergehende Auswahl (sog. Clicks) – all dies wird analysiert und intern zu einer digitalen Identität zusammengefasst.

436 Zur Verankerung der Gewährleistungziele des Modells in der DSGVO siehe *Datenschutzkonferenz des Bundes und der Länder*, Das Standard-Datenschutzmodell (Version 1.1), S. 18 f.
437 Siehe Kapitel D.I.2.
438 BVerfGE 125, 260 (319).

Als Gefahr ergibt sich also nicht nur der bloße Kontrollverlust über die erhobenen Daten, sondern auch die Verarbeitung durch künstlicher Intelligenzen und anderen Algorithmen, welche wiederum eigene Risiken aufweisen. Beispielsweise greifen Art. 22 Abs. 1 und Erwägungsgrund 91 der DSGVO die bei der automatisierten Verarbeitung personenbezogener Daten zum Zwecke des Profilings auf und verweisen insbesondere auf eine Diskriminierung durch automatisierte Entscheidungsalgorithmen, was sich in einer Gefährdung des Gleichbehandlungsgrundsatzes aus Art. 3 Abs. 1 GG niederschlagen könnte.

Ferner sind digitale Identitäten auch mittelbar in der technischen Infrastruktur gefährdet. Es erscheint beispielsweise nicht ungewöhnlich, dass durch eine offengelegte digitale Identität ein Man-in-the-Middle-Angriff[439] auf Systeme innerhalb eines Unternehmens oder einem privaten WLAN-Netzwerk gelingen kann. Prominent wurde ein solches Vorgehen im Jahr 2018 im Rahmen des Angriffs der staatlichen Infrastruktur (sog. Bundeshack).[440] Ein solcher Übergriff auf die Daten Personen stellt insbesondere ein entsprechendes Risiko für das Unternehmen bzw. die juristische Person dar, wenn es zu einem digitalen Identitätsdiebstahl kommt. Schließlich könnten sich Leaks von Datensätzen neben den grundrechtlichen Beeinträchtigungen natürlicher Personen auf die Stellung des Unternehmens im Wettbewerb auswirken. Der daraufhin beschädigte Ruf riskiert insofern die berufliche Betätigung nach Art. 12 Abs. 1 GG und ggf. das Betriebseigentum iSd Art. 14 Abs. 1 GG in Form von Datensätzen.[441] Gefahren für verfassungsrechtliche Schutzgüter, sowohl informationell als auch technisch, sind damit vorerst hinreichend aufgezeigt.

439 Bei einem Man-in-the-Middle-Angriff handelt es sich um ein Szenario, bei welchem sich der Hacker als veritabler Mittler zwischen zwei kommunizierenden Schnittstellen ausgibt. Dadurch gelingt es dem Hacker, vertrauenswürdige Kommunikation mitzulesen und ggf. auch vollständig umzuleiten. Näher *Hellmann*, IT-Sicherheit, S. 35 ff.

440 Zur Vorgehensweise beim Bundestags-Hack 2015 siehe etwa https://www.heise.de/security/meldung/Bundestags-Hack-Angriff-mit-gaengigen-Methoden-und-Open-Source-Tools-3129862.html. Zur Lage im Falle des „Bundeshack 2018“ gibt es nur wenige Informationen, die dennoch auf eine ähnliche Vorgehensweise bzgl. der IVBB-internen Outlook-Server hindeutet.

441 Zum Zusammenspiel siehe vgl. *Axer* in: Epping/Hillgruber, BeckOK GG, Art. 14, Rn. 27.

Die verkürzte und nur oberflächliche Prüfung zeigt schon die Relevanz der Materie der digitalen Identität. Die digitale Identität als Schnittstelle für Systeme sowie in ihrer Gesamtheit als Ebenbild der analogen Persönlichkeit bedarf eines umfänglichen Schutzes vor Eingriffen Dritter gleichermaßen wie vor Eingriffen des Staates. Obschon an dieser Stelle keine konkreten Gefahren und Szenarien ausführlich dargestellt werden, zeigt sich die negative Seite der Digitalisierung und Vernetzung von Informationen schon an wenigen Beispielen. Prinzipiell ist die Schutzpflicht als verfassungsrechtliches Regulativ damit von besonderem Rang. Daraus kann aber nicht der Schluss gezogen werden, dass sich daraus die Lösung der obigen wie zukünftiger Risikoszenarien ableitet. Die stetige Fortentwicklung von Soft- und Hardware und die Facettenvielfalt des Internets ergeben nämlich ebenso ein Füllhorn an Handlungsmöglichkeiten des Staates.[442] Eine Verpflichtung zu einem bestimmten Handeln kann daher auch im Rahmen dieser Arbeit nicht festgestellt werden. Stattdessen werden im Folgenden geeignete und effektive Möglichkeiten aufgezeigt, soweit sich im Einzelfall eine konkrete Gefährdung des Grundrechts ergibt. Schließlich ist es Aufgabe der Schutzpflicht, typische (digitale) Problemlagen der heutigen Gesellschaft auch grundrechtstypisch zu betrachten und den Ruf nach der Gewährleistung grundrechtlicher Freiheit zu konkretisieren.[443]

IV. Das Zusammenwirken der subjektiv- und objektiv-rechtlichen Wirkdimensionen

Die Verfassung ist, wie dieses Kapitel zeigt, in ihrer Schutzwirkung als multidimensionales Schutzkonzept aufzufassen, das als Richtung – denn so will es Art. 1 Abs. 1 GG expressis verbis – den Schutz des Menschen und seiner Freiheit im Blick hat. Auf dem Boden der objektiv-rechtlichen Wirkdimension der Verfassung als solches wirken aus den einzelnen Grundrechten auch subjektiv-rechtliche

442 *Schliesky* et al., Schutzpflichten und Drittwirkung im Internet, S. 104.
443 Vgl. *Möstl*, DÖV 1998, 1029 (1030).

Aspekte hindurch. Darunter sind unter anderem der status negativus sowie status positivus der einzelnen Grundrechte einzuordnen. In deren Konnex ist ferner das Konzept der Schutzpflicht aufzunehmen, welche aufgrund ihres präventivhindernden Charakters[444] einen nahezu eigenständigen Wert erlangt. Die Verschmelzung der subjektiv- und objektiv-rechtlichen Gehalte führt als Konzept zu einem vollumfänglichen Schutz, der auch in Zukunft einen Schutz bieten soll und der dynamischen Interpretation des Grundgesetzes inherent ist.

Diese Interpretationsweise kommt, soweit dies vorläufig abstrakt festgestellt werden konnte, dem Begriff der digitalen Identität zugute. So kann dem status negativus als Abwehrfunktion der Grundrechte die Einschränkung der Nutzung digitaler Identitäten oder der unzulässigen Profilbildung im Rahmen hoheitlicher Tätigkeiten zugerechnet werden, jedoch nicht die Abwehr von Eingriffen zwischen Privaten. Der status positivus verweist in seiner teilhaberechtlichen Dimension dagegen auf die infrastrukturelle Gewährleistung der digitalen Identität, wohingegen eine Teilhabe an der Gleichbehandlung in Zugang und Nutzung digitaler Identitäten nur schwerlich ersichtlich ist. Verbleibende Lücken, wie jene gegenüber Privaten, sind entweder durch die Auffangwirkung von Grundrechten oder die Verpflichtung des Gesetzgebers zum beschützenden Einschreiten im Rahmen der Schutzpflichtenerfüllung zu schließen. Die fortschreitende Entwicklung im Bereich der Informatik, ein dadurch ausgelöster Verfassungswandel und die damit einhergehende neue Lesart von Generalklauseln spielen hierbei eine wichtige Rolle. Letztere deutet aber auf die Einzelfallbezogenheit hin, die im Rahmen bloß einer Untersuchung kaum abschließend beurteilt werden kann.

444 *Pietrzak*, JuS 1994, 748 (750)

D. Konkrete Schutzaspekte kraft Verfassungsrecht

Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses" Datum mehr.
– BVerfGE 65, 1 (45) – Volkszählung

Die bisherigen Ausführungen münden nun in der materiellen Auseinandersetzung mit den Grundrechtsgütern in digitalen Belangen. Wurde der Untersuchungsgegenstand bislang nur definitorisch (Kapitel B.) und abstrakt (Kapitel C.) umrissen, so ist nun zu zeigen, inwieweit die digitale Identität materiell von der Verfassung bereits umfasst oder erst im Wege der Auslegung der relevanten sachlichen Schutzbereiche hineinzulesen ist. Hierbei ist, wie bereits in Kapitel B.III. festgestellt, zwischen natürlichen Personen und juristischen Personen iSd Art. 19 Abs. 3 GG zu differenzieren. Weiter ist die Untersuchung materiell in einen informationellen bzw. datenmäßigen und in einen technischen Schwerpunkt aufzuteilen. Während in ersterem die Daten im Rahmen ihrer Verfügungsmacht und in ihrem Informationsgehalt betrachtet werden, bezieht sich der technische Aspekt auf informationstechnische Bezüge und deren grundrechtliche Einordnung.

I. Informationelle bzw. datenmäßige Betrachtungsweise

Zunächst ist sich der informationellen Betrachtung der digitalen Identität zu widmen, auch um die Grundlage für die darauffolgende technische Betrachtung zu schaffen. Im Mittelpunkt steht also die Betrachtung der digitalen Identität als Sammlung von Informationen iSv „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person“[445]. Es kommt daher vorliegend nicht auf die einzelne Information und beispielsweise ihr isoliertes Risiko für eine Verletzung des Schutzes personenbezogener Daten und der Rechte und Freiheiten der Identitätsinhaber an. Stattdessen ist auf die Kombination einzelner Informationen und daraus entstehende Synergien einzugehen, welche die digitale Identität besonders kennzeichnen.

1. Zur digitalen Identität natürlicher Personen

Vorrangig ist sich den Synergieeffekten der digitalen Identität einer natürlichen Person zuzuwenden. Verfassungsrechtlich kann dabei auf die bisher in der Rechtswissenschaft angewendeten Grundrechte bezüglich einzelner Informationen – namentlich das Allgemeine Persönlichkeitsrecht des Art. 2 Abs. 1 iVm 1 Abs. 1 GG – sowie einzelne sonstige Schutzgüter im Rahmen bestimmter, spezieller Grundrechtsausübung zurückgegriffen werden. In letzterem Fall sticht jedoch die rechtswissenschaftliche Diskussion im Rahmen des Rechts auf Dateneigentum gem. Art. 14 Abs. 1 GG heraus; ihr kommt daher eine umfangreichere Betrachtung zu. Ferner ist im Rahmen der Berufsfreiheit gem. Art. 12 Abs. 1 GG die im Aufkeimen zu begreifende Strömung zu betrachten, die auf personenbezogenen Daten basierende Ergebnisse von Algorithmen als Arbeitslohn und dementsprechend die Einspeisung von Daten als Tätigkeit diskutiert.

445 BVerfGE 65, 1 (42).

a) Allgemeines Persönlichkeitsrecht, Art. 2 Abs. 1 iVm 1 Abs. 1 GG

Das Allgemeine Persönlichkeitsrecht beinhaltet als „unbenanntes Freiheitsrecht“[446] mangels eines konkretisierenden Wortlauts oder anderer Anhaltspunkte jedoch keinen durchweg eigenen Grundrechtsgehalt, sondern besteht aus mehreren Teilaspekten. Es entspricht einem Konglomerat. Dies ist sowohl auf seine Herleitung[447] als auch die Subsidiarität[448] und Entwicklungsoffenheit (technisch wie materiell)[449] des Grundrechts zurückzuführen. Gemein ist jedoch allen Teilaspekten, dass sie im Kern der Selbstbewahrung, Selbstdarstellung oder Selbstbestimmung dienen.[450] Die jeweiligen Aspekte sind, sei es durch die Berücksichtigung im Rahmen der Verhältnismäßigkeit[451] oder die materielle Einordnung[452], durch die Dimensionen der Sphärentheorie geprägt. Neben einer Vielzahl an Fallgruppen, die auf Basis zivilgerichtlicher Rechtsprechung entstanden sind,[453] haben sich das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme herauskristallisiert und als eigenständige Grundrechte etabliert. Sie stehen

446 So BVerfGE 54, 148 (153) sowie *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2, 14 aE mwN; *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 64.

447 Hierzu (kritisch) *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2, Rn. 33.

448 Diese gilt jedoch nicht gegenüber der Handlungsfreiheit gem. Art. 2 Abs. 1 GG. Siehe *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 66; *Kloepfer*, VerfR II, § 56, Rn. 67.

449 In materieller Hinsicht BVerfGE 54, 148 (153 f); *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 229, 272; *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2, Rn. 17; *Degenhart*, JuS 1992, 361 (366, 368). Technisch dagegen stRspr BVerfGE 65, 1 (42); 113, 29 (46); 115, 166 (188); 115, 320 (341 f.); 118, 168 (184); 120, 378 (397); 130, 151 (183).

450 Vgl. *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2, Rn. 34.

451 Vgl. *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 4; *Degenhart*, JuS 1992, 361 (363 f); *Kloepfer*, VerfR II, § 56, Rn. 65, 92.

452 So sind für *Lang* in: Epping/Hillgruber, BeckOK GG, Art. 2, Rn. 35 ff die Inhalte der Sphärentheorie bereits zur Umschreibung der Schutzgehalte des Allgemeinen Persönlichkeitsrechts anzuwenden. Ähnlich auch *Kloepfer*, VerfR II, § 56, Rn. 51 f.

453 Zu den Ursprüngen in der Rechtsprechung siehe nur *Degenhart*, JuS 1992, 361 (362 f).

daher neben dem Allgemeinen Persönlichkeitsrecht als vollwertige Grundrechte auf gleicher Stufe.[454]

454 Zur informationellen Selbstbestimmung siehe *Kunig*, Jura 1993, 595 (603/604); *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I GG, Rn. 281, 334; *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 66 f; uneinheitlich eine Verselbstständigung einbeziehend *Dreier* in: Dreier, GG, Art. 2 I, Rn. 79. Dementgegen ablehnend BVerfGE 118, 168 (184); 120, 274 (311); BVerfG, Beschluss vom 23.10.2006 – Az. 1 BvR 2027/02 –, Rn. 27 nach juris = DuD 2006, 817 (818 f); *Murswiek* in: Sachs, GG, Art. 2, Rn. 68, 72; *Stern*, StaatsR IV/1, S. 231 f; *Kingreen/Poscher*, Staatsrecht II, Rn. 449 als Recht der Selbstdarstellung; *Luch*, Medienpersönlichkeitsrecht, S. 127 f; *Jandt* in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 17, Rn. 17; *Schertz*, NJW 2013, 721 (722, 724). Die Ablehnung des BVerfG hat sich jedoch mit Urteil vom 6.11.2019 – Az. 1 BvR 16/13 –, Rn. 84 zu einer ausdrücklichen Anerkennung als selbstständiges Grundrecht, wenn auch ohne nähere Begründung, gewandelt; bestätigt im Beschluss vom 25.2.2020 – Az. 1 BvR 1282/17 –, Rn. 6 mittels getrennter Benennung und Prüfung. Hinsichtlich des GGVIS befürwortend *Ambrock* in: Jandt/Steidle, Datenschutz im Internet, A.II., Rn. 39 aE; vgl. *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 208 f; sogar beide Ansichten bejahend *Herrmann*, GGVIS, S. 109 f; scheinbar auch BVerfG, Beschluss vom 8.6.2021 – 1 BvR 2771/18 –, Rn. 29. Dagegen ausschließlich als Ausprägung des Allgemeinen Persönlichkeitsrechts bezeichnend BVerfGE 120, 274 (313); BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, Rn. 307; *Murswiek* in: Sachs, GG, Art. 2, Rn. 68, 73c; *Hufen*, Staatsrecht II, § 12, Rn. 3 aE; *Kloepfer*, VerfR II, § 56, Rn. 97 aE; *Freimuth*, Gewährleistung der IT-Sicherheit, S. 149; *Jandt* in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 17, Rn. 20; *Luch*, MMR 2011, 75 (76); *Sachs*/*Krings*, JuS 2008, 481 (483). In beiden Fällen spricht gegen eine Einordnung als bloße Ausprägung die dogmatische Anwendung beider Grundrechte im Wege der Grundrechtskonkurrenzen: Bei der Abgrenzung zu Art. 10 und 13 GG treten beide Grundrechte stets als subsidiär auf, wobei die informationelle Selbstbestimmung wiederum lex specialis gegenüber der Vertraulichkeit und Integrität informationstechnischer Systeme ist – z.B. E 125, 260 (310). Dies stimmt zwar mit der generellen Konzeption des Allgemeinen Persönlichkeitsrechts überein, führt allerdings zu Schwierigkeiten in der Grundrechtsprüfung. Es erscheint widersprüchlich, einzelne Unterarten zueinander in ein Verhältnis des lex specialis/lex generalis zu setzen, die wiederum auf Basis eines auffangähnlichen Grundrechts fußen (so BVerfGE 120, 274 (313)), namentlich dem Allgemeinen Persönlichkeitsrecht. Gerät eine der beiden Ausprägungen in Kollision, würden schon keine Unterschiede im Schutzumfang der ausgeprägten Grundrechte bestehen. Ebenso bilden beide ein gemeinsames, sich ergänzendes Schutzkonzept. Sofern am Ausprägungsnormativ festgehalten würde, kann nur von einer Koexistenz und einem gleichberechtigten Zusammenwirken ausgegangen werden. Unterschiede bestehen aber sowohl hinsichtlich des Schutzbereiches als auch im Rahmen der Rechtfertigung. Gerade das GGVIS kennzeichnen Richtervorbehalt und Kernbereichsschutz seit BVerfGE 120, 274 (335 f); auch zeigt sich in der Definition des Schutzbereiches sub D.II.4. eine materielle Differenz. Die informationelle Selbstbestimmung ist zwar durch die Sphärentheorie beeinflusst, jedoch durch die aufgezeigten speziellen Anforderungen der Informations-, Auskunfts- und Berichtigungsrechte vielseitig ausstaffiert und erweitert. Qua verfassungsgerichtlicher Rechtsprechung hat sich eine ausführliche Spezifizierung ergeben, die unweigerlich eine Verselbstständigung beider ehemaligen Grundrechtsausprägungen erkennen lässt.

Folglich stehen diese Grundrechte mit ihrem informationellen Bezug zur digitalen Identität im Vordergrund der weiteren Untersuchung. Den übrigen Aspekten des Persönlichkeitsrechts kommt im Rahmen der Bearbeitung bloß ein ausfüllender Charakter zu, da sich im Ergebnis die Entwicklungsoffenheit des Allgemeinen Persönlichkeitsrechts per se auch auf die konkreten Ausprägungen der Selbstbewahrung, Selbstdarstellung und Selbstbestimmung erstrecken.

b) Das Grundrecht auf informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung des Art. 2 Abs. 1 iVm 1 Abs. 1 GG lässt sich mehrfach in diese Kategorien einordnen. Mit seiner Prämisse des Schutzes persönlicher bzw. personenbezogener Daten vor einer unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe[455] flankiert es sowohl den Aspekt der Selbstdarstellung als auch jenen der Selbstbestimmung, auf den zweiten Blick auch die Selbstbewahrung. Schließlich dient das grundrechtlich geschützte Handeln der selbstbestimmten Weitergabe von Daten insbesondere dazu, das eigene (auch digitale) Bild in der Gesellschaft zu beeinflussen.[456] Werden Daten bzw. Informationen bewusst zurückgehalten, schafft dies einen „informationellen Rückzugsort", der zugleich dem Aufrechterhalten von Intim- und Privatsphäre in der Informationsgesellschaft dient.[457] Zweckgemäß soll durch diese und andere Handlungsmöglichkeiten die Selbstbestimmung über den Verbleib und die Verwendung der Daten besonders geschützt werden. Andernfalls „kann [der Einzelne] in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden"[458]. Aus dem Grundrecht werden daher

455 BVerfGE 65, 1 (41 ff, 43); *Murswiek/Rixen* in: Sachs, GG, Art. 2 I, Rn. 72.

456 Vgl. *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 17; *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 43 f; *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 316 ff. Ein umfassendes Verfügungsrecht über die Darstellung in der Öffentlichkeit ist jedoch ausgeschlossen, vgl. BVerfGE 101, 361 (380).

457 Vgl. *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I GG, Rn. 331.

458 BVerfGE 65, 1 (43) – Einfügung durch den Bearbeiter.

Informations- bzw. Auskunfts-, Berichtigungs- und Löschungsrechte als angemessene Instrumente herausgelesen.[459] Eine Konkretisierung dieser ist bereits durch den deutschen (siehe §§ 32 ff BDSG) und europäischen (siehe Art. 5, 12 ff DSGVO) Gesetzgeber vorgenommen worden.

Anhand dieser Definition bleibt zu klären, ob der Schutzgegenstand entsprechend die digitale Identität einbezieht – begrifflich wie hermeneutisch – und inwiefern sich dies auf den sachlichen Schutzbereich der informationellen Selbstbestimmung auswirkt.

aa) Entwicklungsoffenheit des Schutzgegenstandes Für die Betrachtung des Schutzbereiches aus einem datenschutzrechtlichen wie digitalen Blickwinkel ist es im Vorfeld notwendig, den Schutzgegenstand herauszuarbeiten. Daher soll die Reichweite des Grundrechts bestimmt und die digitale Identität in ebendiese eingeordnet werden, indem vonseiten einfachgesetzlich vorgesehener Instrumente der informationellen Selbstbestimmung der verfassungsrechtliche Schutzbereich näher umrissen wird. Vor dem damit rechtlich und technisch gezeichneten Hintergrund ist auf den verfassungsrechtlichen Kern des Grundrechts und die Notwendigkeit des Schutzes aufgrund aktueller Gefahren einzugehen.

Die einstige Formulierung des Bundesverfassungsgerichts bei der Herausbildung des Grundrechts auf informationelle Selbstbestimmung wirkt heute missglückt, wenn „persönliche Daten“[460] als zu schützendes Gut definiert werden. Die Eigenschaft eines Datums, „persönlich“ zu sein, kann sich auch darin äußern, dass sie subjektiv verliehen wird und damit objektiv bzw. abstrakt nicht nachvollziehbar

459 Vgl. BVerfGE 65, 1 (46); 100, 313 (361); *Rudolf* in: Merten/Papier, HGr IV, § 90, Rn. 30, 46 ff; *Kunig*, Jura 1993, 595 (601). Gerade Berichtigungs- und Löschungsrechte bei unrichtigen Informationen sind auf das Allgemeine Persönlichkeitsrecht zurückzuführen. So finden sich dort im Falle der unrichtigen Berichterstattung der Medien entsprechende Möglichkeiten der Gegendarstellung – siehe nur BVerfGE 63, 131 (142 f) sowie *Bethge* in: Sachs, GG, Art. 5, Rn. 164 ff. Zur europarechtlichen Sicht des Selbstdatenschutzes siehe vgl. *Kamann/Braun* in: Ehmann/Selmayr, DSGVO, Art. 17, Rn. 8.

460 BVerfGE 65, 1 (42/43) – jedoch eigenständig anhand des Begriffs aus § 2 Abs. 1 BDSG a.F. definierend.

ist. Insofern ähnelt sie einem Affektionsinteresse[461] an Daten. Richtiger, und so auch im Datenschutzrecht berücksichtigt, sind *personenbezogene* Daten durch das Grundrecht geschützt. Als Daten sind dabei sowohl codierte als auch uncodierte Informationen zu bezeichnen. Handelt es sich um codierte Informationen, müssen diese stets interpretiert bzw. übersetzt werden,[462] beispielsweise von Maschinencode in für den Menschen lesbaren Informationen. Informationen ohne Codierung oder nach einer Decodierung sind dagegen „persönliche Lebenssachverhalte"[463], wie beispielsweise der Name oder das Geburtsdatum. Ferner sind auch innere Zustände (Meinungen, Wünsche, Motive) oder sachliche Umstände (Vermögensverhältnisse, Vertragsbeziehungen) unter diesen Begriff zu subsumieren.[464] Sie bedürfen keiner weiteren Interpretation. Es kommt folglich nicht darauf an, welcher Sphäre die Daten entstammen.[465] Sie müssen sich lediglich einer natürlichen Person wie dem Grundrechtsträger zuordnen lassen, entweder aufgrund ihres Informationsgehalts (z.B. vollständiger Name) oder durch weitere Möglichkeiten der Identifikation (z.B. Aggregation, Aussonderung oder Kombination).[466]

Wenngleich die Schutzbedürftigkeit der Grundrechtsträgers nicht nur auf den Fortschritt der Informationstechnik zurückzuführen ist[467], ist sich im Rahmen dieser Bearbeitung hauptsächlich dem Einfluss des digitalen Fortschritts auf die eingangs dargelegte Schutzrichtung zu widmen. Das einzelne Datum – oder die einzelne Information – als Teil der digitalen Identität stellt eine Aussage über persönliche Lebenssachverhalte dar, die vom Schutz des Grundrechts umfasst ist. Eine positive Ausübung der informationellen Selbstbestimmung unter Nutzung

461 Vgl. zur Begrifflichkeit *Oetker*, NJW 1985, 345 (346).

462 *Rudolf* in: Merten/Papier, HGr IV, § 90, Rn. 30; *Freimuth*, Gewährleistung der IT-Sicherheit, S. 66 f.

463 BVerfGE 65, 1 (42).

464 Vgl. *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1, Rn. 8; Art. 2 lit. a Datenschutz-RL 95/46/EG.

465 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 19. Vgl. auch BVerfGE 65, 1 (45) und E 120, 378 (399), wo von einer persönlichkeitsrechtlichen Einordnung anhand der Sensibilität des Datums Abstand genommen wird.

466 BVerfGE 65, 1 (43 f); zur Aggregation insbesondere BVerfG, Beschluss vom 10.11.2020 – Az. 1 BvR 3214/15 –, Rn. 71, 73. Vgl. auch Art. 4 Nr. 1 DSGVO.

467 So *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 73, der die informationelle Selbstbestimmung auch in der Aktenführung und ähnlichen analogen Vorgängen zutreffend anerkennt.

einfachgesetzlich verbürgter Rechte ist ohne Hindernisse möglich. Dies müsste sich jedoch auch auf die digitale Identität als Ganzes übertragen lassen. Dazu könnte sich zunächst der Idee des digitalen Persönlichkeitsrechts beliehen werden.[468] Auf Grundlage der Entwicklungsoffenheit des Allgemeinen Persönlichkeitsrechts[469] als gedanklich-historische Quelle sowie des Grundrechts auf informationelle Selbstbestimmung selbst[470] sind die Aspekte der Selbstbewahrung, Selbstdarstellung und Selbstbestimmung gegenüber neuen Technologien zu öffnen. Dies schließt gerade die neuen Formen der Datenverarbeitung und -speicherung ein, welche oftmals durch Fortschritt in Rechner-[471] oder Software-Architektur eingeleitet werden. Beispielhaft kann hier die „Wiederentdeckung" der künstlichen Intelligenz genannt werden, die jüngst auch in Form von eigenständigen Hardware-Chips in Smartphones und anderen Geräten ihren Platz findet.[472] So führte der zunehmende Einsatz der künstlichen Intelligenz zur automatisierten Entscheidungsfindung zur Fassung des Art. 22 DSGVO.[473] Zum Zwecke dieser (automatisierten) Datenauswertung durch Hard- oder Software werden die Datensätze auf Muster überprüft und vorsortiert bzw. aufbereitet, sodass es sich potentiell auch bei diesen verknüpften und geordneten Daten um digitale Identitäten handeln könnte. Jedoch, auch abseits dieser Art der Verarbeitung, steht die Profilbildung zur besseren Auffindbarkeit von Informationen im Fokus der Digitalisierung des informationellen Selbstbestimmungsrechts. Sind Informationen oder Daten nicht in einer für die Analyse bzw. Verarbeitung geeigneten Ordnung, steigt der Rechenaufwand in der Verarbeitung stark an – Soft- und Hardware

468 Hierzu grundlegend *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 45 f.
469 Siehe Fn. 449.
470 BVerfGE 65, 1 (41 f): „moderne Informationsverarbeitungstechnologien".
471 Dies meint beispielsweise den Aufbau von Prozessoren oder den Entwurf von Komponenten wie Arbeitsspeicher und Platine/Mainboard. Im Detail siehe *Hellmann*, Rechnerarchitektur, S. 4 f.
472 So beispielsweise Intel, die die Machine-Learning-Prozesse auf einen eigenständigen Prozessorkern auslagern – siehe nur https://newsroom.intel.com/editorials/intels-new-self-learning-chip-promises-accelerate-artificial-intelligence/.
473 Vgl. *Scholz* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 22 DSGVO, Rn. 8 f; *Buchner* in: Kühling/Buchner, DSGVO, Art. 22 DSGVO, Rn. 1.

arbeiten ineffizient oder gar entgegen dem beabsichtigten Zweck.[474] Demgemäß sortieren zum Beispiel Suchmaschinen die von Webseiten Dritter erlangten Informationen vor, um ein möglichst aufschluss- um umfangreiches Suchergebnis zu präsentieren.[475] Dabei kommt es regelmäßig vor, dass bei Eingabe eines vollständigen Namens ein „mehr oder weniger detailliertes Profil" entsteht, das zahlreiche Aspekte des Privatlebens enthält und deren Ermittlung und Zusammenstellung ohne die Suchmaschine kaum oder nur schwer hätte erfolgen können.[476] Die Verknüpfung einzelner personenbezogener Daten durch (private) Anbieter zu einem Profil ist daher von herausragender Bedeutung für das Persönlichkeitsrecht und die informationelle Selbstbestimmung[477], ohne dass es einer künstlichen Intelligenz bedarf. Technischer Fortschritt und (verfassungsrechtlicher) Datenschutz stehen sich in diesem Punkt mithin gegenüber, verhalten sich vereinzelt konträr zueinander. Dieses Spannungsverhältnis ist erst durch die einzelfallbezogene Verhältnismäßigkeitsprüfung aufzulösen, wodurch kollidierende Verfassungsgüter ein ein angemessenes Verhältnis gesetzt werden. Als Maßstab dient insbesondere das Machtgefälle zwischen Diensteanbieter und Nutzer. Die Privatsphäre des Nutzers, verfassungsrechtlich also jene Aussagen über Lebenssachverhalte mit Nähe zu Art. 1 Abs. 1 GG, ist daher von entsprechendem Gewicht in der Abwägung.[478] Pauschal kann nach der Rechtsprechung des EuGH[479] gelten: Je mehr Informationen bzw. personenbezogene Daten zu einem Profil oder einer anderen datenbankähnlichen Struktur zusammengeführt werden, desto sensibler und tiefgreifender ist

474 Zur Schätzung der Komplexität von Algorithmen bei der Analyse und Verarbeitung von Daten einschließlich ihrer Strukturierung im Allgemeinen siehe *Herold*/*Lurz*/*Wohlrab*, Grundlagen der Informatik, S. 380 ff.

475 Vgl. *Dörr*/*Natt*, ZUM 2014, 829 (835 f).

476 EuGH, Urteil vom 13.05.2014, Az. C-131/12, Rn. 37 f; vgl. auch BVerfG, Beschluss vom 6.11.2019 – Az. 1 BvR 16/13 –, Rn. 103, 139.

477 EuGH, Urteil vom 13.05.2014, Az. C-131/12, Rn. 80; BVerfG, Beschluss vom 10.11.2020 – Az. 1 BvR 3214/15 –, Rn. 71, 73.

478 EuGH, Urteil vom 13.05.2014, Az. C-131/12, Rn. 81. Vgl. auch *Kamann/Braun* in: Ehmann/Selmayr, DSGVO, Art. 17, Rn. 8; *Herbst* in: Kühling/Buchner, DSGVO, Art. 17, Rn. 69 unter Verweis auf EuGH, Urteil vom 9.3.2017, Az. C-398/15 – Manni –, Rn. 60. Ausführliche Kriterien aufstellend *Artikel 29-Datenschutzgruppe*, WP 225, S. 12 ff.

479 EuGH, Urteil vom 13.05.2014, Az. C-131/12, Rn. 37, 80; Urteil vom 21.12.2016, Az. C-203/15 u.a., Rn. 99; Urteil vom 5.6.2018, Az. C-210/16, Rn. 33 ff.

der Eingriff in das Allgemeine Persönlichkeitsrecht[480] bzw. das Grundrecht auf informationelle Selbstbestimmung[481]. Um diesem Risiko der Verfeinerung der Datensätze gewahr zu werden, muss der Nutzer als „Herr über seine Daten" auf den Verbleib einwirken können – unabhängig von einer Quantität oder Qualität des Datensatzes. Die Verknüpfung führt geradewegs dazu, dass bei Schutz des einzelnen personenbezogenen Datums erst recht auch die verknüpfte (digitale) Identität mit seinem Aussagegehalt auf Basis des Gehaltes der Einzeldaten dem verfassungsrechtlichen Schutz unterliegen muss.

Ein weiterer Ansatzpunkt zu Gunsten der Anwendung des Grundrechts hinsichtlich verknüpfter Datensammlungen iSv digitalen Identitäten findet sich im Konstrukt der Datenportabilität. Entstanden ist dieses erst im Rahmen der Verhandlungen zur DSGVO ohne eine vorhergehende Entsprechung in der EU-Datenschutz-RL 95/46/EG. Dahinter verbirgt sich, wie Art. 20 Abs. 1, Abs.2 sowie Erwägungsgrund 68 der DSGVO näher erläutern, die Öffnung bestehender Dienste zu Austausch und Übertragung von personenbezogenen Daten. So sollen personenbezogene Daten in einem „strukturierten, gängigen und maschinenlesbaren Format"[482] entweder dem Nutzer bzw. der betroffenen Person[483] selbst zur Verfügung gestellt werden (sog. indirekte Weitergabe) oder unmittelbar an einen anderen Diensteanbieter bzw. Verantwortlichen geleitet werden (sog. direkte Weitergabe).[484] Auf diese Weise soll die betroffene Person „eine bessere Kontrolle über die eigenen Daten haben"[485]. Der Fokus liegt damit deutlich auf der informationellen Selbstbestimmung über den Verbleib der Daten, vorausgesetzt die vorangegangene Weitergabe der Daten erfolgte bewusst auf Basis einer Einwilligung oder eines Vertrages – vgl. Art. 20 Abs. 1 lit. a und b DSGVO. Eine

480 Vgl. BVerfG, Beschluss vom 6.11.2019 – Az. 1 BvR 16/13 –, Rn. 121 ff. Jedoch trennt das BVerfG die Daten-Ebene der informationellen Selbstbestimmung vom Allgemeinen Persönlichkeitsrecht – Rn. 91.

481 BVerfG, Beschluss v. 10.11.2020 – Az. 1 BvR 3214/15 –, Rn. 96, 109.

482 Art. 20 Abs. 1 DSGVO.

483 Als solche gilt gem. Art. 4 Nr. 1 DSGVO jede Person, die Rechte bezüglich ihrer (personenbezogenen) Daten geltend macht.

484 Zu den Arten der Weitergabe *Kamann/Braun* in: Ehmann/Selmayr, DSGVO, Art. 20, Rn. 1. Als Zweistufenmodell darstellend *Strubel*, ZD 2017, 355 (356).

485 ErwGr 68, S. 1 DSGVO.

Förderung dieser Erweiterung der Selbstbestimmungsmöglichkeiten ergibt sich durch die obligatorische Formulierung der Norm, die durch die Durchsetzbarkeit bei Zuwiderhandeln gem. Art. 77, 79 DSGVO noch verstärkt wird.[486] Die daraus entstehende Zwangslage soll die Verantwortlichen dazu „motivieren", interoperable Formate zu entwickeln[487] oder bestehende Schnittstellen auch für andere Anbieter mit gängigen Formaten zur Verfügung zu stellen.[488] Die Wirkung der Norm entfaltet sich so nicht nur datenschutzrechtlich oder zu Gunsten der informationellen Selbstbestimmung, sondern weist auch eine wettbewerbs- und binnenmarktpolitische Zielsetzung auf.[489] Durch die Öffnung der Schnittstellen sollen insbesondere sog. Lock-In-Effekte[490] und eine marktbeherrschende Stellung aufgelöst werden.[491] Schließlich würde so der Aufwand für einen Wechsel zwischen verschiedenen Anbietern (sog. Wechselkosten) verringert und mittelbar

486 Vgl. *Sperlich*, DuD 2017, 377. Zu weiteren Möglichkeiten siehe *Kamann/Braun* in: Ehmann/Selmayr, DSGVO, Art. 20, Rn. 46.

487 ErwGr 68, S. 2 DSGVO sowie vgl. *Sperlich*, DuD 2017, 377.

488 Zu letzterem sei angemerkt, dass ErwGr 68 S. 7 DSGVO auf eine Unterscheidung zwischen kompatiblen und interoperablen Datensystemen hinweist. Im Fokus der DSGVO steht damit das interoperable System, das die Datenübertragbarkeit in der Konzeption bereits berücksichtigt. Vgl. definiert ISO/IEC 2382-01 den Begriff als „The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units." Gegensätzlich gilt als Kompatibilität „The capability of a functional unit to meet the requirements of a specified interface without appreciable modification." Folglich ist Art. 20 Abs. 1, Abs. 2 DSGVO ist so zu verstehen, dass die Einrichtung von Dateisystemen, die bloß mit bestehenden Verarbeitungssystemen kompatibel sind, nicht ausreicht. Vielmehr bedarf es eines eigenen Standards, der wohlweislich von branchentypischen Faktoren beeinflusst wird – vgl. nur *Artikel 29-Datenschutzgruppe*, WP 242 rev.01, S. 17.

489 Scheinbar als vorwiegende Zielrichtung sehend *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, § 4, Rn. 19; ähnlich als „möglicherweise überwiegend" herausstellend *Kamann/Braun* in: Ehmann/Selmayr, DSGVO, Art. 20, Rn. 3. Darauf deutet ebenfalls *Jülicher/Röttgen/von Schönfeld*, ZD 2016, 358 (360) hin und verweist auf die Historie der Norm. Dagegen *Herbst* in: Kühling/Buchner, DSGVO, Art. 20, Rn. 4, welcher die datenschutzrechtliche Wirkung „allenfalls als Nebeneffekt" einordnet.

490 Zum Begriff siehe *Conrad/Licht* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 39, Rn. 475 sowie zur Entstehung von Wechselkosten siehe *Podszun/Schwalbe*, NZKart 2017, 98 (100).

491 *Strubel*, ZD 2017, 355 (355, 359).

der Wettbewerb zwischen den Marktteilnehmern gefördert.[492] In der Materie des Verfassungsrechts kommt diese Wirkung der informationellen Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG zugute, speziell für die digitale Identität: Beginnend bei der Terminologie des Instruments, verweist der Wortlaut des Art 20 Abs. 1 DSGVO auf eine datenbankmäßige Struktur mehrerer personenbezogener Daten; die Daten sind *strukturiert* und *maschinenlesbar*.[493] Die digitale Identität zeichnet gerade ihre Sortierung und Verkettung der (personenbezogenen) Daten aus.[494] Wird der Anspruch aus Art. 20 Abs. 1 DSGVO also geltend gemacht, erhält der Begehrende ein Abbild seiner digitalen (Teil-)Identität beim Anbieter und verfügt auf diese Weise über die Daten. Es handelt sich jedoch nur um ein Abbild, da das Recht auf Datenportabilität nur die (indirekte oder direkte) Weitergabe regelt.[495] Es kann sich schon technisch nicht um „Originaldaten" handeln, wenn Daten unbegrenzt vervielfältigt werden können. Das Löschungsrecht bleibt insofern bestehen und muss für einen vollständigen Anbieterwechsel ohne Datenspuren eigenständig ausgeübt werden, Art. 20 Abs. 3 S. 1 DSGVO. Dies schadet allerdings nicht der informationellen Selbstbestimmung, sondern begünstigt sie durch die entstehende Wahlfreiheit.[496] Eine unmittelbare Kopplung von Wechsel und Löschung entspräche zwar dem Ansatz der Datenminimierung. Sodann würde allerdings nicht dem Willen des Betroffenen bzw. Dateninhabers entsprochen, der jedoch inherent im Mittelpunkt des Grundrechts auf informationelle Selbstbestimmung steht. Zusammengefasst dienen die aufgezeigten Regelungen insbesondere,

492 Vgl. *Kamann/Braun* in: Ehmann/Selmayr, DSGVO, Art. 20, Rn. 3; *Albrecht*/*Jotzo*, Das neue Datenschutzrecht der EU, § 4, Rn. 20; *Jülicher*/*Röttgen*/*von Schönfeld*, ZD 2016, 358 (360); *Artikel 29-Datenschutzgruppe*, WP 242 rev.01, S. 5.

493 Der Begriff „maschinenlesbar" ist durch ErwGr 21 RL 2013/37/EU definiert: „Ein Dokument sollte als maschinenlesbar gelten, wenn es in einem Dateiformat vorliegt, das so strukturiert ist, dass Softwareanwendungen die konkreten Daten einfach identifizieren, erkennen und extrahieren können. In Dateien verschlüsselte Daten, die in maschinenlesbarem Format strukturiert sind, sind maschinenlesbare Daten. Maschinenlesbare Formate können offen oder geschützt sein; sie können einem formellen Standard entsprechen oder nicht. Dokumente, die in einem Dateiformat verschlüsselt sind, das eine automatische Verarbeitung einschränkt, weil die Daten nicht oder nicht ohne Weiteres aus ihnen extrahiert werden können, sollten nicht als maschinenlesbar gelten."

494 Siehe hierzu die Definition in Kapitel B.I.4.

495 Vgl. *Jülicher*/*Röttgen*/*von Schönfeld*, ZD 2016, 358 (360).

496 Im Ergebnis so auch *Jülicher*/*Röttgen*/*von Schönfeld*, ZD 2016, 358 (360/361).

mit den Worten der Artikel-29-Datenschutzgruppe ausgedrückt, „[...] to *empower* data subjects regarding their own personal data [...]“.[497]

Die aufgezeigten Ansätze können allerdings nur als Indizien gelten, da sich das Verfassungsrecht per se nicht aus dem einfachen Recht definiert. Vielmehr stellt das einfachgesetzliche Recht die Konkretisierung der verfassungsrechtlich gewährten Spielräume dar. Es ist daher notwendig, die erwähnten Indizien auf den verfassungsrechtlichen Boden des informationellen Selbstbestimmungsrechts zu stellen, unter Einbeziehung der eingangs erwähnten Entwicklungsoffenheit des Grundrechts. Überdies ist das Grundrecht im Licht des Europarechts zu begreifen.[498] Dies gebietet sich schon nach jüngster Rechtsprechung des Bundesverfassungsgerichts[499], sofern der DSGVO aufgrund ihrer Regelungsform als Verordnung ein vollharmonisierender Charakter zugesprochen wird[500]. Ob letzteres der Fall ist kann vorliegend jedoch dahingestellt bleiben, wo der unionsgrundrechtliche wie verfassungsrechtliche Gehalt der Datenschutzgrundrechte weitgehend übereinstimmt[501]. Das Grundrecht auf informationelle Selbstbestimmung ist demgemäß um die Aspekte des Grundrechts auf Datenschutz gem. Art. 8 GrC sowie

497 *Artikel 29-Datenschutzgruppe*, WP 242 rev.01, S. 4 – Hervorhebung im Original nicht enthalten. Ähnlich auch ErwGr 68, S. 1 DSGVO.

498 Andernfalls käme es zu einer Kollision zwischen Verfassungsrecht und EUV/AEUV. Insofern ist die Auslegung auch zu Gunsten des Anwendungsvorrangs unionsrechtskonform vorzunehmen – vgl. *Ruffert* in: Calliess/Ruffert, EUV/AEUV, Art. 1 AEUV, Rn. 24.

499 Grundlegend BVerfG, Beschluss vom 6.11.2019 – Az. 1 BvR 276/17 –, Rn. 42 ff. Hierauf bezugnehmend BVerfG, Urteil vom 19.5.2020 – Az. 1 BvR 2835/17 –, Rn. 84 sowie Beschluss vom 27.5.2020 – Az. 1 BvR 1873/13 u.a. –, Rn. 83 ff.

500 In der Literatur wird, ausgehend von der versuchten Harmonisierung der DS-RL 95/46/EG (siehe ErwGr 3 DSGVO) sowie ErwGr 10 DSGVO, insgesamt regelmäßig von einer Vollharmonisierung ausgegangen – siehe nur *Schantz* in: Wolff/Brink, BeckOK DatenschutzR, Art. 1 DSGVO, Rn. 8 f, wohl zweifelnd *Buchner* in: Kühling/Buchner, DSGVO, Art. 1, Rn. 5. In einzelnen Öffnungsklauseln der DSGVO besteht dagegen Uneinigkeit, wie beispielsweise für den Beschäftigtendatenschutz des Art. 88 DSGVO – exemplarisch zum Begriffsverständnis der „spezifischeren Vorschriften“ *Maschmann* in: Kühling/Buchner, DSGVO, Art. 88 DSGVO, Rn. 29 ff. Ob für die Betrachtungsweise des BVerfG dennoch eine punktuelle Betrachtung der Öffnungsklauseln und der konkrete Derogationsspielraum vorzunehmen ist, oder ob dies dem Ziel des gleichwertigen Schutzniveaus der DSGVO (vgl. ErwGr 10) zuwider ist, zeichnet sich bis zuletzt weder in Rechtsprechung noch Literatur ab.

501 Vgl. *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 8 GRC, Rn. 12 ff; *Knecht* in: Schwarze, EU-Kommentar, Art. 8 GRC, Rn. 4 ff. Ebenso *Roßnagel*, NJW 2019, 1 (2) unter Verweis auf *Kingreen* in: Calliess/Ruffert, EUV/AEUV, Art. 7 GrC, Rn. 4, 10.

das europäische Grundrecht auf informationelle Selbstbestimmung aus Art. 7, 8 GrC[502] zu erweitern.[503] So „mutiert" das weit zu verstehende Grundrecht auf informationelle Selbstbestimmung mittels Europäisierung ebenfalls zum Datenschutzgrundrecht.[504] Signifikante Merkmale der Ausübung der informationellen Selbstbestimmung sind schon durch den Wortlaut die Einwilligung und Zweckbindung der Datenverarbeitung (Art. 8 Abs. 2 S. 1 GrC) sowie die erwähnten Berichtigungs- und Auskunftsansprüche (Art. 8 Abs. 2 S. 2 GrC) umfasst.[505] Diese Erfordernisse an eine Datenverarbeitung wurden schon früh bei der Schöpfung des Grundrechts auf informationelle Selbstbestimmung berücksichtigt und herausgestellt. Aus- und Verwertung eines Datums „hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab."[506] Dieser Verwendungszusammenhang determiniert bereits Informationsbeschaffung und -verarbeitung, einschließlich ihrer Intensität.[507] Verbunden mit dem Zweckerfordernis ist zugleich ein Mindestmaß an Transparenz, die im Rahmen der (informierten) Einwilligung über ebendiese Zwecke aufklärt. Anderenfalls wird „der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über [ihn] weiß"[508] – die Souveränität der Entscheidung kann mit abnehmender Informiertheit bezweifelt werden. Mangelt es an einer – mittlerweile obligatorischen, vgl. Art. 12 Abs. 1 DSGVO – Aufklärung im Vorfeld, so muss dem Grundrechtsträger die Möglichkeit zur Einforderung der

502 *Roßnagel*, NJW 2019, 1 (2); *Klement* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 7 DSGVO, Rn. 19; *Marsch*, Das europäische Datenschutzgrundrecht, S. 208 f.

503 Zur europarechtsfreundlichen Lesart des Grundrechts auch *Hufen*, Staatsrecht II, § 4, Rn. 11; *Lenaerts*, EuR 2012, 3 (14 f); *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 8 GrC, Rn. 4; *von Grafenstein*, The Principle of Purpose Limitation in Data Protection Laws, S. 111 ff.

504 *Britz*, EuGRZ 2009, 1 (5 f).

505 Zu beiden Prinzipien ausführlich *Marsch*, Das europäische Datenschutzgrundrecht, S. 157-177.

506 BVerfGE 65, 1 (45). Ferner zum Grundsatz der Offenheit der Erhebung und Nutzung personenbezogener Daten BVerfGE 125, 260 (335/336).

507 *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I GG, Rn. 331.

508 BVerfGE 65, 1 (43).

Informationen gegeben werden. Dies ist nicht zuletzt sinnvoll, um das im Verhältnis zwischen Privaten auftretende Ungleichgewicht[509] bestmöglich aufzulösen und das liberale Menschenbild der Verfassung aufrechtzuerhalten; es begünstigt die digitale Souveränität[510]. Mit der Konnexität von Zweckbindung und Informationstechnologie wird aber zugleich die Dynamik und Entwicklungsoffenheit fest in die rechtliche Würdigung eingebunden. Sie muss nach dem weiten Begriffsverständnis[511] auch zugunsten des bereichsdogmatischen Ausbalancierens[512] umfangreich verstanden werden, also nicht nur im technologischen Sinne. Entwicklungsoffen bedeutet auch, dass neue Kommunikationsformen und -arten oder Trends im Sinne einer vorübergehenden Erscheinung geschützt sind. Ebenso müssen von der Grundrechtsnorm aktuelle Instrumente des Gesetzgebers umfasst sein, wenn diese dem Schutzzweck der informationellen Selbstbestimmung dienen. Eine Öffnung von technischen Schnittstellen, die staatliche Normierung oder Gewährleistung sicherer Kommunikationsprotokolle über ein Audit oder Möglichkeiten der Regulierung eines datenschutzrechtlichen level playing field sind demgemäß als Konkretisierung zu sehen. Neben Zweckbindung und Transparenz tritt folglich die Entwicklungsoffenheit als Gradmesser der informationellen Selbstbestimmung. Darüber hinaus – so zumindest die Datenschutzkonferenz[513]

509 Hierzu *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I GG, Rn. 345 f.

510 Zum Begriff *BITKOM*, DuD 2018, 294 (296), jedoch ohne verfassungsrechtlichen bzw. juristischen Bezug. Dieser wird mittelbar durch *Fox*, DuD 2018, 271 und *Beyerer*/*Müller-Quade*/*Reussner*, DuD 2018, 277 (278) aufgegriffen. So versteht *Fox*, DuD 2018 gerade Kompetenz und Verständnis eines „aufgeklärten" Kunden hierunter, was mit dem (datenschutzrechtlichen) Konstrukt der informierten Einwilligung übereinstimmt. Spezifischer arbeiten *Beyerer*/*Müller-Quade*/*Reussner* Kriterien der Infrastruktur-, Daten-, Entscheidungs- und Plattformsouveränität heraus. *Hackenjos*/*Mechler*/*Rill*, DuD 2018, 286 (286 f) legen den Schwerpunkt dagegen in der IT-Sicherheit, um die Selbstbestimmtheit entsprechend technisch zu schützen. Dieser Ansatz wird durch den Beitrag von *Broadnax* et al. durch konkrete Vorschläge für Hard- und Software gestützt – *Broadnax* et al., DuD 2018, 74 (76 f). Der Beitrag von *Lambach*/*Oppermann*, Governance 2022, 1 (6 ff) zeigt aber, dass der Begriff für verschiedene Narrative steht, von denen die datenschutzrechtliche Facette nur eine ist.

511 Vgl. BVerfGE 65, 1 (41): „Die bisherigen Konkretisierungen durch die Rechtsprechung umschreiben den Inhalt des Persönlichkeitsrechts nicht abschließend.".

512 Siehe C.III.1.

513 *Datenschutzkonferenz des Bundes und der Länder*, Das Standard-Datenschutzmodell (Version 1.1), S. 17 – nicht mit in neuere Fassung übernommen.

– sind auch die Erforderlichkeit der Datenverarbeitung (einschließlich Datenminimierung)[514], der Grundsatz der Intervenierbarkeit[515] der Datenverarbeitung sowie die Sicherheit der Verarbeitungsvorgänge[516] auf das Volkszählungsurteil des Bundesverfassungsgerichts zurückzuführen. Jeweils nähren sie sich aus der verfassungsrechtlichen Selbstbestimmung des Art. 2 Abs. 1 iVm 1 Abs. 1 GG, forcieren die quantitative wie qualitative Entscheidungsfreiheit bzw. Souveränität des Individuums. Die Freiheit, im digitalen Raum „zu tun und zu lassen, was die Rechte anderer nicht verletzt“[517] und „in freier Selbstbestimmung als Glied einer freien Gesellschaft“ zum Schutz von Wert und Würde[518] zu handeln, ist von hohem Wert. Ob digital oder analog, die Selbstbestimmung bezweckt als elementarer Bestandteil der freiheitlichen und demokratischen Gesellschaft eine Stärkung des Gemeinwesens.[519] Umso mehr muss der verfassungsrechtliche Schutz auch Gefahren und Risiken neuer Arten der Datenverarbeitung abwehren. Ein anderes Verständnis wäre mit einer der Digitalisierung zeitgemäßen „Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar“[520], sodass datenschutzrechtliche Prinzipien wie das Gebot der Zweckbindung sowie das Gebot der Bestimmtheit und Klarheit (bzw. Transparenz) in die Prüfung der Verhältnismäßigkeit i.e.S. Eingang gefunden haben[521].

514 Siehe nur BVerfGE 65, 1 (46), fortgeführt in E 125, 260 (333).

515 Wohl in BVerfGE 65, 1 (42 f), wenn in „wann und innerhalb welcher Grenzen“ sowie die darauffolgenden Ausführungen zur Selbstbestimmung auch die Kehrseite der Einwilligung – der Widerruf – hineingelesen wird.

516 Wohl in BVerfGE 65, 1 (49): „Zur Sicherung des Rechts auf informationelle Selbstbestimmung bedarf es ferner besonderer Vorkehrungen für Durchführung und Organisation der Datenerhebung und Datenverarbeitung[...].“ Möglicherweise besteht in dieser Hinsicht auch ein Schutz durch das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, wie unter D.II.4. vertiefter erörtert wird.

517 *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2 I, Rn. 13 unter Verweis auf den Entwurfstext des Art. 2 Abs. 1 GG.

518 BVerfGE 65, 1 (41).

519 *Giesen*, JZ 2007, 918 (921 f).

520 Vgl. BVerfGE 65, 1 (43).

521 BVerfG, Beschluss v. 27.5.2020 – Az. 1 BvR 1873/13 –, Rn. 127 ff.

Hohe Risiken für das Grundrecht ergeben sich allerdings auch aus dem Umgang mit sog. Identitätsdatenleaks und Übergriffe von Seiten Privater. Sind umfängliche, vollständige Datensätze mit Identitätsdaten öffentlich und im Klartext im Internet einsehbar, geht damit sowohl ein entsprechendes Missbrauchspotential als auch eine daraus resultierende Gefahr für Grundrechtsgüter einher. Insofern sei zuletzt bezüglich der Öffnung der informationellen Selbstbestimmung für den Schutz der digitalen Identität die in diesem Fall be- und entstehende grundrechtliche Schutzpflicht herauszustellen.[522] Ausgangspunkt hierfür ist das nicht mehr nur das Gefahrenpotential, sondern die faktische Beeinträchtigung – wie sich an den seit dem Jahr 2018 vermeldeten Identitätsdatendiebstählen erkennen lässt: 500 000 Nutzerkonten bei einem Online-Rollenspiel[523], Datensätze von etwa 124 000 Hotelgästen[524] zuzüglich der Daten von 500 Millionen Hotelgäste der Mariott-Hotelkette[525], der Kundendatensatz des Domain-Anbieters DomainFactory[526] und 1,9 Millionen Passwörter wurden im Klartext veröffentlicht[527]. Besonders gravierend war der Datendiebstahl von sog. Access Token[528] bei Facebook, der etwa 50 Millionen Nutzer betrifft,[529] sowie die Offenlegung von 419 Millionen Mobiltelefonnummern mit dazugehörigen Profilidentifikationsnummern[530]. Die Liste lässt

522 Zu den Kriterien der Schutzpflichtenprüfung siehe Kapitel C.III.1.

523 Siehe https://www.heise.de/security/meldung/Datenleck-bei-Mortal-Online-Kriminelle-boten-500-000-Nutzeraccounts-zum-Kauf-an-4154668.html.

524 Siehe https://www.heise.de/security/meldung/Datenleck-bei-FastBooking-Hacker-klauen-Daten-von-ueber-124-000-Hotelgaesten-4093080.html.

525 Siehe https://www.heise.de/security/meldung/Marriott-Daten-von-500-Millionen-Hotelgaesten-abgegriffen-4236576.html.

526 Siehe https://www.heise.de/newsticker/meldung/Datenleck-bei-Domainfactory-Hacker-knackt-Systeme-laesst-Kundendaten-mitgehen-4102881.html.

527 Siehe https://netzpolitik.org/2018/jugendgefaehrdend-millionen-passwoerter-von-knuddels-de-standen-offen-im-netz/.

528 Ein Access Token wird erstellt, wenn der Nutzer sich durch ein Programm (z.B. eine Drittanbieter-App) bei einem Dienst anmeldet. Der Token dient dann als Zertifikat, welches Informationen zur (positiven) Berechtigung der Dienstenutzung enthält. Je nach Programmierung enthält der Token auch die Login-Daten, also Benutzername und Passwort. Vertiefend hierzu siehe *Eckert*, IT-Sicherheit, S. 702 f sowie zum OAuth-Verfahren *Petrlic*/*Sorge*, Datenschutz, 72/73.

529 Siehe https://www.heise.de/newsticker/meldung/Fast-50-Millionen-Facebook-Nutzer-von-Hacker-Angriff-betroffen-4178529.html.

530 Siehe https://netzpolitik.org/2019/419-millionen-betroffene-datenleck-bei-facebook-gab-handynummern-preis/.

sich nahezu unendlich fortführen, z.B. mit dem Leak bzw. Doxing von Login-Daten und weiteren privaten Daten von Prominenten und Bundestagsabgeordneten durch den Hacker „g0d“ bzw. „0rbiter“[531] und den umfangreichen Datenleak der Collection 1 bis 5, welcher 2,2 Milliarden Accounts umfasst[532]. Grundsätzlich enthalten diese Datensammlungen nicht nur um bloße Login-Daten, sondern unter Umständen detailreiche Datensätze mit Bank- und Adressdaten[533] oder Informationen zur sexuellen Identität und anderen besonderen personenbezogenen Daten iSd Art. 9 Abs. 1 DSGVO. Es ist also von einem hohen Schadensumfang auszugehen, da bei derartig reichhaltigen Datensätzen auch Fälle des Identitätsdiebstahls auftreten. Allerdings dürfen den Betroffenen bei solchen Vorfällen keine Maßnahmen zum Selbstschutz[534] entgegengehalten werden, um die grundrechtliche Schutzbedürftigkeit zu mindern oder erst zu aktivieren. Die Schwelle ist für technische Sicherheitsmaßnahmen zum Selbstdatenschutz nicht hoch anzusetzen, sodass Expertenkenntnisse wie das Einrichten und Nutzen von VPN-Verbindungen oder abseits der vom Betriebssystem vorgehaltenen Verschlüsselungstechniken nicht erwartet werden können. Ähnlich kritisch zu beobachten ist die Notwendigkeit, die eigenen Daten durch die Angabe von sog. Fake-Daten – also durch bewusst falsche Angaben – zu schützen.[535] Stattdessen sollten neben einem Bewusstsein für den Umgang oder die Weitergabe von Daten die bekannten Hinweise für die Nutzung von Passwörtern oder zur sicheren Kommunikation über das Internet[536] beachtet werden. Eine entsprechende Sensibilisierung kann sowohl durch die Datenschutzbehörden (Art. 57 Abs. 1 lit. b DSGVO) als auch den Diensteanbieter erfolgen, der bereits zum Ermöglichen einer datensparsamen und – wenn möglich

531 Siehe nur https://www.heise.de/newsticker/meldung/Massen-Doxxing-Beschuldigter-soll-Passwoerter-teilweise-im-Darknet-gekauft-haben-4270379.html.

532 Siehe https://www.heise.de/security/meldung/Neue-Passwort-Leaks-Insgesamt-2-2-Milliarden-Accounts-betroffen-4287538.html.

533 Siehe beispielsweise die Auflistung der im DomainFactory-Leak enthaltenen Daten unter https://www.heise.de/forum/heise-online/News-Kommentare/Datenleck-bei-Domainfactory-Hacker-knackt-Systeme-laesst-Kundendaten-mitgehen/Folgende-Datenfelder-waren-in-der-DB/posting-32665013/show/.

534 Einige Ansätze einschließlich der Verwendung von Leak Checkern aufzeigend *Eikenberg*, c't 5 (2019), 32 ff.

535 Hierzu ausführlich *Schnabel*/*Freund*, CR 2010, 718 ff.

536 Beispielsweise *Karaboga* et al., White Paper Selbstdatenschutz, S. 20 ff.

– pseudonymen Nutzbarkeit des Angebots angehalten ist (Art. 25 Abs. 1, 32 Abs. 1 DSGVO). Umfangreiche Identitätsdatendiebstähle sowie Leaks der Datensätze sind zudem oftmals nicht auf das Verschulden der Nutzer, sondern auf technische Mängel oder unzureichende Schutzmaßnahmen des Diensteanbieters zurückzuführen. Selbst effektivste Maßnahmen zum Selbstschutz können die Mängel in der technischen Infrastruktur nicht beheben.[537] Einer Schutzbedürftigkeit der Nutzer steht daher nichts in diesem Dreiecksverhältnis entgegen. Demgemäß besteht eine Gefährdung grundrechtlicher Interessen vonseiten Privater, die aufgrund ihrer Schadensqualität ein Handeln des Staates notwendig erscheinen lässt; eine Schutzpflicht aus dem Grundrecht auf informationelle Selbstbestimmung liegt vor. Der Erfüllung dieser Pflicht ist der Gesetzgeber aber bereits nachgekommen, sowohl präventiv als auch repressiv. Letzteres kann auf die Straftatbestände gem. §§ 202a ff StGB, insbesondere der Datenhehlerei, und den (Identitäts-)Betrug gem. § 262 Abs. 1 StGB gestützt werden. Einer Ausweitung des Missbrauchsrisikos rechtswidrig erlangter Identitätsdaten wirken die erst jüngst erlassenen Meldepflichten für verantwortliche Unternehmen sowohl an die zuständige Datenschutzbehörde (Art. 33 DSGVO) als auch die betroffene Person (Art. 34 DSGVO) entgegen. In umfangreichen Fällen kann allerdings auch auf eine Information durch öffentliche Bekanntmachung erfolgen, also Meldung über weit verbreitete Medienangebote wie Rundfunk oder Online-Presse.[538] Darüber hinaus gelten besondere Meldepflichten für digitale Dienste (§ 8c Abs. 3 S. 1 BSI-G) und kritische Infrastrukturen (§ 8b Abs. 4 BSI-G) iSd § 2 Abs. 10, 11 BSI-G. Dies befreit den Gesetzgeber jedoch nicht von der stetigen Aufgabe im Rahmen der grundrechtlichen Schutzpflichten, diese auch fortwährend zu überwachen und bei mangelhafter Wirkung entsprechend nachzubessern.

In der Gesamtschau spricht eine Vielzahl der Argumente für eine Einordnung der digitalen Identität in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung. Würde gegensätzlich und so entgegen der prädestinierten Entwicklungsoffenheit der informationellen Selbstbestimmung argumentiert, dann

537 Vgl. auch BVerfGE 120, 274 (306); *Hoffmann-Riem*, JZ 2008, 1009 (1016).
538 *Brink* in: Wolff/Brink, BeckOK DatenschutzR, Art. 34, Rn. 40-43.

bestünde eine Schutzlücke, die sodann zur Lücke in der Überwachungs- und Verhütungspflicht des Staates vor Gefahren für digitale Identitäten erwächst. Diese Annahme widerspricht schlussendlich der beabsichtigten subsidiären Funktion des Grundrechts, das für moderne Entwicklungen und die mit ihnen verbundenen neuen Gefahren für die menschliche Persönlichkeit offen formuliert ist[539]. Damit ändert sich im Grundsatz nichts am verfassungsrechtlichen Schutz der digitalen Identität aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG.

bb) Varianten der digitalen Identität Der nun eröffnete und prima facie anwendbare Schutzbereich erfordert anhand der in Kapitel B.I. aufgezeigten Begriffsklärung eine differenzierte Betrachtung – daher nur „prima" facie. Umfang und Einzelheiten des Schutzes hängen von folgenden Parametern ab: Zunächst können die digitalen Identitäten auf „echten" Daten basieren oder mittels Synthese in künstlicher Form vorliegen. Ähnlich künstlich, da nicht unmittelbar oder (stets) zuordenbar, müssen digitale Identitäten aus Klardaten und aus pseudonymisierten und anonymisierten Datensätzen differenziert betrachtet werden. Schlussendlich kommt der Informiertheit über das Vorhandensein einer digitalen Identität eine vertiefende Betrachtung zu.

(1) Synthetisierte Datensätze Zuvorderst ist sich der Nutzung von digitalen Identitäten zur Generierung von sog. synthetisierten Daten zu widmen. So werden künstliche Datensätze als Resultat von Verfahren bezeichnet, die „echte" Daten durch fiktive Werte ersetzen, um Statistiken auf Basis personenbezogener Daten möglichst datenschutzkonform zu ermöglichen.[540] Dazu werden von einem bestimmten Datensatz Stichproben erhoben und auf eine Struktur oder ein Verhältnis der einzelnen Daten zueinander analysiert. Das erkannte Muster wird dann im Ergebnis beibehalten, jedoch werden sämtliche personenbezogenen Daten –

539 BVerfGE 65, 1 (41).

540 Beispielhaft seien an dieser Stelle nur das Paper von *Nettleton*, Social Network Analysis and Mining 2016, Article 44 zur Generierung von Social-Network-Statistiken und die Ausführungen von *Abdollahpouri*/*Qavami*/*Moradi*, Multimedia Tools and Applications 2018, 8475 zur Erzeugung von Nutzungs- und Verhaltensprofilen bei IPTV.

insbesondere sensible Daten, vgl. Art. 9 Abs. 1 DSGVO – entfernt und durch künstliche Werte ersetzt.[541] Grundvoraussetzung dieser Modelle der Datensynthese sind daher stets die Abbildbarkeit des Originaldatensatzes und das Ersetzen durch geeignete künstliche Werte.[542] Bei der Verarbeitung der Daten bestehen verschiedene Ansätze, beispielsweise auch der Einsatz von Machine-Learning-Algorithmen und Deep Learning zur automatisierten Mustererkennung.[543]

Es erscheint daher nicht fernliegend, im Falle der besonderen Verarbeitungssituation für diese Prozesse auch geltendes Datenschutzrecht einzubeziehen und eine notwendige Disponibilität aufseiten des Grundrechtsträgers anzunehmen. Dies muss zumindest bis zum Zeitpunkt gelten, wenn der künstliche Datensatz durch einen Ersetzungsalgorithmus erstellt wird und so eine automatisierte Entscheidung im Rahmen der Mustererkennung entsteht (vgl. Art. 22 Abs. 1 DSGVO). Die Entscheidung selbst entfaltet gegenüber den Datensubjekt auch eine rechtliche Wirkung, da das Datum durch die Ersetzung und Übertragung des abstrakten Aussagegehaltes dem Rechtskreis des Datensubjekts qua automatisierter Verarbeitung entzogen wird. Die Erhebung für den Originaldatensatz muss daher sowohl nach verfassungsrechtlichen Grundsätzen als auch geltendem Datenschutzrecht (Art. 22 Abs. 2 lit. a und c DSGVO) mitgeteilt werden. Gleiches gilt für die weitere Verarbeitung und den Verbleib der Daten nach Erstellen des synthetischen Datensatzes, die aufgrund des (verfassungsrechtlichen) Transparenzerfordernisses geboten ist. Im Wege der Ersetzung durch fiktive Angaben über Lebenssachverhalte ohne signifikante Einwirkung auf das Endergebnis kann es aber gelingen, anonyme bzw. anonymisierte und dennoch verwertbare Datensätze zu erhalten. Die Eigenschaft der Anonymität tritt schon dann ein, wenn personifizierende bzw. identifizierende Merkmale hinreichend ersetzt wurden und dies nicht wieder rückgängig zu machen ist.[544] Mithin wird diese Art der Anonymisierung (scheinbar)

541 Zum Vorgang im Einzelnen siehe *Drechsler*/*Jentzsch*, Synthetische Daten, S. 7 ff; *Raji*, DuD 2021, 303 (305 ff).
542 *Drechsler*/*Jentzsch*, Synthetische Daten, S. 10 f.
543 *Drechsler*/*Jentzsch*, Synthetische Daten, S. 11 f.
544 *Drechsler*/*Jentzsch*, Synthetische Daten, S. 19; *Raji*, DuD 2021, 303 (306 f). Ausführlicher in Kapitel D.I.1.b)bb)(2).

kaum durch eine Verknüpfung mit anderen synthetisierten Datensätzen oder öffentlich verfügbaren Daten aufzulösen sein. Gerade weil Merkmale fehlen, die eine Einzigartigkeit begünstigen und der Datensatz nur noch auf für die Statistik notwendigen Angaben ausgedünnt wird, sinkt das Risiko, synthetische Daten mit anderen Daten verknüpfen zu können, erheblich – sie entsprechen letztlich anonymen Daten.[545] Der Vorgang der Datensynthese ist daher zunächst als wirksames Mittel anzusehen, Datenschutz in Forschung und Entwicklung bei der Auswertung von Statistiken zu gewährleisten. Eine Loslösung des Personenbezugs führt jedoch zwangsläufig dazu, wenngleich sie auf personenbezogenen Daten basieren, dass die Datensätze nicht mehr Gegenstand des (verfassungsrechtlichen) Datenschutzrechts sind.[546]

Konsequent könnte daher auch angenommen werden, dass die digitale Identität nach einer Synthese ebenfalls aus dem datenschutzrechtlichen Rahmen fällt. Dafür spricht eindeutig, dass der Vorgang den Personenbezug auflöst – mithin auch das persönlichkeitsrechtliche Moment des Art. 2 Abs. 1 iVm 1 Abs. 1 GG entfällt. Ein Risiko, die Selbstbestimmung und Selbstbewahrung könnte durch die Offenlegung der syntethisierten digitalen Identitäten gefährdet werden, besteht schlichtweg nicht. Gegen die aufgeworfene These spricht allerdings, dass es für den Begriff der digitalen Identität nach hiesigem Verständnis[547] schon nicht auf den Personenbezug ankommt. Er dient vielmehr als allgemeiner Maßstab für die Risiko- und Schutzhöhe. Dies ist zum einen im technischen Begriff begründet, fußt aber weiterhin auf der Auffangwirkung des Grundrechts auf informationelle Selbstbestimmung. Insofern schließt das Bundesverfassungsgericht zwar prima facie andere Daten abseits von personenbezogenen Daten definitorisch aus, bezieht mithin nur persönliche und sachliche Angaben über eine Person ein.[548] Andererseits stellt es fest, dass ein Datum durch Verknüpfung und Verarbeitung

545 So auch *Drechsler*/*Jentzsch*, Synthetische Daten, S. 19 f; *Raji*, DuD 2021, 303 (307). Vgl. auch *Hammer* in: Jandt/Steidle, Datenschutz im Internet, B.IV., Rn. 288; *Hammer*/*Knopp*, DuD 2015, 503 (506 f).

546 Vgl. zur Anwendbarkeit der Datenportabilität auf Rückschlüsse aus personenbezogenen Daten *Artikel 29-Datenschutzgruppe*, WP 242 rev.01, S. 10 f.

547 Im Detail sub B.I.

548 BVerfGE 65, 1 (42).

auch erst personenbezogen werden kann: „Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr."[549] Dies meint jedoch gerade nicht anonymisierte wie pseudonymisierte Daten, sondern vielmehr Informationen über persönliche oder sachliche Verhältnisse, die *bis dato* keinen Stellenwert hatten. Beispielsweise erscheint der Fakt, dass ein bestimmtes Produkt mehrfach von einer Person in einem Geschäft aus dem Regal genommen und begutachtet wurde, nutzlos. Übertragen in das digitale Zeitalter und auf Online-Shops entsteht aber ein besonderes Interesse an dieser Information, da sie für Werbezwecke genutzt werden könnte.[550] Qua (verfassungsgerichtlicher) Definition bezieht sich das Grundrecht also nur auf mittelbar oder unmittelbar personenbezogene Daten.

Folglich ergibt sich kein Schutz für synthetisierte digitale Identitäten durch das Grundrecht auf informationelle Selbstbestimmung. Der Schutz endet mit der Entfernung von Merkmalen, die einen Personenbezug zulassen bzw. eine entsprechende Nähe zur Persönlichkeit iSd Art. 2 Abs. 1 iVm 1 Abs. 1 GG aufweisen. Dennoch bleibt (sogleich) zu bedenken, dass die Anonymisierung aufgrund des technischen Fortschritts und der Kombinationsmöglichkeiten nicht stets vor der Anwendung des Datenschutzrechts schützt, sondern ganz im Sinne des relativen Personenbezugs stets (wieder) zu einem personenbezogenen Datum werden kann. Dies gilt auch im Fall synthetischer Datensätze, wenn die Synthetisierung der Anonymisierung einheitlicher Datensätze dient und/oder sich die Auflösbarkeit der Anonymisierung durch Synthetisierung ankündigt.[551] Durch die Anonymisierung mittels Datensynthese können aus diversen Datensätzen neue digitale Identitäten gewonnen werden, sofern sie ausreichenden strukturellen wie inhaltlichen

549 BVerfGE 65, 1 (45).

550 Dazu hat sich insbesondere das Nudging auf vielerlei Weise etabliert, z.B. indem das Produkt durch personalisierte Werbung gesondert beworben wird. Diese und weitere Situationen aufzeigend *Venzke-Caprarese*, DuD 2017, 577 (577); *Obergfell*, ZLR 2017, 290 (293) zur individualisierten Preisbildung. Zur Thematik im Privacy-Kontext siehe nur *Kapsner*/*Sandfuchs*, Review of Philosophy and Psychology 2015.

551 Zur Rückführbarkeit des Personenbezuges ausführlich *Stadler*/*Oprisanu*/*Troncoso*, Synthetic Data – Anonymisation Groundhog Day, S. 7 f sowie *von Maltzan*, IoTBDS 2022, 215 ff.

Aussagegehalt aufweisen. Diese ähneln aber wegen ihres uneindeutigen Persönlichkeitsbezugs und der Rekombination verschiedener Identitäten jedoch fiktiven Identitäten und haben, soweit sie keine „eigene Persönlichkeit“[552] darstellen, kein Anrecht auf grundrechtlichen Schutz – weder zugunsten des Erstellers dieser synthetisierten digitalen Identitäten noch zugunsten des ursprünglichen Identitätsinhabers. Im Ergebnis entsprechen sie der idealen Typik anonymer Daten, soweit die verwendeten Synthetisierungsmaßnahmen nicht derart angreifbar sind, dass das Risiko der Auflösung der Anonymisierung merklich ansteigt.

(2) Anonymität und Pseudonymisierung: Das Kriterium des Personenbezugs In Anbetracht dieser Schlussfolgerung erscheint es überaus fraglich, einen verfassungsrechtlichen Schutz einer pseudonymen oder anonymisierten digitalen Identität anzunehmen. Infolgedessen bleibt auch dies vertieft zu überprüfen, unter Bezugnahme auf die im Datenschutzrecht geführte Diskussion über den Personenbezug des Datums.

Folglich ist die unter B.I.3.c) begonnene Diskussion aufzugreifen. Der Personenbezug eines Datums und jener der digitalen Identität sind aufgrund des gemeinsamen Kerns, dem Datum, unvermeidbar miteinander verknüpft und wirken sich entsprechend auf die Betrachtung aus. Eine stets strenge, differenzierte Einordnung ist jedoch kaum möglich, da ein Datum je nach Kontext, Verwendungszweck oder Vergleichsobjekt zu einem anderen Personenbezug führt. Beispielsweise kann er sich erst aus dem Zweck oder Ergebnis einer Datenverarbeitung ergeben.[553] Die

552 Zu denken wäre hier an digitale Identitäten, die als Kunstfigur dennoch grundrechtlichen Schutz erhalten, also Art. 5 Abs. 3 S. 1 Alt. 1 GG zugeordnet werden können. Einfachgesetzlich könnte für solche Fälle möglicherweise das Urheberrecht herangezogen werden, wenn sich die künstlerischen Aspekte der digitalen Identität gerade durch Werke des Urheberrechts (Schriftwerke, Bildwerke) besonders äußern. Hierzu fehlt es bislang an weiterer rechtswissenschaftlicher Auseinandersetzung.

553 *Artikel 29-Datenschutzgruppe*, Opinion 4/2007 on the concept of personal data, S. 10 f; *Klabunde* in: Ehmann/Selmayr, DSGVO, Art. 4, Rn. 10 unter Bezug auf EuGH, Urteil vom 20.12.2017, Az. C-434/16 – Nowak.

Begriffe des Personenbezuges (vollständige Identifizierbarkeit), der Pseudonymität (Identifizierbarkeit in Abhängigkeit der Sichtweise)[554] und der Anonymität (keine Identifizerbarkeit)[555] gehen fließend ineinander über.[556] Ihre Bestimmung kann daher nur relativ erfolgen, unter Einbeziehung aller einer Person zugänglicher und ihrem Ermessen nach wahrscheinlich zur Identifizierung genutzter Mittel.[557] Zur Ermittlung der Wahrscheinlichkeit einer Identifikation durch diese Mittel ist ein objektiver Maßstab zu wählen.[558] Ist der Übergang zwischen den Sphären der Identifikation aufgrund technischer oder physischer Vorkehrungen nicht möglich, liegt die sog. Unverkettbarkeit (auch: Nichtverkettbarkeit oder Unverknüpfbarkeit) vor. Dieses Prinzip ist durch die Datenschutzkonferenz in die Schutzziele des Standarddatenschutzmodells aufgenommen worden und stellt sowohl eine Konkretisierung der Zweckbindung als auch der Datenminimierung dar.[559] Der fast unmöglichen Trennung der Arten des Personenbezugs ist durch die Erreichung dieses Datenschutzziels zu begegnen, insbesondere durch die technischen Vorsichtsmaßnahmen. Zwar dienen Pseudonymisierung und Anonymisierung selbst dazu, die Unverkettbarkeit aufrecht zu erhalten. Um aber einer erneuten Verkettbarkeit vorzubeugen, bedarf es weiterer Schritte wie einer gesonderten Verwaltung der Datensätze bzw. digitalen Identitäten. Eine Veränderung der Daten und damit des Inhalts der digitalen Identität sowie das Anonymisieren

554 Zum Begriff Art. 4 Nr. 5 DSGVO sowie vgl. § 3 Abs. 6a BDSG a.F.; *Petrlic*/*Sorge*, Datenschutz, S. 13/14; *Hansen*/*Walczak*, RDV 2019, 53 (53 f).

555 Zum Begriff nur oberflächlich ErwGr 26 S. 5 DSGVO sowie vgl. § 3 Abs. 6 BDSG a.F.; *Klabunde* in: Ehmann/Selmayr, DSGVO, Art. 4, Rn. 20; *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1, Rn. 31 f; *Petrlic*/*Sorge*, Datenschutz, S. 12/13. Ausführlich zum Verfahren *Hammer* in: Jandt/Steidle, Datenschutz im Internet, B.IV., Rn. 287 ff.

556 Zu weiteren Sub-Kategorien auch *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 61 f.

557 So ErwGr 26 S. 3 DSGVO, beruhend auf EuGH, Urteil vom 19.10.2016, Az. C582/14 – Breyer –, Rn. 49. Vgl. auch EuGH, Urteil vom 20.12.2017, Az. C-434/16 – Nowak –, Rn. 31 ff. Infolgedessen scheint der relative Ansatz vorherrschend, wenngleich sich die deutschen Gerichte bislang nicht explizit hierzu geäußert haben. Hierzu im Detail *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1, Rn. 25 ff; *Herbst*, NVwZ 2016, 902 (903 ff, 905).

558 ErwGr 26 S. 4 DSGVO. Vertiefend auch *Hofmann*/*Johannes*, ZD 2017, 221 (224).

559 *Datenschutzkonferenz des Bundes und der Länder*, Das Standard-Datenschutzmodell (Version 1.1), S. 15 f, 20 sowie *Datenschutzkonferenz des Bundes und der Länder*, Das Standard-Datenschutzmodell (Version 2.0b), S. 27; *Petrlic*/*Sorge*, Datenschutz, S. 14. Hierfür ebenfalls sprechend *Roßnagel*, ZD 2018, 339 (341).

und Pseudonymisieren der gesamten digitalen Identität als datenschutzrechtliche Verarbeitung könnte allerdings zu einer Veränderung im verfassungsrechtlichen Schutz führen – sowohl auf Ebene des Schutzbereichs als auch hinsichtlich der Verhältnismäßigkeitsprüfung.

Der Schutzbereich der informationellen Selbstbestimmung umfasst, wie ausgeführt[560], jedes Datum mit Personenbezug. Nach den hiesigen Ausführungen zählen dazu grundsätzlich auch verknüpfte Datenbestände wie die digitale Identität. Häufig wird sie im Verhältnis zwischen Nutzern jedoch nicht unmittelbar personenbeziehbar benutzt, sondern mittels Kennung wie einem selbst gewählten Benutzernamen. Damit ähnelt die Kennung bzw. das Pseudonym gewissermaßen einer Maske, hinter die lediglich der Anbieter der Plattform – also der Verwalter der digitalen Identitäten – blicken kann. Der Personenbezug ist somit in seiner Qualität nur teilweise vorhanden: Nutzer von Pseudonymen auf „gleicher Ebene" können häufig keine Verknüpfung zwischen Pseudonym und Orthonym herstellen, während – sofern vorhanden – der Diensteanbieter bei direkten bzw. „sprechenden" Angaben (Name als Teil der Mailadresse, Adresse, etc.) oder durch die Möglichkeit eines Informations- oder Auskunftsanspruchs (z.B. § 101 Abs. 9 UrhG; § 14 Abs. 3-5 TMG a.F. bzw. § 21 Abs. 1 TTDSG iVm § 24 Abs. 1 Nr. 2 BDSG) eine Verknüpfung herstellen kann.[561] Überdies muss sie nicht auf den Namen referenzieren und infolgedessen identifizierend sein; eine Individualisierung mittels Verknüpfung mehrerer Aussagen über eine Person reicht aus.[562] Die Konstellation der einseitigen Zuordnung (z.B. beim Verantwortlichen oder

560 Siehe D.I.1.b).

561 Derart differenzierend *Roßnagel*/*Scholz*, MMR 2000, 721 (727) sowie *Roßnagel*, ZD 2018, 243 (245); *Hammer*/*Knopp*, DuD 2015, 503 (507). Dieses Verständnis ist jedoch nur in qualitativer Hinsicht anzuwenden, zugunsten der Klarheit des Begriffs – siehe *Knopp*, DuD 2015, 527 (529). Kritisch zur Differenzierung ebenfalls *Karg*, DuD 2015, 520 (521 f). Bloß zur sprechenden Eigenschaft siehe *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1 DSGVO, Rn. 39.

562 *Karg*, DuD 2015, 520 (523); *Artikel 29-Datenschutzgruppe*, Opinion 4/2007 on the concept of personal data, S. 14 sowie *Artikel 29-Datenschutzgruppe*, Opinion 05/2014 on Anonymisation Techniques, S. 14; vgl. auch *Hammer* in: Jandt/Steidle, Datenschutz im Internet, B.IV. Rn. 288.

einem Dritten als Treuhänder[563])[564] ist dem Zweck des Pseudonyms fast schon inherent, da es stets wenigstens eine Stelle mit Zuordnungsmöglichkeit gibt.[565] Ein Pseudonym kann die Personenbeziehbarkeit sowie Identifizierbarkeit daher lediglich erschweren, eine Verknüpfbarkeit durch Recherche nur unterbrechen und einer weiteren Verarbeitung auf Basis von Verkettung entgegenwirken.[566] Dies erfordert unter anderem die Verschiedenheit aller genutzter Pseudonyme untereinander sowie eine Vermeidung doppelter Metadaten.[567] Ein vollständiger Ausschluss entspricht dem Verhältnis der Anonymität. Es muss also eine unmittelbare oder mittelbare Identifizierbarkeit vorliegen, vgl. auch Art. 4 Nr. 1 DSGVO. Darauf verweist auch das Bundesverfassungsgericht, indem es die „Nutzbarkeit und Verwendungs*möglichkeit*" als Referenzpunkt für die Schutzwürdigkeit des personenbezogenen Datums vor einer automatischen bzw. technischen Verarbeitung erklärt.[568] Insofern wirkt sich eine Pseudonymisierung – nachträglich wie originär[569] – nur im Einzelfall im Rahmen der Möglichkeitsprüfung darauf aus, ob ein Personenbezug vorliegt. Diesen Ansatz greift die DSGVO auf und stellt fest: „Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden."[570] Dieser Weisheit Schluss bedeutet jedoch

563 Zum Konstrukt des Datentreuhänders siehe nur *von Ulmenstein*, DuD 2020, 528 ff.

564 Zu den drei Arten des Pseudonyms *Roßnagel*/*Scholz*, MMR 2000, 721 (725) und *Hammer*/*Knopp*, DuD 2015, 503 (507).

565 *Knopp*, DuD 2015, 527 (529).

566 *Hammer*/*Knopp*, DuD 2015, 503 (505) sowie *Knopp*, DuD 2015, 527 (527/528). Weiter bezweckt die Pseudonymisierung die Unterstützung des Verantwortlichen bei der Einhaltung des Datenschutzrechts, so ErwGr 28 DSGVO. Dies ist jedoch missverständlich, setzt die Vergabe von Pseudonymen auf Seiten des Verantwortlichen die entsprechenden technischen Anforderungen voraus. Eine Umgehung des Klarnamenzwangs, wie er laut AGB bei Facebook vorherrscht, kann keineswegs hierunter zu fassen sein. Dies würde die Erfüllung datenschutzrechtlicher Vorgaben vielmehr auf die Inhaber digitaler Identitäten bzw. betroffene Personen verlagern und damit der Zweckrichtung des Datenschutzrechts (vgl. Art. 1 Abs. 2 DSGVO) zuwiderlaufen.

567 Vgl. *Artikel 29-Datenschutzgruppe*, Opinion 4/2007 on the concept of personal data, S. 18.

568 Vgl. BVerfGE 65, 1 (45).

569 Vertiefend zur Differenzierung *Schleipfer*, ZD 2020, 284 ff.

570 ErwGr 26 DSGVO.

nicht, dass jedes Pseudonym als personenbezogenes Datum zu sehen ist. Darauf weist schon das Wort „sollen“ im zitierten Erwägungsgrund hin, ebenso der eben erwähnte Möglichkeitsansatz des Bundesverfassungsgerichts. Der Verweis des Erwägungsgrundes 26 S. 2 DSGVO auf das Wissen Dritter, welches in die Ermittlung einzubeziehen ist, hindert dieses Verständnis nicht. Schließlich ist mit der Rechtsprechung des EuGH zur Ermittlung des Personenbezugs klargestellt worden, dass eine Zurechnung des Wissens Dritter nur bei entsprechenden Informationsansprüchen oder anderen rechtlichen Grundlagen zugunsten des Verantwortlichen möglich ist.[571] Mitnichten ist dieses Merkmal also rein-objektiv zu verstehen, sondern die bloße Möglichkeit einer Auflösung des Pseudonyms durch einen beliebigen Dritten oder gar von Jedermann einzubeziehen.[572] Eher gilt bei der Betrachtung von zunächst nicht-personenbezogenen Daten ein objektiver Maßstab unter Einbeziehung aller möglicher (subjektiver) Informationsquellen, derer sich der Verarbeitende bedienen kann und nach Rechtsprechung des EuGH auch erwartungsgemäß tun würde.[573] Ist die Herstellung des Bezugs entsprechend schwierig oder schließt ihn nahezu aus, genügt das Pseudonym seinem Zweck.[574] In jedem Fall erweitert sich bei positivem Ergebnis der Schutz der digitalen Identität um die Elemente des Persönlichkeitsrechts, da auf Daten-Ebene die Aspekte der Persönlichkeitssphären sichtbar werden. Je näher die möglichen Verknüpfungen die (analoge) Persönlichkeit abbilden, desto schützenswerter sind die Daten im Rahmen der Abwägung.[575] Darüber hinaus kommt einem Pseudonym auch ein mittelbarer Schutz durch die Kommunikationsgrundrechte zu. Die Nutzung von Decknamen oder verschleierten Identitäten ist, wie erwähnt, zur Umgehung von Chilling Effects von besonderer, meinungsfördernder Bedeutung: Durch die

571 EuGH, Urteil vom 19.10.2016, Az. C-582/14 – Breyer –, Rn. 39 ff; Urteil vom 20.12.2017, Az. C-434/16 – Nowak –, Rn. 31 ff.

572 So im Ergebnis auch *Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 4 Nr. 1 DSGVO, Rn. 61; *Hofmann*/*Johannes*, ZD 2017, 221 (224).

573 EuGH, Urteil vom 19.10.2016, Az. C-582/14 – Breyer –, Rn. 49. Ebenso *Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 4 Nr. 1 DSGVO, Rn. 59 f; *Herbst*, NVwZ 2016, 902 (903 f). Möglichkeiten und Szenarien der Aufdeckung eines Pseudonyms erläuternd *Hansen*/*Walczak*, RDV 2019, 53 (55 f).

574 Siehe § 3 Abs. 6a BDSG a.F.

575 Vgl. BVerfGE 65, 1 (42).

Verwendung eines Pseudonyms besteht die Möglichkeit, seine Meinung auch bei streitbaren Argumenten frei und ungehindert zu äußern.[576] Die Angst vor Ächtung oder Repressionen fällt gewissermaßen mit Ablegen der Maske; sie verbleibt bei der pseudonymen Identität. Im Austausch prägt diese Art der freien Meinungsäußerung auch die kommunikative Persönlichkeitsentfaltung aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG.[577] Die Freiheit in diesen Punkten findet dennoch ihre Grenzen in den kollidierenden Rechten Dritter, sei es nur hinsichtlich der Abgrenzung von Schmähkritik und Satire. Unabhängig vom eigentlichen Verwendungszweck sind pseudonyme digitale Identitäten wegen ihrer potentiellen, wenn nicht gar inherent einseitigen, Personenbeziehbarkeit auch vom Schutz des Grundrechts auf informationelle Selbstbestimmung umfasst – sowohl als Instrument zwecks Selbstdatenschutz[578] als auch als Verpflichtung der Diensteanbieter zum Schutz der Grundrechte der betroffenen Personen.

Fraglicher erscheint dagegen die Einordnung von anonymen digitalen Identitäten in den Schutzbereich der informationellen Selbstbestimmung. Mit Blick auf die eingangs aufgeführte Definition ist dies von vornherein zu verneinen, mangelt es schon an einem Personenbezug des Datums sowie anderweitiger persönlichkeitsrechtlicher Relevanz. Einen anderen Schluss lässt das binäre Verhältnis zwischen Personenbezug und Anonymität[579] wohl nicht zu. Vergleichbar mit Sachdaten[580] enthalten anonyme bzw. anonymisierte Datensätze häufig nur Aussagen, welche Hinweise auf Personengruppen oder generelle gesellschaftliche Verhältnisse enthalten. Davon sind jedoch personenbezogene Sachdaten, also Angaben über eine Person durch einen Gegenstand (z.B. Standortdaten des Mobiltelefons), zu unterscheiden.[581] Folglich mangelt es anonymen Daten grundsätzlich bereits an jeglicher Prämisse der Einzigartigkeit oder Detailliertheit. Datenverknüpfungen

576 *Kersten*, JuS 2017, 193 (196).
577 BVerfGE 65, 1 (43) sowie Urteil v. 25.2.2020 – Az. 1 BvR 1282/17 –, Rn. 7; *Härting*, NJW 2013, 2065 (2068).
578 *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 56, 60 ff.
579 Hierzu *Karg*, DuD 2015, 520 (520) sowie vertiefend *Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 4 Nr. 1 DSGVO, Rn. 14 f.
580 Ähnlich *Karg*, DuD 2015, 520 (522). Zum Begriff *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1 DSGVO, Rn. 12 f.
581 *Karg*, DuD 2015, 520 (522).

zwischen solchen „aussagenlosen“ Daten – welche dann eine digitale Identität iSd Untersuchung darstellen – sind regelmäßig in der Statistik zu finden, weshalb das anonyme Datum bzw. auch das anonyme (Persönlichkeits-)Profil für diesen Bereich aus gezeigten Gründen von besonderer Bedeutung ist.[582] Bereits der Gedanke an eine Verknüpfung deutet aber an, dass eine weitergehende Verknüpfung mit anderen Datensätzen möglicherweise das Risiko einer Auflösung der Anonymität birgt – vorausgesetzt, die Daten weisen im Gegensatz zu synthetisierten digitalen Identitäten einen personenbezogenen Teilgehalt des Originaldatums auf. Nicht nur der bloße Fakt der Digitalisierung und die Steigerung der Rechenkapazität (z.B. durch Quantencomputer) sowie die fortschreitende Vernetzung aller Informationstechnik sprechen dafür, dass das Potential der Zuordnung steigt.[583] Auch die große Menge an öffentlich zugänglichen Informationen – sowohl aus

582 Siehe nur BVerfGE 65, 1 (47) sowie E 150, 1 (Rn. 223 f) – Zensus 2011. Vgl. auch *Hölzel*, DuD 2018, 502 (503).

583 Beispielsweise BVerfGE 120, 274 (304): „Kapazität ihrer Arbeitsspeicher und der mit ihnen verbundenen Speichermedien“; *Artikel 29-Datenschutzgruppe*, Opinion 05/2014 on Anonymisation Techniques, S. 8: „research, tools and computational power evolve“; *Karg*, DuD 2015, 520 (520): „Entwicklung der Informations- und Kommunikationstechnologie“; *Roßnagel/Scholz*, MMR 2000, 721 (723): „die gegenwärtigen und künftigen technischen Möglichkeiten der elektronischen Datenverarbeitung“. Jüngst mündet diese Problematik im Stichwort „Kryptoagilität“, das die Flexibilität beim Austausch von Verschlüsselungsalgorithmen beschreibt – hierzu ausführlich *Hagemeier*, DuD 2019, 631 ff.

rechtmäßigen (soziale Netzwerke)[584] wie rechtswidrigen Quellen (Identitätsdatenleaks)[585] – führt dazu, dass auch „Neugierige" Zugriff auf Kontextwissen haben und über Schlussfolgerungen weitere Datensätze oder gar öffentlich einsehbare digitale Identitäten finden. Um ein anonymisiertes Datum bzw. einen anonymisierten Datensatz erneut zu de-anonymisieren, reichen bereits 15 Merkmale aus demografischen oder statistischen Daten – z.B. Alter, Geschlecht, Ort, Persönlichkeitstyp, etc. – aus.[586] Die Idee der absoluten Anonymität kann dahingehend bezweifelt werden. Vielmehr ist von einem stetig variablen Restrisiko auszugehen.[587]

584 *Hammer*/*Knopp*, DuD 2015, 503 (505).

585 Wenngleich auf der Ebene der DSGVO bislang in Einklang mit der Rechtsprechung des EuGH angenommen wurde, dass in die Ermittlung der Wahrscheinlichkeit einer Zuordnung nicht rechtswidrige Mittel einzubeziehen sind – so zumindest *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1 DSGVO, Rn. 29 und *Karg* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 4 Nr. 1 DSGVO, Rn. 64 –, ist dennoch das aufkommende Risiko einer Offenlegung der Zuordnung zu diskutieren. Die reine Möglichkeit einer Zuordnung durch Abruf und Einbeziehung der öffentlich einsehbaren Datensätze ist schließlich nicht unmöglich. Dagegen ist jedoch ins Feld zu führen, dass sich die Reichweite des Wissens nur auf „vernünftigerweise" und rechtliche Mittel begrenzt. Insbesondere nennt der EuGH in der Breyer-Entscheidung Rechtsansprüche des Verantwortlichen auf Auflösung der IP-Adresse. Einen Anspruch oder ein anderweitiges, ähnliches rechtliches Interesse zur Verknüpfung der eigenen digitalen Identitäten mit fremden Datensätzen zur Auflösung von Pseudonymen besteht nicht. Vielmehr würde dies eine Umgehung des Einwilligungsrechts des Betroffenen sowie der gesamten Konzeption des Datenschutzrechts als Verbot mit Erlaubnisvorbehalt umgehen. Das Datenschutzrecht endet jedoch nicht dort, wo Daten – widerwillig – öffentlich gemacht wurden. Der grundrechtliche Schutz kann nur durch den Betroffenen selbst, partiell und zweckgebunden gelockert werden. Diese Lockerung, die nicht als Aufgabe iSe Grundrechtsverzichts anzusehen ist, ist Teil der Ausübung des Grundrechts auf informationelle Selbstbestimmung. Ein Grundrechtsschutz ist daher insbesondere im Drittverhältnis gegenüber „Neugierigen" relevant, wenn diese die Datensätze nutzen und verarbeiten. Darunter zählt auch, Verknüpfungen mittels Recherche herzustellen und vorzuhalten.

586 Siehe hierzu die Studie *Rocher*/*Hendrickx*/*de Montjoye*, Nature Communications 10 (2019), S. 5.

587 Ebenso *Artikel 29-Datenschutzgruppe*, Opinion 05/2014 on Anonymisation Techniques, S. 8/9; *Karg*, DuD 2015, 520 (525); *Hofmann*/*Freiling*, ZD 2020, 331 (334).

Dieses Restrisiko erschöpft sich im gegenwärtigen Verständnis der Anonymität.[588] Zum einen kann hier bzgl. des Personenbezugs erneut der Möglichkeitsansatz der verfassungsrechtlichen Rechtsprechung herangezogen werden, ebenso die weiteren Grundsätze der Ermittlung des Potentials für einen Personenbezug. Konkretisiert werden letztere durch das zeitliche wie leistungsgerichtete Moment, die Anonymität aufzulösen. Eingeführt wurden diese mit § 3 Abs. 6 BDSG a.F. Danach war die Anonymität faktisch schon gegeben, wenn der Personenbezug „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" möglich war. Die Formulierung nimmt die vom Bundesverfassungsgericht vorgesehene Entwicklungsoffenheit der informationellen Selbstbestimmung auf und begreift sie als Aufgabe der Gewährleistung.[589] Im Umkehrschluss kann aus den Kriterien des § 3 Abs. 6 BDSG a.F. auch die fortwährende Berücksichtigung technischer Möglichkeiten der Auflösung bei der Bewertung der Anonymisierungsverfahren verstanden werden, die dann zu einer stetigen Aufgabe der Anpassung und ggf. Nachbesserung der Anonymisierungsverfahren erwächst. Mit Recht wurde die Idee des § 3 Abs. 6 BDSG a.F. daher in Erwägungsgrund 26 der DSGVO übernommen und allgemein in die Ermittlung des Personenbezuges einbezogen.

Die (weitere) Definition der Anonymität innerhalb des Datenschutzrechts de lege lata ist jedoch ausgeblieben. Eine Definition über landesrechtliche Vorschriften kann je nach Ausgestaltung unter dem vollharmonisierenden Ansatz der DSGVO zumindest kritisch gesehen werden.[590] Vielmehr das binäre Verhältnis zwischen Personenbezug und Anonymität gestärkt worden. Dies ist insofern bedenklich,

588 Anders *Stürmer*, ZD 2020, 626 (629), wobei jene Ansicht einem gewichtigen Widerspruch zugrunde liegt: Nach dem dort vertretenen Herausfallen personenbezogener Daten aus dem Anwendungsbereich der DSGVO muss konsequent auch die Überprüfungspflicht auf eine Auflösbarkeit der Daten und ein Wiederaufleben des Datenschutzrechts hin entfallen. Dass diese letztendlich weiterhin bestehen bleibt erscheint in der streng binären Lesart widersprüchlich.

589 Vgl. BVerfGE 65, 1 (48): „Es müssen klar definierte Verarbeitungsvoraussetzungen geschaffen werden, die *sicherstellen*, daß der Einzelne unter den Bedingungen einer automatischen Erhebung und Verarbeitung der seine Person betreffenden Angaben nicht zum bloßen Informationsobjekt wird." In der Literatur von einer Gewährleistung hinsichtlich der Anonymisierung ausgehend *Karg*, DuD 2015, 520 (525). Dies wird auch durch die entwicklungsoffene Formulierung des einfachgesetzlichen Personenbezugs gestützt, siehe *Hofmann*/*Johannes*, ZD 2017, 221 (224 f).

590 Hierzu ausführlich *Meyer*, ZD 2021, 669 (672 ff).

als dass der verfassungsrechtliche Schutz nicht an dieser Stelle endet – wenngleich sich das Grundrecht auf informationelle Selbstbestimmung per Definition ausschließlich auf personenbezogene Daten bezieht.[591] Gewissermaßen als Reflex muss auch die (gewählte) Anonymität, also das bewusste Nicht-Offenlegen von Informationen, Teil der Ausübung des Grundrechts sein.[592] Gerade diese Variante bezweckt in ihrer reinsten Form das Moment der Selbstbewahrung als informationellen Rückzugsort. Dafür spricht zudem das aus dem Persönlichkeitsrecht erwachsende Recht auf Anonymität, wobei das Grundrecht auf informationelle Selbstbestimmung dazu als lex specialis iSe Konkretisierung anzusehen ist.[593] Zugleich wird ihre Rolle im demokratischen Meinungs- und Kommunikationsprozess[594] sowie ihr partizipatorischer Aspekt[595] berücksichtigt. Die Geltung des Grundrechts reicht jedoch nur so weit, wie die Befugnis über die personenbezogenen Daten einschließlich ihrer Verknüpfung zu digitalen Identitäten reicht. Die weitere Verarbeitung anonymer Daten entzieht sich diesem Herrschaftsbereich. Darüber hinaus – und daher begrifflich zu differenzieren – sind originär anonyme Daten im Gegensatz zu anonymisierte Daten diesem Herrschaftsbereich schon von Beginn an entzogen, da sie von vornherein keine personenbezogenen oder andere Einzelangaben über persönliche oder sachliche Verhältnisse einer Person enthalten. Angesichts der beschriebenen Wahrscheinlichkeit der De-Anonymisierung anonymer Daten scheint die Verbannung aus dem Herrschaftsbereich des Grundrechtsträgers allerdings nicht mehr den tatsächlichen Gegebenheiten angemessen.

591 Siehe nur BVerfGE 65, 1 (42).

592 Mit gleichem Ergebnis *Luch*, Medienpersönlichkeitsrecht, S. 133; *Bäumler* in: Bäumler/von Mutius, Anonymität im Internet, 1 (5). Dagegen ein eigenständiges Grundrecht annehmend *Kersten*, JuS 2017, 193 (195 f). Weitere dogmatische Konstruktionen einschließlich damit zusammenhängende Probleme aufzeigend *von Mutius* in: Bäumler/von Mutius, Anonymität im Internet, 12 (12) mwN, wobei im Weiteren (S. 15 ff) die Anonymität als „selbstständiges Teilrecht" des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG hergeleitet wird. Dies wirkt allerdings dann diffus, wenn bei der Einordnung gegenüber dem Grundrecht auf informationelle Selbstbestimmung sowie den übrigen Teilgehalte des Allgemeinen Persönlichkeitsrechts dann ein aus der informationellen Selbstbestimmung herzuleitendes Gebot der Anonymisierung erwähnt wird. Eine Trennung dieser Art wirkt inkonsequent.

593 *Kersten*, JuS 2017, 193 (195).

594 Hierzu *Kersten*, JuS 2017, 193 (201 f).

595 *Hartmann*, MMR 2017, 383 (385).

Zwar würde durch die strikte Trennung die klare Dogmatik aufrecht erhalten werden können, wie sie mit dem BDSG a.F. eingeführt wurde. Schon 2007 erkennt *Krügel* dementgegen, dass die Qualität der Anonymität von einer Einzelfallentscheidung abhängig ist[596] – und nimmt so den relativen Ansatz des Personenbezuges der heutigen DSGVO vorweg. Das weitere Festhalten an veralteten Dogmen käme folglich einer Augenwischerei gleich, wo die Grenze zwischen Personenbezug (direkt oder bei Pseudonym) und Anonymität zunehmend verschwimmt und je Sichtweise des Verantwortlichen anders zu entscheiden ist. Der erkennbare, aber ungeregelte Bereich zwischen diesen Begriffen, wo eben nicht „ein bisschen Datenschutz" herrscht,[597] müsste daher durch den europäischen wie nationalen Gesetzgeber befüllt werden. Zumindest erscheinen die vereinzelten Ansätze in der Literatur nicht ausreichend, um die Übergänge datenschutzrechtlich abzusichern. So wird zwar der risikobasierte Ansatz der DSGVO hervorgehoben und über das Kriterium des Personenbezugs gestellt[598] oder eine Fokussierung auf die Prüfung der Merkmale des Personenbezugs der Reihenfolge und Systematik nach forciert[599]. Der risikobasierte Ansatz ist allerdings bereits Teil der Prüfung des Personenbezugs, wie auch der von *Schmitz* aufgezeigte Erwägungsgrund 75 die „unbefugte Aufhebung der Pseudonymisierung" benennt. So gesehen rekurriert die datenschutzrechtliche Risikobetrachtung auch auf die relative Betrachtung des Personenbezugs, welcher die Risiken der Änderung des Datenbestandes, der unternehmerischen Interessen oder technischen Verarbeitungsmöglichkeiten aufgreift. Sie schließen sich – entgegen der Ansicht von *Schmitz* – nicht aus.[600] Eine

596 *Artikel 29-Datenschutzgruppe*, Opinion 4/2007 on the concept of personal data, S. 21; *Europäischer Datenschutzbeauftragter*, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of COVID-19 outbreak, S. 5 Rn. 15: „contextual elements that may vary case by case"; mwN auch *Gierschmann*, ZD 2021, 482 (483 f).

597 *Karg*, DuD 2015, 520 (523).

598 *Schmitz*, ZD 2018, 5 (8).

599 *Krügel*, ZD 2017, 455 (456).

600 Hiervon ausgehend wohl *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1 DSGVO, Rn. 22.

dezidierte Prüfung der Merkmale hilft jedoch nicht über die Dynamik des Personenbezuges weg, wenngleich sie ein zeitliches Moment enthält[601]. Die bereits erwähnte Betrachtung des Personenbezugs in den Stadien des Zwecks, des Inhalts und des Ergebnisses der Verarbeitung, auf die *Krügel* verweist, führt auch bei einer möglichen De-Anonymisierung zu einem Personenbezug. Dieser kann sich nämlich als Ergebnis einer Aggregation – also einer Verarbeitung – ergeben, wenn der Verarbeitende nach allgemeinem Ermessen auf Mittel und Informationen in seiner Sphäre zurückgreifen kann und würde. Zumindest besteht hierin zunehmend das Risiko für die Rechte und Freiheiten der Träger des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG und auch des Grundrechts auf Datenschutz aus Art. 8 GrC.

Die Stärke bzw. „Robustheit“[602] der Anonymisierung von Daten kann dahingehend bezweifelt werden, obschon diese Art der Verarbeitung von Daten mit einer Gewährleistung dieses Status einhergeht. Von Seiten des Gesetzgebers sollte daher stets Wert auf eine „echte“ bzw. absolute[603] Anonymisierung gelegt, also als Standard iSd Stands der Technik etabliert, werden. Unter echter Anonymisierung ist jede Verarbeitung von personenbezogenen Daten zu verstehen, die die Identifizierbarkeit einer Person unmöglich macht.[604] Unmöglich meint dabei jedoch allein faktisch nicht identifizierbar, also ganz im Verständnis des § 3 Abs. 6 BDSG a.F.

601 Die Betrachtung des Personenbezuges geschieht im (potentiellen) Moment der Datenverarbeitung, wie sich indirekt aus ErwGr 26 S. 4 aE entnehmen lässt – so auch *Krügel*, ZD 2017, 455 (456). Dies ermöglicht zwar im Ansatz eine relative Betrachtung, da es nur auf die Möglichkeiten im Moment der besagten Verarbeitung ankommt. Relativ betrachtet werden müssen aber auch die Vorgänge der Datenverarbeitung selbst, also sowohl Inhalt, Zweck und Ergebnis der Datenverarbeitung in Abhängigkeit vom Datensatz und ggf. weiteren Faktoren. Damit greift eine Fokussierung der Relativität lediglich auf das zeitliche Moment zu kurz.

602 Hierzu *Europäischer Datenschutzbeauftragter*, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of COVID-19 outbreak, S. 5 Rn. 15, 16.

603 Als absolute Anonymisierung wird das eine Re-Identifizierung ausschließende Verändern der Daten verstanden. Hiervon ist die formale Anonymisierung, also die Entfernung direkter Merkmale wie Name, Anschrift, etc. zu trennen. – So *Hornung*/*Wagner*, ZD 2020, 223 (224); *Watteler*/*Kinder-Kurlanda*, DuD 2015, 515 (516).

604 *Klabunde* in: Ehmann/Selmayr, DSGVO, Art. 4, Rn. 20.

nur unter großem zeitlichen, finanziellen oder technischen Aufwand.[605] Von Seiten des Staates sind diesbezüglich allerdings keine Vorgaben ersichtlich, weshalb sich an der Richtlinie des faktischen State of the Art bzw. Standes der Wissenschaft und Technik zu orientieren ist. Dies folgt sowohl aus den datenschutzrechtlichen Bestimmungen der Art. 25, 32 DSGVO[606] als auch im Wege der mittelbaren Drittwirkung der informationellen Selbstbestimmung, welche Nutzungsverträge von Plattformen oder technischer Infrastruktur z.B. in Generalklauseln durchdringt. Grundsätzlich sind danach technisch geeignete und erforderliche Mittel zu wählen, die sowohl die Dienstleistung ermöglichen als auch die Rechte und Freiheiten des Nutzers – beispielsweise in Form der Schutzziele des Art. 5 Abs. 1 DSGVO – berücksichtigen.[607] Nach Möglichkeit sind also unmittelbar anonyme Daten zu erheben und mit Blick auf den Verarbeitungs- bzw. Verwendungszweck zur Zweckerfüllung auch anonymisierte Daten zu verwenden. Befinden sich verschiedene anonyme und/oder anonymisierte Datensätze an einem Speicherort, könnte dies die Unverkettbarkeit beeinträchtigen. Denn auch durch das Vergleichen und Kombinieren dieser Datensätze können sich Muster ergeben, die auf eine bestimmte Person zurückzuführen sind und die Identifizierbarkeit erhöhen (sog. record linkage).[608] Sodann fungieren die einzelnen Daten als Quasi-Identifier des Musters.[609] Überdies ist das Anonymisierungsverfahren nach dem Stand der Wissenschaft und Technik auszurichten: Die Auswahl des Verfahrens sollte jeweils im Sinne der Verhältnismäßigkeit sowie der datenschutzrechtlichen Zielstellungen der Datenminimierung und Zweckbindung getroffen werden. Das Verfahren der Generalisierung ermöglicht beispielsweise die Reduktion des Datensatzes auf nur noch notwendige Teile. Dazu können im Sinne einer Generalisierung Teile des

605 Bereits BVerfGE 65, 1 (49); ferner *Schild* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), § 3 BDSG 2003 [aK], Rn. 96 f.

606 Hierauf bezugnehmend *Ritter* in: Schwartmann et al., DSGVO/BDSG, Art. 32, Rn. 34.

607 *Hartung* in: Kühling/Buchner, DSGVO, Art. 25 DSGVO, Rn. 20 sowie *Jandt* in: Kühling/Buchner, DSGVO, Art. 32 DSGVO, Rn. 5; *Baumgartner* in: Ehmann/Selmayr, DSGVO, Art. 25, Rn. 14 f.

608 Siehe hierzu die Angriffsbeispiele in *Petrlic*/*Sorge*, Datenschutz, S. 34 ff. Vgl. auch *Hölzel*, DuD 2018, 502 (504) und *Schwartmann*/*Weiß*, Entwurf für einen Code of Conduct zum Einsatz DSGVO konformer Pseudonymisierung, S. 21.

609 Zum Begriff *Hölzel*, DuD 2018, 502 (504) sowie *Petrlic*/*Sorge*, Datenschutz, S. 30 f.

Datensatzes gelöscht oder so vergröbert bzw. aggregiert werden, dass das Merkmal bei inhaltsgleichen Aussagen den gleichen Wert erhält.[610] Auch ließen sich die Datensätze im Rahmen des Möglichen verzerren oder randomisieren, indem die Daten in einem Datensatz bzw. einer Datenbank vertauscht (sog. Swapping)[611] oder durch Hinzufügen von Werten bzw. gleichmäßigem Erhöhen der Werte (z.B. alle Werte +10) „verfälscht" werden.[612] Letzteres ist aber nur dann möglich, wenn der (statistisch relevante) Aussagegehalt der Daten im Ergebnis erhalten bleibt. Eine Kombination beider Verfahrensrichtungen ist ferner in der Synthese der Datensätze zu sehen, die unter D.I.1.b)bb)(1) dargestellt wurde. Diese Bandbreite[613] zeigt, dass eine sichere Anonymisierung auf lange Sicht – allerdings nicht dauerhaft – durchaus möglich ist.

Eben aufgezeigte Möglichkeiten einer beständigen Anonymität und das zuvor aufgeworfene Ergebnis der fraglichen (absoluten) Anonymität stehen sich nun gegenüber, sind aber nur prima facie widersprüchlich. Der Widerspruch deutet lediglich darauf hin, dass die bisherige Regelungsweise im Datenschutzrecht sowie der Ausschluss anonymer wie anonymisierter Daten vom Grundrecht auf informationelle Selbstbestimmung dem grundrechtlichen Gewährleistungsverständnis zuwider läuft. Wenngleich Ansätze für eine sichere Anonymisierung in der Praxis bestehen, trägt die mangelnde Regelung weder zur Klarheit im Umgang mit derartigen Daten noch hinsichtlich einer sicheren Verarbeitung bei. Schon das Fehlen einer Definition zum Zwecke der Abgrenzung ist seit der Neufassung des BDSG zu bemängeln.[614] Weiter ist die Anonymisierung von Daten, die datenschutzrechtlich vereinzelt zum Schutz personenbezogener Daten gefordert wird[615], nur wenig etabliert worden. Im Bereich der IT-Sicherheit führt leider auch keine Erläuterung

610 *Hammer* in: Jandt/Steidle, Datenschutz im Internet, B.IV., Rn. 290; *Buchmann*, DuD 2015, 510 (511). Für Beispiele siehe *Petrlic*/*Sorge*, Datenschutz, S. 32 f.

611 *Hölzel*, DuD 2018, 502 (505).

612 *Artikel 29-Datenschutzgruppe*, Opinion 05/2014 on Anonymisation Techniques, S. 12; *Buchmann*, DuD 2015, 510 (511).

613 Weitere Verfahren aufzeigend *Artikel 29-Datenschutzgruppe*, Opinion 05/2014 on Anonymisation Techniques, S. 11 ff.

614 Daher ebenso eine klare Definition fordernd *Winter*/*Battis*/*Halvani*, ZD 2019, 489 (490).

615 Beispielsweise *Buchner/Tinnefeld* in: Kühling/Buchner, DSGVO, Art. 89 DSGVO, Rn. 17.

im Rahmen des BSI-Grundschutz-Kompendiums dazu, dass sich Anonymisierungspraktiken zumindest als freiwillige Standards etablieren.[616] Die begriffliche Unsicherheit erstreckt sich dann auch über den Umgang mit anonymen/anonymisierten Daten und führt zum Trugschluss, dass einmal anonyme Daten immer anonym bleiben – wenngleich das Datenschutzrecht die Prüfungspflicht in einem bloß zur Auslegung zu beleihenden Erwägungsgrund der DSGVO einbezieht. So übersehen, gerät die Weitergabe anonymisierter Daten an Dritte, die womöglich einen Personenbezug herstellen können und der Weitergebende hierüber in Unkenntnis ist, zur Gefährdung der informationellen Selbstbestimmung des Datensubjekts. Schließlich gelten für anonyme wie anonymisierte Daten keine Regelungen zur Information über die Datenweitergabe; das Datenschutzrecht ist nicht anwendbar, es gibt eine derartige Regelung schlichtweg nicht. Das datenschutzrechtliche wie verfassungsrechtliche Ziel, personenbezogene Daten vor den Gefahren des technischen Fortschritts zu schützen, kann auf diese Weise nicht erfüllt werden. Zwangsnotwendig, auf Basis der Schutzpflichten aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG[617] sowie zur Herstellung der Rechtsklarheit und Bestimmtheit gem. Art. 20 Abs. 1, Abs. 3 GG, bedarf es hier einer Nachrüstung sowie Wächterposition des Staates zur Absicherung des Grundrechtsschutzes. Als Vorbild kann hierbei das japanische Modell dienen, welches umfassend auf Begriffsdefinition, geeignete Anonymisierungspraktiken, Datensicherheit, Informationspflichten usw. eingeht.[618]

Vor diesem Hintergrund ist der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung sowohl für pseudonyme wie anonyme digitale Identitäten eröffnet. Für originäre Pseudonyme wie nachträglich pseudonymisierte Daten ergibt sich kein Unterschied in der Ermittlung des Personenbezugs – das Pseudonym

616 Die Abschnitte CON.1 „Kryptokonzept“ und CON.2 „Datenschutz“ enthalten hierzu keine Informationen – siehe https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html. Zur Wirkung des Grundschutz-Kompendiums als „Soft Law“ *Djeffal*, MMR 2019, 289 (292). Die daraus resultierende Lücke kritisierend *Gehrmann*/*Voigt*, CR 2017, 93 (98).

617 Zur Schutz- und Gewährleistungsverantwortung des Staates ausführlich *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 17 ff.

618 *Geminn*/*Laubach*/*Fujiwara*, ZD 2018, 413 (417 ff) sowie *Roßnagel*/*Geminn*, ZD 2021, 487 (490).

dient lediglich als Instrument des (Selbst-)Datenschutzes zur Segregation der Informationsverteilung. Anonyme Daten fallen zwar nicht unmittelbar unter den durch das Bundesverfassungsgericht ausdefinierten Schutzbereich, sind allerdings in der Reflexwirkung dennoch diesem Grundrecht zuzuordnen. Dies als weitere (eigenständige) Ausprägung des Allgemeinen Persönlichkeitsrechts zu begreifen würde die Ausbildung des Grundrechts auf informationelle Selbstbestimmung nur demontieren. Dogmatisch nachvollziehbarer ist es, das Grundrecht um diese Komponente zu erweitern. Demgemäß wäre jedes Datum vom grundrechtlichen Schutz umfasst, was in seiner Wirkung mit dem absoluten Verständnis des Personenbezugs gleich gesetzt werden könnte. Dem ist jedoch zu entgegnen, dass die relative Betrachtungsweise des Personenbezugs für die Ermittlung des (grundrechtlichen) Risikos für die betroffenen Personen ebenso notwendig ist und sich der Schutz der verschiedenen Sphären – also direkter Personenbezug, indirekter Personenbezug u.a. bei Pseudonymen und Anonymität mit geringem bis nicht bestehendem Personenbezug – in einfachgesetzlicher wie grundrechtlicher Hinsicht unterscheidet. Nur so kann die einst durch das Bundesverfassungsgericht gewählte Losung „Es gibt kein belangloses Datum.“[619] umgesetzt werden, wenn die Relevanz bzw. das Risiko jeden Datums einzelfallbezogen berücksichtigt wird. Gerade bei Datensammlungen wie der digitalen Identität drängt sich diese Betrachtungsweise auf.

Als Konsequenz ist die eben dargestellte Würdigung des Personenbezugs auf die Verhältnismäßigkeitsprüfung zu übertragen. Ausgehend davon, dass sich eine feststehende Einordnung in die aufgeführten Begrifflichkeiten nicht umsetzen lässt und vielmehr ein dynamisch-kontextuelles Verhältnis vorliegt, bedarf es einer entsprechenden Anpassung im Rahmen der Verhältnismäßigkeit. Notwendig ist hierzu zunächst der Personenbezug der digitalen Identität: Je nach Einordnung bei der Prüfung des Schutzbereiches ist zunächst zu differenzieren, ob die Daten bei der Erstellung der digitalen Identität originär anonym/pseudonym oder durch spätere Verarbeitung anonymisiert bzw. pseudonymisiert sind. Im ersteren Fall ergibt sich stets ein stärkeres Schutzniveau der Daten, da von Beginn an dem

619 BVerfGE 65, 1 (45).

Verantwortlichen keine Verknüpfung bzw. kein Rückschluss auf das Individuum bekannt ist.[620] Anders liegt der Sachverhalt, wenn der Zustand der Anonymität oder Pseudonymität erst hergestellt wird, sodass es besonderer Vorkehrungen bedarf – beispielsweise des erwähnten Löschens der Originaldaten oder auch eine Abschottung der anonymisierten/pseudonymisierten Datensätze[621]. Dies einbeziehend, besteht ein unterschiedliches Gewicht bei einer Abwägung für jeweils direkt personenbeziehbare, pseudonyme/pseudonymisierte und anonyme/anonymisierte digitale Identitäten. Zur weiteren Feststellung dieses Gewichts dient als Orientierung und Abstraktionsebene die durch Rechtsprechung[622] und Literatur[623] ausdifferenzierte Sphärentheorie des Allgemeinen Persönlichkeitsrechts. Sie soll in der Gesamtschau allerdings nicht zur Einführung strenger Grenzen zwischen Schutzgraden führen, sondern vielmehr die Sensibilität oder das Interesse an der

620 Vgl. *Härting*, NJW 2013, 2065 (2070); *Schleipfer*, ZD 2020, 284 (284, 287 ff).

621 *Hammer* in: Jandt/Steidle, Datenschutz im Internet, B.IV., Rn. 287.

622 Zur Intimsphäre: BVerfGE 6, 32 (41); 27, 1 (6); 34, 238 (245 f); 38, 316 (320). Zur Privatsphäre: 27, 344 (350); 34, 238 (245); 35, 202 (220); 44, 197 (203). Zur Sozial- und Öffentlichkeitssphäre: BVerfGE 35, 35 (39); 35, 202 (220); 80, 367 (373).

623 *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 103 ff; *Degenhart*, JuS 1992, 361 (363 f). Im Detail auch *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 72 ff; *Rudolf* in: Merten/Papier, HGr IV, § 90, Rn. 67 ff.

Privatheit des Datums im Kontext der digitalen Identität ausmachen.[624] Gradmesser dieser Theorie ist die Nähe des persönlichkeitsrechtlichen Sachverhalts zur Menschenwürde bzw. der Intimsphäre als letzter „Kernbereich privater Lebensgestaltung“[625]. Als Kontrapunkt dazu dient die Öffentlichkeits- bzw. Sozialsphäre[626], die durch den Bezug zur Allgemeinheit geprägt ist. Ein Überwiegen der

624 Die Sphärentheorie im Bereich der informationellen Selbstbestimmung ablehnend *Nebel*, ZD 2015, 517 (519 f), ähnlich auch *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 106; *Kunig*, Jura 1993, 595 (602 f). Dementgegen *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 77; *Rudolf* in: Merten/Papier, HGr IV, § 90, Rn. 67; *von Mutius* in: Bäumler/von Mutius, Anonymität im Internet, 11 (19, 21 f, 24 f) und ausführlich *Luch*, Medienpersönlichkeitsrecht, S. 123 f. Letzterer Ansicht ist schon deshalb zuzustimmen, weil die von *Nebel* behauptete Abkehr des BVerfG von der Sphärentheorie hinsichtlich des Grundrechts auf informationelle Selbstbestimmung nicht besteht. Vielmehr nimmt das BVerfG in seiner Tagebuch-Entscheidung ausdrücklich eine Einordnung in die Sphären vor, beschränkt sich aufgrund des Sachverhalts lediglich auf die Intimsphäre als (letzter) Kernbereich privater Lebensgestaltung – siehe nur BVerfGE 80, 367 (374). Dies berücksichtigt wider Erwarten auch *Kunig*. Folglich geht es zumindest von zwei Bereichen aus, nämlich Intim- und Privatsphäre – dieser Ansicht auch *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 285 mwN. Darüber hinaus berücksichtigt *Nebel* nicht, dass in der Entscheidung zur Online-Durchsuchung im Jahr 2008 das BVerfG erneut die Sphären in Erwägung zieht. Es stellt jedoch fest, dass eine genaue Zuordnung des Datums oft nicht vorgenommen werden kann. „Das hat zur Folge, dass mit der Infiltration des Systems nicht nur zwangsläufig private Daten erfasst werden, sondern der Zugriff auf alle Daten ermöglicht wird, so dass sich ein umfassendes Bild vom Nutzer des Systems ergeben kann.“ Es geht daher über den Schutz der Privatsphäre hinaus – so BVerfGE 120, 274 (311 f). Dies wird auch in der Entscheidung zur Vorratsdatenspeicherung – BVerfGE 125, 260 (319) – bekräftigt, indem die Vertraulichkeit der Informationen in Bezug zur Intimsphäre gesetzt wird. Insofern kann höchstens ein Abrücken von einer strengen Einordnung in digitalen Belangen darin gesehen werden, nicht jedoch eine vollständige Abkehr von verschieden geschützten Lebensbereichen in Form der Sphären. Andernfalls bliebe die bis zuletzt vom BVerfG vertretene Lehre vom unantastbaren Kernbereich unberücksichtigt, die es ohne eine Sphärentheorie nicht gäbe. Gerade jene Vertreter der Ansicht, welche die informationelle Selbstbestimmung als bloße Ausprägung des Allgemeinen Persönlichkeitsrechts ansehen, müsste ein Versagen der Sphärentheorie aus dogmatischer Sicht fremd sein.

625 BVerfGE 109, 279 (314); 120, 274 (335); 141, 220 (276 f). *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 75 ff; *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 106.

626 Beide Begriffe differenzierend *Degenhart*, JuS 1992, 361 (364), wobei die Sozialsphäre sich lediglich im Informationsaustausch mit anderen Menschen ergibt und es für die Öffentlichkeitssphäre nicht auf einen bestimmten Empfänger/Adressaten ankommt. Davon ist aber die private, familiäre Kommunikation zu unterscheiden, welche Teil der Privatsphäre ist.

Allgemeininteressen im Abwägungsprozess ist hier schon nicht notwendig aufgrund der mangelnden Nähe zum Kernbereich.[627] Dazwischen befindet sich die Privat- bzw. Geheimsphäre, die eines Eingriffes nur bei überwiegenden Interessen der Allgemeinheit und bei Wahrung des Verhältnismäßigkeitsgebots zugänglich ist. Sie zeichnet sich gerade dadurch aus, dass sie als bewusst bzw. selbstbestimmt ausgeformter Bereich privater Lebensgestaltung – räumlich wie sachlich – der Öffentlichkeit (partiell) entzogen ist.[628]

Diese Grundsätze sind auf die Abwägung des Schutzes digitaler Identitäten als Teil der informationellen Selbstbestimmung mit kollidierenden Interessen formelhaft zu übertragen: Je näher der informationelle Gehalt der digitalen Identität der Menschenwürde ist, desto schützenswürdiger ist das Interesse des Grundrechtsträgers und desto höher ist es zu gewichten. Diese Qualität des Datums wird durch die Verknüpfung von personenbezogenen Daten zu einer digitalen Identität signifikant erhöht. Darin verwirklicht sich auch das Kriterium der Quantität bzw. „Datenmasse". Beide Aspekte greifen sodann die seit dem Volkszählungsurteil vom Bundesverfassungsgericht geäußerte Gefahr vor Verknüpfungsmöglichkeiten auf, welche Teil der Begründung für das Grundrecht auf informationelle Selbstbestimmung ist.[629]

Überdies kann die Stärke des Personenbezugs als Indiz für die Sensibilität der Inhalte – und damit eine Nähe zur Menschenwürde des Art. 1 Abs. 1 GG – herhalten. Je weniger qualitativ bzw. „reich" der Datensatz an Informationen über persönliche Angaben ist – so z.B. bei anonymen digitalen Identitäten –, desto einschneidender ist eine Offenlegung und Anreicherung durch Verknüpfung oder andere Verarbeitungsvorgänge in das Grundrecht auf informationelle Selbstbestimmung. Grundlage dessen ist die Überlegung, dass bewusst anonym angelegte

627 Vgl. BVerfGE 101, 361 (370); *Degenhart*, JuS 1992, 361 (364). Vertiefend zum Sozialbezug *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 43 f; *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 316 f.

628 BVerfGE 44, 197 (203); 90, 255 (260); vgl. auch E 101, 361 (368, 373 f). *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 277 f; *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 79 f; *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 38 f; *Kloepfer*, VerfR II, § 56, Rn. 53; *Degenhart*, JuS 1992, 361 (364).

629 Siehe nur BVerfGE 65, 1 (45).

Identitäten regelmäßig dazu dienen, die wahre Identität zu verbergen und ein Geheimhaltungsinteresse des Grundrechtsträgers zum Ausdruck bringen. Anonymität und Selbstbestimmtheit müssen heute mehr denn je bewusst und proaktiv hergestellt werden, um die stetig gegebene Personenbeziehbarkeit bei der Nutzung des Internets zu unterbrechen.[630] Hingegen ist bei einer zumindest partiellen Verknüpfung ähnlich einem pseudonymen/pseudonymisierten Datenbestand die Stärke der Belastung abzusprechen, spricht doch durch die einseitige Information des Diensteanbieters und die qualitative Anonymität gegenüber anderen Dienstenutzern für eine selbstbestimmte Informationsweitergabe. In der Parallelwertung entspricht dieses Verhältnis dem der Privatsphäre, wo beispielsweise Informationen im Rahmen von Gesprächen nur einem engen Personenkreis offengelegt werden und nicht notwendigerweise ein digitales Sakrosankt darstellen. Das führt jedoch nicht zu einem mangelnden Schutz, denn das mit der Weitergabe der Daten verbundene Missbrauchsrisiko wird durch einfachgesetzliche wie verfassungsrechtliche Prinzipien des Datenschutzes aufgefangen, unter anderem der Zweckbindung[631] oder der Datenminimierung iSe Erforderlichkeitsprüfung bei der Datenerhebung[632]. Digitale Identitäten, die Informationen öffentlich teilen – vergleichbar mit dem öffentlich einsehbaren Profil bei sozialen Netzwerken[633] –, entsprechen dagegen vielmehr der Sozial- bzw. Öffentlichkeitssphäre. Das jeweilige Eindringen in diese Bereiche, die fast schon einer virtuellen Räumlichkeit des Internets anmuten, bedarf dann der eingangs aufgeführten berechtigten Interessen zur Rechtfertigung des Eingriffs. Darüber hinaus ist in die Einordnung auf dieser Skala der (damit verknüpfte) Inhalt der digitalen Identität einzubeziehen. Unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts zur Auswertung von Tagebüchern ist entscheidend, ob es sich um Informationen handelt, die aufgrund ihrer Eigenart einer Sphäre angehören.[634] Beispielsweise

630 Ähnlich *Tucker*, MIT Technology Review 4 (2013), 64 f. Hierzu sogleich Kapitel D.I.1.b)bb)(3).
631 *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2 I, Rn. 116 f.
632 Vgl. *Herbst* in: Kühling/Buchner, DSGVO, Art. 5 DSGVO, Rn. 57; zutreffend als Teil der Verhältnismäßigkeitsprüfung prüfend *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 5 DSGVO, Rn. 120.
633 Vgl. zur Höchstpersönlichkeit nicht-öffentlich zugänglicher Inhalte eines Nutzerkontos BGH, Urteil vom 12.7.2018, Az. III ZR 183/17, Rn. 39 – zitiert nach juris.
634 Vgl. BVerfGE 80, 367 (374 f).

kann dies für die datenschutzrechtlich besonders geschützten besonderen personenbezogenen Daten iSd Art. 9 Abs. 1 DSGVO angenommen werden, wobei sich eine Intimität insbesondere in den Daten zur sexuellen Selbstbestimmung, der Gesundheit oder politischen Gesinnung zurechnen lässt.[635] Abseits dieser aus der höchst subjektiven Prüfung[636] der Sphärentheorie stammenden Indizien wirkt sich auch die Art und Weise der Datenerlangung auf die Verhältnismäßigkeit aus, u.a. die Heimlichkeit der Maßnahme oder die Anlass- und Verdachtsbezogenheit der Erhebung.[637]

Der Schutz der digitalen Identität ist demnach abhängig vom Personenbezug der Datensammlung. Doch nicht nur der Gehalt wirkt sich auf den Umfang und die Stärke grundrechtlichen Schutzes aus, auch die Variante der Aufbewahrung und Nutzung sind wertend einzubeziehen. Im Rahmen des Schutzbereiches ergibt sich so ein breit aufgestellter Schutz, bei dem lediglich die Anonymität zu Problemen führt. Diese können aber durch eine – dogmatisch notwendige – Öffnung des Schutzbereiches der informationellen Selbstbestimmung und einfachgesetzliche Anpassungen umgangen werden. Ferner findet die Stärke des Personenbezugs sich im Abwägungsprozess wieder, um je Einzelfall eine verhältnismäßige Wertung im Kontext der Datennutzung zu ermöglichen. Hierbei gibt der Grad des Personenbezugs Aufschluss darüber, wie privat oder intim die digitalen Aspekte der Identität sind. Weiterhin sind in die Bewertung der eigentliche Informationsgehalt und die bestehende Verkettung sowie eine potentielle Verkettbarkeit der digitalen Identität mit weiteren Datensätzen aufzunehmen. Mangels fester Grenzen zwischen digitalen Sphären, deren Einordnungsschwierigkeit sich schon am relativ festzustellenden Personenbezug entzündet, ist eine dynamische und einzelfallabhängige Prüfung der Verhältnismäßigkeit vonnöten. In dieser Hinsicht besteht aber kein Unterschied zur üblichen Prüfung der Sphärentheorie.[638] Hierfür spricht insbesondere die Rollenprägung der digitalen Identität, welche in der

635 Siehe auch die ausführliche Aufschlüsselung anhand der Stufentheorie von *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2 I, Rn. 118.

636 So klassifizierend *Nebel*, ZD 2015, 517 (517).

637 Diese und weitere Kriterien aufführend *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 77.

638 *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 80.

begrifflichen Herleitung bereits dargestellt wurde und sich auch in den Facetten des Persönlichkeitsrechts wiederfindet.[639]

(3) Digitale Identitäten ohne Kenntnis und/oder Einwilligung Eine weitere Unterscheidung bei der Betrachtung digitaler Identitäten ist aus praktischen Erwägungen vorzunehmen. Auf Basis des weit gefassten Begriffes der digitalen Identität ist nicht ausgeschlossen, dass sie auch gegen oder ohne den Willen des gewöhnlichen Internetnutzers angelegt und verwaltet wird. In letzteren Fällen mangelt es sowohl an Kenntnis als auch an einer Einwilligung über die Datenverarbeitung. Alternativ kann es auch nur an einem der beiden Kriterien – Kenntnis bzw. Bewusstsein und Einwilligung – fehlen. Folglich ist ebenso auf diesen Ebenen zu ermitteln, inwiefern die Einwilligung auf die digitale Identität und den verfassungsrechtlichen Schutz Einfluss nimmt. Dazu wird nachstehend schrittweise sowohl der Schutz mit als auch ohne Einwilligung in Korrelation zur vorhandenen bzw. fehlenden Kenntnis untersucht. Dies wird auch nicht ohne einen Blick auf das geltende Datenschutzrecht zu bewerkstelligen sein.

Vorangestellt bedarf es aber einiger Ausführungen zum Hintergrund der Einwilligung und den verfassungsrechtlichen Wurzeln. Dem Allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG lassen sich nur geringfügig Aspekte der Einwilligung entnehmen, wenngleich sie Gegenstand persönlichkeitsrechtlicher Verfahren vor dem Bundesverfassungsgericht war bzw. ist.[640] Im Bereich des (ebenfalls unbenannten) Grundrechts auf informationelle Selbstbestimmung finden sich ebensowenig Anhaltspunkte im Wortlaut der Verfassung, auch nicht in einem Teil der Wurzel – namentlich der Handlungsfreiheit des Art. 2 Abs. 1 GG als Kern des Grundrechts[641]. Vielmehr ist erneut der Ursprung des Grundrechts – die Volkszählungsentscheidung des BVerfG – zu beleihen, um das Grundrecht in

639 Siehe dazu Kapitel B.I. Hinsichtlich der Rollenprägung der Sphärentheorie siehe *Nebel*, ZD 2015, 517 (517/518).

640 Siehe nur BVerfGE 101, 361 (391).

641 So *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 28, 32 und *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 63, bezugnehmend auf BVerfGE 27, 344 (351) = NJW 1970, 555. Vgl. auch *Jarass* in: Jarass/Pieroth, GG-Kommentar, Art. 2, Rn. 38.

dieser Hinsicht zu definieren. Rein begrifflich setzt die informationelle Selbstbestimmung auch die Möglichkeit voraus, die Selbstbestimmung aktiv auszuüben. Ein bloßes Verharren in der Rolle des Abwehrrechts entspricht zumindest weniger besagter Wurzel des Grundrechts in Art. 2 Abs. 1 GG. Vielmehr setzt die individuelle Selbstbestimmung voraus, „daß [sic] dem Einzelnen [die] Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten".[642] Damit umfasst das Grundrecht „die Befugnis des Einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen".[643] Sie ist damit als elementare Funktionsbedingung für das freiheitlich-demokratische Gemeinwesen zu verstehen, die auf Art. 2 Abs. 1 GG zurückzuführen ist[644] und das Hauptinstrument der Datensouveränität darstellt[645]. Dies schließt die bereits erläuterten Informations- und Auskunftsrechte ebenso ein, beispielsweise das Recht auf Korrektur bzw. Richtigkeit der Daten.[646] Weiter ist als actus contrarius auch der Entzug der Einwilligung in Form des Widerrufes vom verfassungsrechtlichen wie funktionalen Verständnis umfasst. All diese einzelnen, durch die einfachen Gesetze konkretisierten Handlungen dienen dazu, die Grundrechtsausübung des Art. 2 Abs. 1 iVm 1 Abs. 1 GG zu ermöglichen oder zumindest zu begünstigen. So führen Informationsrechte unter Umständen erst dazu, sich mit den einzelnen Verarbeitungszwecken auseinanderzusetzen und nicht in eine nicht erforderliche Verarbeitung einzuwilligen. Teil der (informationellen) Selbstbestimmung ist auch die eigenständige Überprüfung und darauf basierend das Ausrichten des Handelns. Darüber hinaus wird durch Einwilligung und Widerruf das eigenständige Verwalten der Rechte zur Datenverarbeitung ermöglicht. Wird konträr zum Dargelegten in der Einwilligung ein Grundrechtsverzicht gesehen – erkennt in der Einwilligung also die Aufgabe des Grundrechtsschutzes im

642 BVerfGE 65, 1 (42) – Einfügungen durch den Bearbeiter.
643 BVerfG, Beschluss vom 23.10.2006 – Az. 1 BvR 2027/02 –, Rn. 27 nach juris = DuD 2006, 817 (818 f) unter Verweis auf BVerfGE 65, 1 (43).
644 BVerfGE 65, 1 (43).
645 Vgl. *Krüger*, ZRP 2016, 190 (190).
646 So auch *Rudolf* in: Merten/Papier, HGr IV, § 90, Rn. 46 ff; *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 20, 81 ff.

Falle eines bevorstehenden Grundrechtseingriffs – ist dieser Ansatz unter Hinweis auf die bereits in Kapitel C. dargelegten Schutzkonzepte und ein unnötiges Überlappen des bereits inkludierten Schutzes der informationellen Selbstbestimmung abzulehnen.[647] Dem Grundrecht auf informationelle Selbstbestimmung ist ein umfassender status positivus immanent.

Eine Einwilligung in die Datenverarbeitung muss weiter bestimmte Voraussetzungen erfüllen, die sich nur ansatzweise dem Verfassungsrecht und überwiegend dem einfachgesetzlichen Datenschutzrecht entnehmen lassen. Während sich das Bundesverfassungsgericht einer Definition entzieht[648], kann nur auf die in der Literatur[649] und zunächst den Gesetzgeber ausgeformte Definition zurückgegriffen

647 Im Punkt der Differenzierung von Grundrechtsverzicht und -gebrauch sind sich die Meinungen in der Literatur einig – vgl. *Hufen*, Staatsrecht II, § 6, Rn. 42 sowie *Fischinger*, JuS 2007, 808 (809); *Kloepfer*, VerfR II, § 49, Rn. 69-70; *Geiger*, NVwZ 1989, 35 (37); ausführlich *Stern*, StaatsR III/2, § 86. Ebenfalls hat sich einheitlich herausgebildet, dass der Begriff des Grundrechtsverzichts zunächst fälschlicherweise mit dem Totalverzicht gleichgesetzt wurde – *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 1 Abs. 3, Rn. 301. Die weitere Differenzierung bewegt sich jedoch im Spektrum zwischen der Gleichsetzung von Einwilligung und Verzicht – so iE *Fischinger*, JuS 2007, 808 (813); scheinbar auch *Kingreen*/*Poscher*, Staatsrecht II, Rn. 193 f und *Robbers*, JuS 1985, 925 (927) – und einer terminologischen Trennung – so *Kloepfer*, VerfR II, § 49, Rn. 69-70; *Hufen*, Staatsrecht II, § 6, Rn. 43; *Stern*, StaatsR III/2, S. 893 ff; 905 ff. Im Hinblick auf das Persönlichkeitsrecht sowie das Grundrecht auf informationelle Selbstbestimmung besteht jedoch, wie angedeutet, auch ein status positivus. In dieser Hinsicht braucht es gerade nicht der Terminologie des Verzichts, da eine Grundrechtsausübung schon durch das jeweilige Grundrecht mitgeschützt wird – so *Stern*, StaatsR III/2, S. 908 sowie *Geiger*, NVwZ 1989, 35 (37), iE daher differenzierend *Jarass*, NJW 1989, 857 (860). Das Gleichsetzen von Einwilligung und Verzicht, wie es *Fischinger* vorschlägt, verkennt die verfassungsrechtliche Dogmatik in diesem Punkt und basiert im Schwerpunkt auf Folgerungen des Strafrechts (siehe *Fischinger*, JuS 2007, 808 (810)), wie einst auch *Amelung* – siehe kritisch in diesem Punkt *Stern*, StaatsR III/2, S. 905 f. Folglich ist der Differenzierung von Grundrechtsverzicht und Einwilligung anzuschließen, die Einwilligung also als Grundrechtsausübung zu verstehen. So iE auch BVerfG, Beschluss vom 23.10.2006 – Az. 1 BvR 2027/02 –, Rn. 27 nach juris = DuD 2006, 817 (818 f); *Klement* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 7, Rn. 18 f; *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2 I, Rn. 228 f; vgl. *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 8 GRC, Rn. 20;*Bleckmann*, JZ 1988, 57 (60).

648 Siehe nur BVerfGE 34, 238 (245, 247), wo lediglich das Fehlen einer Einwilligung moniert wird. Auch die erneute Auseinandersetzung mit selbiger Materie anlässlich der Überprüfung der Volkszählung 2011 greift nur bestehende Judikatur auf und stellt einzelne Kriterien etwas deutlicher heraus – siehe BVerfGE 150, 1 (Rn. 218-227) = NVwZ 2018, 1703 (1714 f).

649 *Geiger*, NVwZ 1989, 35 (36); *Kunig*, Jura 1993, 595 (600 f); *Jarass*, NJW 1989, 857 (860).

werden. Dabei ist in der Auslegung auch Art. 8 Abs. 2 GrC zu berücksichtigen, worin die Einwilligung ausdrücklich als eingriffsausschließender Legitimationsgrund[650] genannt wird, geknüpft an eine entsprechende Zweckbenennung.[651] Einfachgesetzlich ist Art. 4 Nr. 11 DSGVO zu betrachten, welcher Ansätze des nationalen Verständnisses gem. § 4a BDSG a.F.[652] enthält. So statuiert dieser ebenso, dass die Einwilligung unmissverständlich und in informierter Weise abgegeben werden muss. Artikel 7 DSGVO erweitert die Definition unter anderem um das Kriterium der Freiwilligkeit der Willensbekundung.[653] Dem Kriterium der Informiertheit kommt im Lichte des datenschutzrechtlichen wie verfassungsrechtlichen Transparenzerfordernisses ein definitorischer Schwerpunkt zu und kann in der Kenntnis über den Einwilligungsinhalt[654] zusammengefasst werden. Davon ist das Einwilligungsbewusstsein iSe Erklärungsbewusstseins – also die Kenntnis vom Umstand, eine rechtserhebliche Erklärung abzugeben – zu differenzieren.[655] Ein Umgang mit den eigenen, personenbezogenen Informationen setzt stets ein Verständnis der Weitergabe und der daran gebundenen Folgen voraus. Rekurrierend auf den Gedanken der Privatautonomie des Art. 2 Abs. 1 GG[656] dient diese Transparenz – gerade in Missverhältnissen von Wissen oder Machtpositionen

650 Ganz h.M., siehe *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 8 GrC, Rn. 20; *Jarass* in: Jarass, GrC-Kommentar, Art. 8, Rn. 9; *Kühling/Raab* in: Kühling/Buchner, DSGVO, Einführung, Rn. 29.

651 *Bernsdorff* in: Meyer/Hölscheidt, GrC-Kommentar, Art. 8, Rn. 28; *Kühling/Raab* in: Kühling/Buchner, DSGVO, Einführung, Rn. 29.

652 § 4a BDSG a.F.: „Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben."

653 Zu beiden Neuerungen siehe *Buchner*/*Kühling*, DuD 2017, 544 (545 f).

654 Zur Definition im Detail siehe *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7 DSGVO, Rn. 59; *Klement* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 7 DSGVO, Rn. 72 f; *Heckmann/Paschke* in: Ehmann/Selmayr, DSGVO, Art. 7, Rn. 58. Lösungen zur Umsetzung der informierten Einwilligung aufzeigend *Pollmann*/*Kipker*, DuD 2016, 378 (379 f).

655 Zum Begriff *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7 DSGVO, Rn. 56 f.

656 Zur sedes materiae der Privatautonomie siehe *Isensee* in: Isensee/Kirchhof, HStR VII, § 150, Rn. 57 f.

– dazu, Hemmnisse in der Grundrechtsausübung abzubauen und eine selbstbestimmtere Grundrechtsausübung zu ermöglichen. Weiter entsteht mit dem Vor-Augen-Führen der aus der Datenverarbeitung erwachsenden, möglichen Folgen auch eine Warnwirkung[657] aufseiten des Einwilligenden; die Konfrontation mit dem Einwilligungsgegenstand durch eine „aufgezwungene" geistige Auseinandersetzung fungiert als (vorübergehende) Schwelle. Wie erwähnt, greifen § 4a Abs. 1 BDSG a.F. sowie Art. 4 Nr. 11, 7 DSGVO auf die gleichen Grundsätze zurück und regeln zum Schutz grundrechtlicher Interessen aufkommende Kollisionen in mehrpoligen Verfassungsverhältnissen zwischen Privaten gleichermaßen wie die Datenverarbeitung durch öffentliche Stellen kraft Zustimmung. Zu den Gemeinsamkeiten zählen das faktisch grundsätzliche Schriftformerfordernis[658] gem. § 4a Abs. 1 S.3 BDSG a.F. sowie die expressis verbis freie Entscheidung über die Einwilligung im Falle des § 4a Abs. 3 S. 2 BDSG a.F. In der Gesamtschau der Regelungen kommt die zentrale Rolle der Einwilligung bei der Ausübung des Grundrechts auf informationelle Selbstbestimmung zur Geltung, deren Voraussetzungen auch nach der Novelle durch die DSGVO keinen minderen Schluss zulassen. Trotzdem ist Vorsicht geboten vor einer Aushöhlung der Einwilligung bzw. Selbstbestimmung durch das Meiden anderer, ggf. geeigneter Rechtfertigungstatbestände des Art. 6 Abs. 1 DSGVO.[659]

657 Vgl. *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7 DSGVO, Rn. 59; *Heckmann/Paschke* in: Ehmann/Selmayr, DSGVO, Art. 7 DSGVO, Rn. 57 f; als Sensibilisierung für die Datenverarbeitung/Profilbildung bezeichnend *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 246. Bislang wurde diese durch die Schriftform der Einwilligung erfüllt, siehe *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7 DSGVO, Rn. 27; *Krohm*, ZD 2016, 368 (369). Mit Wegfall dieser Voraussetzung verlagert sich diese Funktion über auf die Ausdrücklichkeit der Einwilligung, wie *Heckmann/Paschke* in: Ehmann/Selmayr, DSGVO, Art. 7, Rn. 36 hervorhebt.

658 Zumindest kann die Beweislast-Regelung des Art. 7 Abs. 1 DSGVO dahin tendierend gelesen werden, dass die Schriftform als rechtssicherste Nachweisform im Grundsatz gewünscht ist. Andere Nachweisarten sind jedoch nicht ausgeschlossen. So auch *Stemmer* in: Wolff/Brink, BeckOK DatenschutzR, Art. 7 DSGVO, Rn. 89 f; *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7 DSGVO, Rn. 27; *Klement* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 7 DSGVO, Rn. 40.

659 Kritisch *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7 DSGVO, Rn. 10 f, 16 f sowie einst *Buchner*, DuD 2010, 39 (40).

Bezugnehmend auf ebendiese gilt es nun, die unterschiedlichen Schutzebenen der digitalen Identität in Bezug auf die Einwilligung sowie die bloße Kenntnis von der Datenverarbeitung herauszuarbeiten. Dabei sind das Bewusstsein über die Datenverarbeitung („Ob“[660]) und die Informiertheit hinsichtlich der Einwilligung nicht synonym, sondern ersteres Teil der Informiertheit. Unter Umständen kann das Bewusstsein auch erst durch die Information eintreten, gerade wenn es sich um eine Auftragsverarbeitung handelt oder eine Datenverarbeitung für den Nutzer sonst nicht ersichtlich ist. Aufgrund der engen Verknüpfung von Informiertheit und Transparenzgebot (verfassungsrechtlich wie datenschutzrechtlich) geht ein mangelndes Wissen über Zweck und Umstände der Datenverarbeitung („Wie“[661]) regelmäßig auf einen Mangel an Transparenz zurück, sei es beispielsweise durch fehlende Informationen oder Verklausulierungen und nicht wie gefordert „in einer klaren und einfachen Sprache“[662]. Umgekehrt können subjektive Faktoren oder Expertenwissen ein Informiertsein schon im Vorfeld auslösen. Unabhängig von beiden Extremen ist im Grundsatz für die Bewertung der Transparenz die Sicht des Durchschnittsadressaten bzw. der beabsichtigten Nutzer- oder Zielgruppe maßgeblich.[663] Demgemäß können die unternehmerische Transparenz und das tatsächliche Bewusstsein über die Datenverarbeitung auch unabhängig voneinander bestehen, wenn der Verantwortliche trotz Kenntnis auf Seiten des Datensubjekts nicht seinen Transparenzpflichten nachkommt. Eine bloß subjektive Informiertheit darf sich nicht positiv für den Datenverarbeitenden auswirken, ihn also von seiner Verantwortlichkeit – einfachgesetzlich wie in mittelbarer Drittwirkung – entbinden. Deshalb ist im Folgenden die bewusste und informierte Einwilligung, die informierte Verarbeitung ohne Einwilligung und die sowohl unbewusste als auch uninformierte Verarbeitung von digitalen Identitäten zu differenzieren. Eine uninformierte Einwilligung ist rechtswidrig und damit nicht einzubeziehen.[664]

660 Ähnlich bezeichnend auch *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 97.
661 Ähnlich bezeichnend auch *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 98.
662 Art. 7 Abs. 1 S. 1 DSGVO.
663 Vgl. ErwGr 39, 58 DSGVO; *Bäcker* in: Kühling/Buchner, DSGVO, Art. 12 DSGVO, Rn. 11; *Quaas* in: Wolff/Brink, BeckOK DatenschutzR, Art. 12 DSGVO, Rn. 12, 15.
664 *Heckmann/Paschke* in: Ehmann/Selmayr, DSGVO, Art. 7, Rn. 61.

Verarbeitung auf Basis einer Einwilligung

Hat der Grundrechtsträger durch die Information des Diensteanbieters qua Datenschutzerklärung oder auf anderem Wege einen entsprechenden Kenntnisstand erlangt und steht ihm die Möglichkeit der Einwilligung offen, so sind keine Probleme ersichtlich. Dabei wird ebenfalls davon ausgegangen, dass sich keine anderen Mängel wie eine Kopplung iSd Art. 7 Abs. 4 DSGVO[665] vorliegt; die Rechte der Art. 12 ff DSGVO werden ebenfalls gewahrt. Insofern kann die informationelle Selbstbestimmung iSd Art. 2 Abs. 1 iVm 1 Abs. 1 GG vollwertig ausgeübt werden.

Verarbeitung ohne Einwilligung trotz Kenntnis

Interessanter ist die Situation einer Datenverarbeitung, die mit Kenntnis des Grundrechtsträgers vorgenommen wird, es allerdings an einer Einwilligung fehlt. Insofern ist der Verantwortliche der Datenverarbeitung nicht von Informationspflichten freigestellt (siehe Art. 13 DSGVO) und muss auch die weiteren Rechte der Art. 12 ff DSGVO grundsätzlich vorsehen. Sodann ist auf die verbleibenden Rechtfertigungsgründe im Datenschutzrecht zurückzugreifen, da es sich dennoch um eine Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung handelt. Im Folgenden sind daher geeignete Rechtfertigungsgründe zur Erhebung und Verarbeitung digitaler Identitäten überblickshaft darzustellen.

Zunächst kann eine solche Konstellation bei einer Datenverarbeitung zum Zwecke der Vertragserfüllung iSd Art. 6 Abs. 1 lit. b DSGVO auftreten. Der Umstand der Vertragserfüllung ist dabei weit zu definieren, sodass sowohl die Datenverarbeitung im Wege einer Vertragsanbahnung sowie zur Erfüllung von Neben- und Rücksichtnahmepflichten ebenfalls darunter zu subsumieren sind.[666] Einem Kunden ohne Nutzerkonto eines Online-Shops ist bei der Bestellung regelmäßig bewusst, dass die Adresse zu Versand und Empfang der Bestellung notwendig

665 Zum Begriff *Klement* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 7 DSGVO, Rn. 57 f; *Ernst*, ZD 2017, 110 (111). Ausführlich hierzu *Engeler*, ZD 2018, 55 (58 ff).

666 *Albers/Veit* in: Wolff/Brink, BeckOK DatenschutzR, Art. 6 DSGVO, Rn. 40 ff; *Wilmer* in: Jandt/Steidle, Datenschutz im Internet, B.II., Rn. 31.

ist. Anderenfalls kann das Vertragsverhältnis nicht erfüllt werden. Jedoch darf es sich aus Gründen der Datensparsamkeit sowie des Wortlautes des Art.6 Abs. 1 lit. b DSGVO lediglich um erforderliche Daten handeln – Vorlieben oder zuletzt betrachtete Artikel sind demnach nicht zu speichern, außer es ist für die laufende Browsing-Session notwendig. In letzterem Fall würde für den Nutzer ein sog. Session Cookie angelegt werden, wenn z.B. in besagtem Online-Shop der gefüllte Warenkorb auch kurzzeitig nach dem Verlassen der Webseite fortbestehen soll.[667] Durch dieses Hilfsmittel wird der Nutzer auch beim erneuten Besuch wiedererkannt. Dennoch müssen die Daten (z.B. die dazugehörige Cookie-ID) anschließend gelöscht werden. Sie dürfen unter diesem Zweck nicht außerhalb der Session zur Analyse und Auswertung zur Einblendung personalisierter Werbung verwendet werden.[668]

Des weiteren kann ein Anlegen und Nutzen der digitale Identität dann gerechtfertigt sein, wenn der Verantwortliche die Daten zur Erfüllung einer normierten oder auferlegten rechtlichen Verpflichtung verarbeitet, Art. 6 Abs. 1 lit. c DSGVO. Damit wirkt die Norm nicht selbst als Rechtfertigungsgrund, sondern fungiert nur als Einfallstor für das Datenschutzrecht der Mitgliedsstaaten oder übrige Regelungen innerhalb der DSGVO.[669] Die mitgliedsstaatliche Regelung muss allerdings ein Ziel von öffentlichem Interesse verfolgen und in einem angemessenen Verhältnis zum verfolgten legitimen Zweck stehen (Art. 6 Abs. 3 S.4 DSGVO), also verhältnismäßig sein. Als Beispiel kann hier die Erfüllung der Speicher- und Meldepflichten zur Telekommunikationsüberwachung aufseiten der Telekommunikationsdiensteanbieter genannt werden, wenn bei Vertragsschluss die Identitätsnachweise einschließlich personenbezogener Daten gem. § 172 Abs. 2 TKG beim

667 *Hellmann*, IT-Sicherheit, S. 156 f; *Eckert*, IT-Sicherheit, S. 154 f.
668 Vgl. auch das Rückspielverbot des ErwGr 162 S. 5 DSGVO – siehe hierzu BVerfG NVwZ 2018, 1703, Rn. 225.
669 *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 83.

Telekommunikationsdiensteanbieter hinterlegt werden. Die dabei erhobenen personenbezogenen Daten werden mithin zum Zweck der Strafverfolgung und Gefahrenabwehr, also zum Schutz der Bevölkerung und damit im öffentlichen Interesse, verarbeitet und dienen nicht der anlasslosen Vorratsdatengewinnung.[670]

Weitaus umfangreichere Aufmerksamkeit kommt dagegen Art. 6 Abs. 1 lit. e sowie lit. f DSGVO zu. Um eine Rechtfertigung für eine Datenverarbeitung mit Kenntnis des Grundrechtsträgers anzunehmen, muss diese nach lit. e zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erfolgen. Im Fokus stehen daher öffentliche verantwortliche Stellen oder nicht-öffentliche, private Stellen mit entsprechender Aufgabenzuteilung (z.B. Beleihung oder Auftragsverwaltung). Hierunter ist unter anderem die Datenverarbeitung zum Zwecke der Wahlwerbung zu fassen, sofern sie den demokratischen Zielen des Art. 38 Abs. 1 S. 1 GG dienlich ist.[671] Dabei sind die datenschutzrechtlichen Prinzipien wie die Unverkettbarkeit oder andere Aspekte der Datenminimierung zu berücksichtigen.[672] Mit Blick auf den Datenschutz-Vorfall um Cambridge Analytica, deren umfangreiche Datensätze auch zur Wahlwerbung im persönlichen Gespräch genutzt wurden,[673] ist die personalisierte Wahlwerbung bei Berücksichtigung der Grundsätze auszuschließen.[674] Ebensowenig darf im Anschluss an die Wahl die auf Basis der Wahlwerbung erstellte Datei durch weitere Daten, z.B. durch Verknüpfung mit der tatsächlich abgegebenen Stimme oder Dokumentieren von angeklickter Wahlwerbung, erweitert und mit angereicherten Profilen versehen werden.[675] Dies widerspricht insbesondere dem Grundsatz der geheimen Wahl gem. Art. 38 Abs. 1 1 GG, wenn

670 BVerfGE 130, 151 (187, 191).

671 ErwGr 56 DSGVO. Vgl. auch *Petri* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 9 DSGVO, Rn. 68.

672 *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 115.

673 Siehe hierzu https://netzpolitik.org/2018/wie-facebook-betroffene-ueber-den-datenfluss-an-cambridge-analytica-informiert/; https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

674 Hierzu ausführlich *Söbbing*, InTeR 2018, 182 (184 ff) sowie *Radke*, K&R 2020, 479 ff.

675 Ähnlich der durch die Österreichische Datenschutzbehörde beschiedene Fall in Bezug auf die Empfängerprofile der österreichischen Post – siehe zusammenfassend https://netzpolitik.org/2019/datenschutzgrundverordnung-18-millionen-euro-strafe-fuer-die-oesterreichische-post/.

der Verarbeitungszweck die Vorhersagbarkeit der Wahl ermöglicht. Höchstens eine stark anonymisierte Statistik ist möglich, um auch die bereits erläuterte record linkage[676] zu vermeiden. Dazu trägt letztlich auch bei, die Daten „spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten", § 50 Abs. 1 S. 3 BMG.

Zuletzt und umfangreich soll zu diesem Komplex Art. 6 Abs. 1 lit. f DSGVO – die Datenverarbeitung bei berechtigtem Interesse – am Beispiel des Trackings analysiert werden. Allgemein setzt diese Norm ein berechtigtes Interesse des Verantwortlichen oder Dritten voraus, welches die Interessen des Betroffenen bzw. Grundrechtsträgers überwiegt. Letzteres meint in der Regel das Grundrecht auf informationelle Selbstbestimmung, dem von vornherein schon eine hohe Schutzwürdigkeit zukommt.[677] Dieser Rechtfertigungsgrund in Form einer Interessenabwägung ist daher gegenüber anderen Rechtfertigungsgründen des Art. 6 Abs. 1 DSGVO iSe Auffangvorschrift und restriktiv anzuwenden.[678] Dennoch kann der Verantwortliche Interessen rechtlicher, tatsächlicher, wirtschaftlicher, künstlerischer oder ideeller Art vorbringen und so auf einen weiten Tatbestand zurückgreifen.[679] Diese finden sich dementsprechend in Grundrechten des Verantwortlichen, wie jene des Art. 12 Abs. 1, 14 Abs. 1 GG in unternehmerischen Belangen oder Art. 5 Abs. 1 S. 1 Alt. 1 und S. 2 Alt. 1 sowie 2 GG.[680] Weitere Interessen finden sich in den Beispielen des Erwägungsgrundes 47 S. 2, 6 und 7

676 Siehe S. 140.

677 Noch *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 148; mit Blick auf das Unionsrecht auch *Richter* in: Jandt/Steidle, Datenschutz im Internet, B.II., Rn. 65 f sowie *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 148. Vgl. *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 6 I DSGVO, Rn. 101; *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 257.

678 ErwGr 47 DSGVO; *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 410. Vgl. zur Wahlmöglichkeit ggü. der Einwilligung *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 6 I DSGVO, Rn. 88 f.

679 *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 146a; *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 6 I DSGVO, Rn. 98; *Richter* in: Jandt/Steidle, Datenschutz im Internet, B.II., Rn. 59. Vgl. auch ErwGr 47 DSGVO.

680 *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 6 I DSGVO, Rn. 98 mwN; *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 147.

sowie in technischer Hinsicht Erwägungsgrund 49 DSGVO. Alle Interessen werden jedoch durch eine umfangreiche Verhältnismäßigkeitsprüfung eingeschränkt, in die auch die datenschutzrechtlichen Grundprinzipien des Art. 5 Abs. 1 DSGVO sowie Art. 2 Abs. 1 iVm 1 Abs. 1 GG, Art. 8 GrC einzubeziehen sind. Folglich finden die Prinzipien von Treu und Glauben sowie Transparenz, Zweckbindung, Datenminimierung und Speicherbegrenzung als auch der Schutz der Integrität und Vertraulichkeit der Daten Anklang.[681] Als Voraussetzung der Datenminimierung, welche die Reduktion der Datenerhebung und Verarbeitung auf das zur Zweckerfüllung Nötige fordert[682], und in engem Zusammenhang mit der Zweckbindung[683], bedarf es einer Verhältnismäßigkeitsprüfung einschließlich besonderer Kriterien der Erforderlichkeit. Danach entfällt eine Rechtfertigung schon dann, wenn sich der beabsichtigte Zweck durch eine weniger invasive Datenverarbeitung erfüllen lässt.[684] Eine umfangreiche Profilbildung im Rahmen einer digitalen Identität widerspricht dem Schutz der Rechte und Freiheiten des Betroffenen: Je granularer das Profil, desto erheblicher der Eingriff und unverhältnismäßiger bzw. argumentationsbedürftiger erscheint grundsätzlich die Datenverarbeitung. Dies ist jedoch einzelfallabhängig, da nicht jegliche Profilbildung durch das Datenschutzrecht untersagt ist.[685] Um dies zu skizzieren, ist am Beispiel des Webtrackings die Vereinbarkeit von Informiertheit und Datenverarbeitungsvorgängen zu betrachten.

681 Zum Anwendungsmodus der Prinzipien als Interpretationslinie und Strukturprinzip einer objektiven Ordnung siehe *Roßnagel*, ZD 2018, 339 (344).

682 *Schantz* in: Wolff/Brink, BeckOK DatenschutzR, Art. 5 DSGVO, Rn. 25-26; *Herbst* in: Kühling/Buchner, DSGVO, Art. 5 DSGVO, Rn. 57.

683 *Herbst* in: Kühling/Buchner, DSGVO, Art. 5 DSGVO, Rn. 56.

684 *Schantz* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 6 I DSGVO, Rn. 100; *Roßnagel*, ZD 2018, 339 (340 f).

685 *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 153, jedoch auf eine starke Tendenz zum Überwiegen der Betroffenenrechte hindeutend *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 153.

Unter (Web-)Tracking kann jede Datenverarbeitung verstanden werden, die durch fortwährende Datenerhebung über zeitliche und technische Grenzen hinweg Informationen speichert und zusammenführt, um sie dann einem bestimmten Verarbeitungszweck zuzuführen.[686] Als Unterart hierzu zählen unter anderem das Retargeting und (Behavioral) Microtargeting. Retargeting weist mit dem Präfix „Re-" schon darauf hin, dass bereits ein Targeting stattgefunden haben muss und auf der gleichen Webseite zu einem späteren Zeitpunkt oder über andere Webseiten bzw. Endgeräte hinweg (sog. Cross-Domain-[687] und Cross-Device-Tracking[688]) ein erneutes Targeting – also ein zielgerichtetes und personalisiertes Ausspielen von Webinhalten (z.B. Werbung) – stattfindet. Dies geschieht regelmäßig über Wiedererkennungsmerkmale wie Werbe-IDs oder andere Praktiken.[689] Microtargeting zeichnet sich dagegen dadurch aus, dass es bei seiner Analyse großer Mengen personenbezogener Daten zur Erstellung von Persönlichkeitsprofilen bzw. digitalen Identitäten eine hohe Granularität des Profils beabsichtigt. Dadurch können beispielsweise Charakteristika oder kognitive und voluntative Schwächen prognostiziert werden.[690] Nanotargeting ist dabei die Steigerung des Microtargetings, zielt also direkt auf einzelne Nutzer und baut auf Profilen mit besonders hoher Granularität auf.[691] Die Unterarten zeichnen jedoch nur bestimmte Herangehensweisen aus, eignen sich in Kombination oder auch einzeln angewendet zu verschiedensten Zwecken. So kann das Tracking dazu dienen, statistische Erhebungen über die Besucher einer Webseite zu ermöglichen und die Reichweite der eigenen Plattform zu maximieren. In diesem Fall könnte es sich bei einem berechtigten Interesse des verantwortlichen Unternehmens aus Art. 12 Abs. 1 GG

686 *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 48 f; *Jandt* in: Jandt/Steidle, Datenschutz im Internet, A.I., Rn. 34; *Schleipfer*, ZD 2017, 460 (461).

687 *Jandt* in: Jandt/Steidle, Datenschutz im Internet, A.I., Rn. 34 sowie *Jandt*, PinG 2019, 145 (146).

688 Hierzu *Quinn* et al., White Paper Tracking, S. 14 f; *Jandt* in: Jandt/Steidle, Datenschutz im Internet, A.I., Rn. 34 sowie *Jandt*, PinG 2019, 145 (146); *Venzke-Caprarese*, DuD 2017, 577 (578); *Hanloser*, ZD 2018, 213.

689 *Venzke-Carparese*, DuD 2018, 156 (158); *Baumgartner/Hansch*, ZD 2020, 435 (435). Ausführlicher mit Beispielen *Venzke-Caprarese*, DuD 2017, 577.

690 *Ebers*, MMR 2018, 423 (423 f); *Quinn* et al., White Paper Tracking, S. 15 f.

691 Siehe *González-Cabañas* et al., Unique on Facebook: Formulation and Evidence of (Nano)targeting Individual Users with non-PII Data, S. 6, 10 f.

handeln, um das eigene Angebot zu optimieren. Eine anonyme oder pseudonyme, statistische Reichweitenanalyse ähnelt dann einer einfachen Kundenumfrage zur Zufriedenheit mit dem Angebot.[692] Andererseits wird das Tracking dazu verwendet, personalisierte Werbung zu generieren oder auf Basis der erhobenen Daten (nutzerspezifische) Preise zu berechnen. Beide Formen basieren im Regelfall auf einer Profilbildung auf Basis personenbezogener Daten. Grundsätzlich besteht ein proportionales Verhältnis zwischen dem berechtigten Interesse des Unternehmens zum Anlegen einer digitalen Identität und dem grund-/datenschutzrechtlichen Interesse des Datensubjekts, sodass Letzteres zunimmt, je aussagekräftiger und umfangreicher der Datensatz ist.[693] Ebenso muss in die Abwägung einbezogen werden, ob mit derartigen Maßnahmen aufseiten des Betroffenen der Datenverarbeitung vernünftigerweise gerechnet werden kann.[694] So besteht durchaus die Möglichkeit, bei einer länger andauernden Kundenbeziehung das Überwiegen des berechtigten Interesses des Unternehmens bzgl. der Direktwerbung anzunehmen.[695] Eine derartige personalisierte Werbung iSe direkten Ansprache unter Verwendung personenbezogener Daten (Name, Adresse) – sog. Direktwerbung[696] – ist im Einzelfall als berechtigtes Interesse zu sehen, das aufgrund Erwägungsgrund 47 S. 7 DSGVO keiner ausführlichen Abwägung bedarf. Zudem ist anzumerken, dass dies den Direktwerbenden nicht von weiteren datenschutzrechtlichen Pflichten wie der Information über das Widerspruchsrecht gem. Art. 21 DSGVO entbindet.[697] Gleichermaßen sind – ohnehin im Rahmen der Abwägung des Art. 6

692 Vgl. *Venzke-Carparese*, DuD 2018, 156 (157 f).

693 *Albers/Veit* in: Wolff/Brink, BeckOK DatenschutzR, Art. 6 DSGVO, Rn. 72; *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 151, 153.

694 ErwGr 47 S. 1 und 3 f DSGVO. So auch *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 152; *Ehmann* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Anlage 3 zu Art. 6 DSGVO, Rn. 31; *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 254 f; vgl. *Ernst*, JZ 2017, 1026 (1035).

695 So *Ehmann* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Anhang 3 zu Art. 6 DSGVO, Rn. 26.

696 Ausführlich zum Begriff siehe *Ehmann* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Anlage 3 zu Art. 6 DSGVO, Rn. 18 f.

697 Siehe Art. 12 Abs. 1 S. 1 sowie Abs. 2 1 iVm 21 Abs. 2 DSGVO. Ausführlich den fortbestehenden Informationspflichten im *Plath*/*Grages*, CR 2018, 777 f, 778 f.

Abs. 1 lit. f DSGVO – die Maßstäbe des Art. 5 Abs. 1 DSGVO zu berücksichtigen. Die darin enthaltene Erforderlichkeit der Datenspeicherung sowie der damit überschneidende Grundsatz der Datenminimierung deuten jedoch an, dass eine dahingehende Granularität zur persönlichen Ansprache dem Zweck der Norm[698] und letztlich auch verfassungsrechtlichen Datenschutz-Prinzipien widerspricht. Wird die digitale Identität, die beim Besuch von Online-Vergleichsportalen angelegt wird,[699] mit personenbezogenen Daten wie An- und Abreisedatum oder der Anzahl der Kinder verknüpft[700] und auf Basis dieses Profils ein personalisierter bzw. individualisierter Preis festgelegt, handelt es sich unter Umständen um die durch Art. 22 Abs. 1 DSGVO erläuterte automatisierte Einzelentscheidung auf Basis des Profilings. Schließlich kann dieses Ergebnis des Algorithmus eine erhebliche rechtliche Wirkung entfalten, wenn der Betroffene gegenüber anderen Nutzern des Portals diskriminiert und folglich in das Recht aus Art. 3 Abs. 1, Abs. 3 GG und Art. 21 Abs. 3 GrC eingegriffen wird.[701] Dies geschieht exemplarisch dann, wenn der Verbraucher bzw. Betroffene der Datenverarbeitung ausschließlich den Preis wählen kann, den das Portal individuell und automatisiert für ihn bestimmt hat und eine Abweichung nur mit technischem Spezialwissen und desto unverhältnismäßigem Aufwand möglich ist. Hiergegen könnte zwar Argument des

698 *Ehmann* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Anhang 3 zu Art. 6 DSGVO, Rn. 29 aE.

699 Diese kann beispielsweise auch in der sog. Werbe-ID bestehen, welche mit fortwährender Nutzung von Smartphones genutzt und mit Drittanbietern geteilt wird. Diese besteht sowohl in Betriebssystemen des Unternehmens Apple (iOS) sowie Google (Android). In Kombination mit weiteren Daten, die durch das Aufrufen und Nutzen von Apps mit Verwendung der Werbe-ID entstehen, bildet sich ein sehr detailreiches und wiedererkennbares Benutzer-Abbild – besagte digitale Identität – ab. Siehe hierzu *Privacy International*, How Apps on Android Share Data with Facebook (even if you don't have a Facebook account), S. 7 f, 13 f sowie den folgenden Absatz im Detail.

700 Siehe *Privacy International*, How Apps on Android Share Data with Facebook (even if you don't have a Facebook account), S. 14/15.

701 Vgl. *Caspar*, PinG 2019, 1 (2); *Tillmann*/*Vogt*, VuR 2018, 447 (450); *Golland*, CR 2020, 186 (192); *Quinn* et al., White Paper Tracking, S. 16. Dagegen ablehnend *Hofmann*/*Freiling*, ZD 2020, 331 (335). Zumindest besteht ein hinreichender Vorbehalt derartiger inidividualisierter Preisbildung (sog. Algorithmic Pricing), so *Paal*, GRUR 2019, 43 (48). Die Zweifel an der Existenz und Durchsetzbarkeit solcher Verfahren, die *Körber*, NZKart 2016, 303 (308) und *Tillmann*/*Vogt*, VuR 2018, 447 (448) hegen, erscheinen wegen ansatzweiser Nachweisbarkeit nunmehr irrelevant.

Wohlfahrtseffekts angeführt werden. Durch die individuelle Preisbindung werden gerade wirtschaftlich schwächeren und weniger attraktiven Kundenkreisen angemessene Preise angeboten, wohingegen finanzstärkeren Kunden entsprechend höhere Preise berechnet werden.[702] Dieser gesamtgesellschaftliche Zweck kann jedoch nicht über die diesen Algorithmen anhaftende mangelnde Transparenz hinweghelfen, welche sowohl die Nachvollziehbarkeit der Preisbildung als auch daran geknüpften Rechte gem. Art. 22 Abs. 3 DSGVO betreffen.[703] Dabei ist schon fraglich, inwieweit sich eine derartige Verarbeitung mit den engen Ausnahmen des Art. 22 Abs. 2 DSGVO vereinen lässt oder ob auf die unternehmerischen Interessen des Art. 6 Abs. 1 lit. f DSGVO zurückgegriffen werden kann.[704] Jedenfalls äußert sich eine derartige algorithmische Voreingenommenheit als Malus der Privatautonomie des Art. 2 Abs. 1 GG[705], wenn eine freie Einwirkung auf den Vertragsschluss kaum noch möglich ist. Beispiels können sich datensparsame Internet- und Plattformnutzer dieser Praxis kaum oder nur schwer entziehen, erleiden möglicherweise Nachteile durch ein Aussperren von diesen Plattformen.[706] Dies ist allerdings nur in Extremfällen anzunehmen, weshalb es stets einer Einzelfallprüfung bedarf.[707] Offen bleibt außerdem, ob ein derartiges „Verstecken"

702 *Hofmann*, WRP 2016, 1074 (1074, 1080 ff). Vgl. auch *Tillmann*/*Vogt*, VuR 2018, 447 (448 f); *Obergfell*, ZLR 2017, 290 (294). Zu diesem und weiteren Vorteilen *Golland*, CR 2020, 186 (189).

703 *Ernst*, JZ 2017, 1026 (1034 f); *Paal*, GRUR 2019, 43 (49); *Ernst*, JZ 2017, 1026 (1035).

704 Schließlich muss nicht stets ein Profiling vorliegen, das Art. 22 DSGVO auslöst. Zumindest unter Vorbehalt bei Art. 6 Abs. 1 lit. f DSGVO diskutierend *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 6 DSGVO, Rn. 42. Den Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO – und damit letztlich auch jene des Art. 22 Abs. 1 – hinterfragend *Hofmann*/*Freiling*, ZD 2020, 331 (335).

705 Hierzu nur *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2 I, Rn. 101. Vgl. Preisgestaltung *Golland*, CR 2020, 186 (190).

706 *Obergfell*, ZLR 2017, 290 (295); vgl. *Ernst*, JZ 2017, 1026 (1034 f).

707 So auch *Tillmann*/*Vogt*, VuR 2018, 447 (450) und *Golland*, CR 2020, 186 (192).

des eigentlichen Preises auch die Informationsfreiheit des Art. 5 Abs. 1 S. 1 Alt. 2 GG beeinträchtigt.[708]

Eine Datenverarbeitung zur Erstellung und Erweiterung digitaler Identitäten kann also im Einzelfall gem. Art. 6 Abs. 1 lit. f DSGVO auch vom berechtigten (rechtlichen, wirtschaftlichen oder ideellen) Interesse des Datenverarbeitenden gedeckt sein, obschon es an einer Einwilligung mangelt. Der weiten Formulierung widerfährt durch Hineinlesen der Grundprinzipien des Datenschutzrechts[709] sowie der Verhältnismäßigkeitsprüfung expressis verbis eine Begrenzung, die den Schutz der Grundrechte und Grundfreiheiten der Inhaber digitaler Identitäten in den Mittelpunkt stellt. Eine Einwilligung ist damit nicht zwingend notwendig, entbindet allerdings nicht allumfassend von Informations-, Auskunfts- und Widerspruchsrechten. Der Schutz des verfassungsrechtlichen wie einfachgesetzlichen Datenschutzrechts besteht folglich auch in gezeigten Situationen fort.

Verarbeitung ohne Kenntnis und Einwilligung

Unter der eingangs aufgeworfenen Fragestellung ist nunmehr abschließend zu untersuchen, wie der Schutz der digitalen Identität ohne Kenntnis oder Einwilligung ausgestaltet ist. Ohne Kenntnis meint hier ohne Bewusstsein über den bloßen Fakt des Bestehens, Anlegens oder jeglicher sonstiger Datenverarbeitung (also „Ob"). Es mangelt damit kausal schon an der Informiertheit über das Kriterium der Einwilligung (vgl. Art. 4 Nr. 11 DSGVO) hinaus. Nicht zwingend geht damit das Entfallen der Transparenz einher, da auch die Möglichkeit eines Dispens von den

708 Dafür spricht zumindest, dass der Begriff der Informationsquelle iSd Grundrechts weit zu verstehen ist und sämtliche Informationsträger einschließt – so *Kühling* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 5 GG, Rn. 40. Zweckmäßig kann ein Vergleichsportal auch dazu dienen, einen Überblick über die Wettbewerber und aktuelle Angebote zu erhalten oder sich einen Überblick über Bewertungen zu verschaffen. Insofern erscheint der Gedanke nicht abwegig – zumindest zum Bewertungsaspekt siehe vgl. *Boehme-Neßler*, K&R 2016, 637 (639). Die Beeinträchtigung ergibt sich jedoch nur zwischen Privaten, sodass sie nur im Rahmen der mittelbaren Drittwirkung geltend gemacht werden kann. Wahrscheinlicher ist jedoch, dass die Diskriminierung von verschiedenen Wettbewerbern durch das Vergleichsportal Gegenstand des Kartellrechts wird – hierzu vgl. *Paal*, GRUR 2019, 43 (44, 48 f).

709 Vgl. *Roßnagel*, ZD 2018, 339 (343, 344) hinsichtlich derer aus Art. 5 Abs. 1 DSGVO.

datenschutzrechtlichen Informations- und Aufklärungspflichten besteht. In diesen Fällen hat der Gesetzgeber die auf verfassungsrechtlicher Ebene vorzunehmende Abwägung kollidierender Rechtsgüter – vorliegend unternehmerische und persönlichkeitsrechtliche Interessen – bereits vorgenommen und durch die Normierung Kollisionen ausgemerzt, abgemildert oder auf andere Entscheidungsträger (z.B. Verwaltungsbehörden) verlagert.[710] Einen derartigen Dispens hat der Gesetzgeber allerdings nur fallspezifisch vorgesehen, in Abhängigkeit von der Art und Weise der Erhebung personenbezogener Daten. Unter anderem entfällt die Informationspflicht gem. Art. 13 Abs. 4, 14 Abs. 5 lit. a DSGVO nach einer Datenerhebung beim Datensubjekt, wenn er/sie bereits Kenntnis von der Erhebung hat. Erfolgt die Erhebung nicht beim Datensubjekt bedarf es gem. Art. 14 Abs. 5 lit. b, 12 Abs. 2 S. 2 iVm 11 Abs. 2 DSGVO dagegen faktischer Hürden, die eine Information unmöglich machen oder zumindest mit unverhältnismäßigem Aufwand verbunden sind. Die damit nur vereinzelt mögliche Freistellung von Auskunfts- und Informationspflichten bestätigt die im Rahmen der verfassungsrechtlich wie datenschutzrechtlich vorgesehenen Notwendigkeit der Transparenz der Datenverarbeitung. Selbst wenn es sich um eine Verarbeitung zu wissenschaftlichen Zwecken handelt, besteht nur eine Freistellung von Lösch- und Auskunftspflichten gem. Art. 89 Abs. 2 DSGVO und berücksichtigt so die Forschungsfreiheit des Art. 5 Abs. 3 S. 2 Alt.2 GG. Die bewusste, aktiv ausgeübte Information als Teil der Transparenz ist folglich von hohem Stellenwert, sodass sie auch nicht bei einem berechtigten Interesse des Verarbeitenden entfällt.

Eine digitale Identität wie das sog. „shadow profile“ (dt. Schattenprofil), das ohne eine ausreichende Information des Inhabers des analogen Pendants angelegt wird, bewegt sich folglich am Rande der datenschutzrechtlichen Rechtmäßigkeit.[711] Die Existenz dieser Variante der digitalen Identität, die sich zunächst nur als Phänomen in den Anfragen von Max Schrems an Facebook und dem anschließenden

710 Vgl. *Bäcker* in: Kühling/Buchner, DSGVO, Art. 12 DSGVO, Rn. 4 sowie Art. 13 DSGVO, Rn. 8 f.

711 Vgl. *Jarass*, NJW 1989, 857 (860).

Verfahren abzeichnete[712], bestätigt sich nunmehr in der informatischen Literatur[713] und letztlich auch in der Befragung von Mark Zuckerberg im Jahr 2018[714]. So beschreibt *Garcia*: „Shadow profiles could be constructed without permission or knowledge of the person who is being profiled, who might not be a user nor agree to the terms of the online service that builds the profile." Dabei führt er erste Anzeichen für Schattenprofile auf eine Sicherheitslücke bei Facebook im Jahr 2013 zurück, die Verknüpfungen zwischen hochgeladenen Telefonbüchern und den darin gespeicherten Personen bzw. Telefonnummern offenlegte.[715] Eine weitere „Sicherheitslücke", die bereits 2011 Hinweise hierfür lieferte, nutzte Max Schrems mit seinem Auskunftsersuchen bei Facebook und gelangte an eine digitale und ungekürzte Kopie seines Datensatzes. Darin zeigten sich die von *Garcia* erwähnten Verknüpfungen, sowie weitere: Unter anderem wurden auch gelöschte Postings, jedes Like und Dislike mit Zeitstempel sowie private Kommunikation – auch nach einem Löschvorgang – von Facebook aufbewahrt.[716] Bei den Daten über ihn selbst handelt es sich nicht um ein Schattenprofil, sondern um eine digitale Identität. Hingegen sind die Daten von Dritten innerhalb seines Datensatzes, die mit weiteren Informationen in dem Datensatz verknüpft sind, ebensolche Schattenprofile. Diese wiederum nutzt Facebook beispielsweise, um potentielle Facebook-Freunde anzubieten und die Nutzer-Netzwerke zu erweitern[717], verwendet sie also zur Verbesserung seines Dienstes und damit innerhalb des berechtigten Interesses des Art. 6 Abs. 1 lit. f DSGVO. Dem steht jedoch

712 Ein Überblick sowie Auszüge aus dem Original-Datensatz finden sich unter http://www.europe-v-facebook.org/DE/Datenbestand/datenbestand.html.

713 *Boda* et al., User Tracking on the Web via Cross-Browser Fingerprinting, S. 31 ff; *Olejnik*/*Castelluccia*/*Janc*, Annals of Telecommunications 2014, 63 ff; *Cao*/*Li*/*Wijmans*, Network & Distributed System Security Symposium 2017, 1 ff; *Venkatadri* et al., Proceedings on Privacy Enhancing Technologies 2018, 1 ff; *Garcia*, Science Advances 2017, 1 ff; *Masood* et al., Proceedings on Privacy Enhancing Technologies 2018, 122 ff.

714 Siehe https://www.youtube.com/watch?v=PzHLwkcSc_s.

715 *Garcia*, Science Advances 2017, 1.

716 Siehe http://www.europe-v-facebook.org/DE/Datenbestand/datenbestand.html unter Nr. 30 „Minifeed", Nr. 45 „Realtime Activities", Nr. 29 „Messages" sowie das Dokument mit „gelöschten" Daten unter http://www.europe-v-facebook.org/removed_content.pdf.

717 Siehe die AGB von Facebook unter https://de-de.facebook.com/legal/terms?locale=de_DE&_fb_noscript=1, insbesondere den Abschnitt „Wir verbinden dich mit Menschen und Organisationen, die dir wichtig sind".

schon auf Ebene des grundgesetzlichen Datenschutzes gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG sowie dem aus Art. 7, 8 GrC die Transparenz und konkret die Informiertheit des Dritten entgegen. Für den Betroffenen besteht nicht die Möglichkeit der Verweigerung der Datenweitergabe an Werbeunternehmen, ebensowenig wie die Löschung oder ein Widerruf einer (vermeintlichen) Einwilligung. All diese Rechte setzen voraus, dass der Betroffene zumindest Kenntnis von der Datenverarbeitung hat. Von einer Kenntnis kann allerdings nicht ausgegangen werden, wenn Daten zum Zwecke der Zwei-Faktor-Authentifizierung an einen Diensteanbieter gegeben werden, welcher sie darüber hinaus und entgegen dem bekannten bzw. zu erwartenden und vereinbarten Zweck auch zur Verknüpfung mit weiteren Profilen und zum Ausspielen personalisierter Werbung nutzt.[718] Bezugnehmend auf die Verbindung zwischen dem Ob und Wie der Datenverarbeitung und deren Verankerung im Grundsatz der Transparenz, wenngleich das Kriterium der Informiertheit expressis verbis lediglich Teil der Voraussetzungen der Einwilligung nach Art. 4 Nr. 11, 7 Abs. 1 DSGVO ist, ist ein derartiges Handeln als intransparent einzustufen. Die Ausübung der informationellen Selbstbestimmung wird erschwert, wenn nicht gar unmöglich in Ermangelung der Kenntnis vom verantwortlichen Datenverarbeitenden. Hiergegen nützt zwar der Auskunftsanspruch gem. Art. 15 Abs. 1 DSGVO, um die Informationen bewusst einzuholen. Was im Fall von Facebook als prominentem Anspruchsgegner funktionieren mag, erweist sich bei der weiteren Betrachtung der Schattenprofile als ungeeignetes Instrument. Digitale Identitäten in Unkenntnis des Identitätsinhabers entstehen nämlich auch dann, wenn umfangreiche Tracking-Methoden zum Einsatz kommen. So ist die Möglichkeit des Webtrackings über Cookies, die einst unabhängig von einem Personenbezug durch die ePrivacy-Verordnung berücksichtigt werden sollte (vgl. Art. 8 ePrivacy-VO-Entwurf)[719], nicht mehr die einzige Möglichkeit zur

718 Siehe *Venkatadri* et al., Proceedings on Privacy Enhancing Technologies 2018, S. 13. Konkret wurde diese Praxis durch Twitter betrieben, wie Medienberichte im Jahr 2019 belegen – exemplarisch nur https://www.golem.de/news/twitter-zwei-faktor-telefonnummer-wurde-zu-werbezwecken-verwendet-1910-144334.html.

719 Der Entwurfstext der ePrivacy-Verordnung ist einsehbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010. Hierzu auch *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 249 f; *Rauer*/*Ettig*, ZD 2018, 255; *Schmitz*, ZRP 2017, 172 (174).

Verfolgung von Handlungsweisen des digitalen Selbst. Vielmehr wird auf die Profilbildung mittels Browser-Daten (sog. Browser-Fingerprinting)[720] oder Tracking-Pixel[721] und -Bilder[722] zurückgegriffen. Ersteres nutzt die Daten des Browsers beim ersten Aufruf der Webseite, die Angaben über Bildschirmgröße, Helligkeit/-Farbspektrum, Endgerät, installierte Plugins (Java, Adobe Flash, AdBlocker, etc.) und damit auch nachgeladene Inhalte dokumentieren.[723] Vereinzelt wird auch auf Browser-Schnittstellen zurückgegriffen, welche lediglich von Hör- und Sehbehinderten genutzt werden und als Teil der digitalen Identität ein entsprechend sensibles, besonderes personenbezogenes Datum (vgl. Art. 9 Abs. 1 DSGVO) darstellen.[724] Dadurch, und in Verbindung mit weiteren Nutzungsdaten oder Cookies, bildet sich ein unverkennbares digitales Abbild des Internetnutzers. Einen Zustand der Anonymität herzustellen oder aufrechtzuerhalten ist daher nahezu unmöglich oder nur umständlich bzw. für geübte Nutzer möglich.[725] Dergleichen ergibt sich, wenn von der Webseite je Nutzer bzw. Webseitenbesucher generierte Bilder als Teil der Webseite auf dem Endgerät gespeichert und zur Wiedererkennung genutzt werden. Dabei handelt es sich jedoch nicht um tatsächliche Bilder, sondern mit Hash-Werten codierte Bilddateien.[726] Hash-Werte zeichnet gerade aus, dass diese Werte bei gleichbleibenden Eingabe-Daten auch dasselbe Ergebnis liefern.[727] Wird eine Webseite also später erneut aufgerufen und vonseiten des Servers abgefragt, ob bereits Webseiten-Daten auf dem Endgerät vorhanden sind, so wird auch

720 *Jandt* in: Jandt/Steidle, Datenschutz im Internet, A.I., Rn. 37; *Boda* et al., User Tracking on the Web via Cross-Browser Fingerprinting, S. 31 (35, 39, 45); *Olejnik*/*Castelluccia*/*Janc*, Annals of Telecommunications 2014, 63 (65, 72); *Cao*/*Li*/*Wijmans*, Network & Distributed System Security Symposium 2017, 1 (2 f).

721 Zur Methodik des Facebook-Tracking-Pixels siehe *Kühnl*, Persönlichkeitsschutz 2.0, S. 27 ff, 29 sowie allgemein *Fox*, DuD 2010, 787. Weitere Tracking-Mechanismen von Facebook darstellend *Karg*/*Thomsen*, DuD 2012, 729 (730 f).

722 Zum individuell generierten Bild unter Verwendung eines Hashes als Authentisierungs-ID siehe *Quinn* et al., White Paper Tracking, S. 12.

723 Vgl. *Boda* et al., User Tracking on the Web via Cross-Browser Fingerprinting, 31 (32); *Bachem* in: Wamser/Fink, Marketing-Management mit Multimedia, 189 (191 f).

724 Art. 4 Nr. 15, ErwGr 35 DSGVO.

725 Mit gleichem Ergebnis hinsichtlich der Tracking-Maßnahmen von Facebook auch *Karg*/*Thomsen*, DuD 2012, 729 (734).

726 Hierzu sowie im Folgenden siehe *Quinn* et al., White Paper Tracking, S. 12.

727 Siehe zum Begriff *Hellmann*, IT-Sicherheit, S. 49 f sowie vertiefend *Eckert*, IT-Sicherheit, S. 366 f.

der Hash-Wert im generierten Bild gemeldet und der Nutzer des Endgeräts erkannt. Genauer gesagt: Nicht der Nutzer, sondern nur das Endgerät kann wiedererkannt werden. Der Prozess der Wiedererkennung ist nicht zu verwechseln mit dem der Identifizierung, welcher die analoge Identität bestätigt und eine direkte Zuordnung zur realen Person ermöglicht.[728] Dennoch kann im Rahmen der Wiedererkennung die Möglichkeit bestehen, dass ein Diensteanbieter bei ihm hinterlegte Daten (z.B. Adressdaten oder den Inhaber aus den Kreditkarten-Daten) zur Verknüpfung mit diesen Daten über den eigentlichen Zweck hinaus nutzt. Dies widerspricht jedoch auf mehreren Ebenen datenschutzrechtlichen Grundsätzen: Die nicht erforderliche Verknüpfung einzelner personenbezogener Daten widerspricht grundsätzlich den Prinzipien der Zweckbindung der genutzten Daten sowie dem der Datensparsamkeit. Darüber hinaus wird der Personenbezug von Daten, denen originär kein solcher möglich war, begünstigt und lässt auch zunächst anonyme Daten (z.B. Hash-Werte) Gegenstand des Datenschutzrechts werden. Weiter kann das Schattenprofil über mehrere Endgeräte gespeist und aufrecht erhalten werden, wie der Forschungsbericht von *Privacy International* belegt.[729] Hieraus können auch Daten über das Nutzungsverhalten gesammelt werden, die bei unterschiedlicher Nutzung ebenfalls Aussagen über Lebenssachverhalte offen legen, beispielsweise über Schlafgewohnheiten, Kaufkraft des Nutzers oder Work-Life-Balance anhand des Online-Verhaltens. Darin bestätigt sich erneut der bereits dargelegte Ansatz der Auflösung der Abgrenzung sowie die dargestellte Abkehr vom Personenbezug des Datums. Die Unvereinbarkeit mit verfassungsrechtlichen wie datenschutzrechtlichen Prinzipien sowie die mangelnde Rechtfertigung nach Art. 6 Abs. 1 DSGVO führen zur Rechtswidrigkeit von Schattenprofilen als bestimmte Form digitaler Identitäten. Schließlich widerspricht der Mangel an Transparenz sowie die Ohnmacht bei der informationellen Selbstbestimmung ebenjenem Grundrecht; ein berechtigtes, überwiegendes Interesse aus Art. 12 Abs. 1, 14 Abs. 1 GG ist letztlich nicht ersichtlich. Die Verarbeitung digitaler Identitäten ohne Kenntnis

728 Hierzu bereits Fn. 98 sowie *Jandt* in: Jandt/Steidle, Datenschutz im Internet, A.I., Rn. 36.

729 Im Detail siehe *Privacy International*, How Apps on Android Share Data with Facebook (even if you don't have a Facebook account), S. 15 f.

des Individuums ist folglich nicht mit dem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG vereinbar.

cc) Ergebnis Gezeigt werden konnte, dass die digitale Identität in ihrem informationellen Gehalt dem Schutz durch das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG unterliegt. Schon das weite Verständnis des Grundrechts selbst hinsichtlich neuer technischer Entwicklungen mit Blick auf neue Varianten und Speicherformen personenbezogener Daten lässt dies zu. Ausdrücklich lässt sich dieses Verständnis in der Fassung der Datenportabilität in Art. 20 DSGVO erkennen, welche letztlich auch auf die Entwicklungsoffenheit des Grundrechts rekurriert.

Die Notwendigkeit dieses Schutzes ergibt sich aus einer Vielzahl von Risiken der Datenverarbeitung, beispielsweise der personalisierten Preisbildung auf Basis digitaler Identitäten oder stetig steigende Gefahr des Identitätsdiebstahls bzw. -missbrauchs. Diesbezügliche Maßnahmen des Staates durch datenschutzrechtliche Regelungen schaffen erste Ansätze, scheitern aber an einem einheitlichen Regelungsbild. Dies lässt sich vor allem daran erkennen, dass spezifische Arten von Sammlungen personenbezogener Daten kaum oder nicht reguliert sind. Ein einheitliches Verständnis sowie ein einheitlicher Umgang mit derartigen Daten fehlt daher. Infolgedessen, und aufgrund technischer Gegebenheiten, verschwimmen die definierten Grenzen zunehmend. Ein effektiver Schutz der digitalen Identität erfolgt daher stets einzelfallbezogen, unter Betrachtung der Stärke des Personenbezuges[730], des informationellen Gehalts und dementsprechender Nähe zur Menschenwürde des Art. 1 Abs. 1 GG. Gerade in letztem Aspekt und hinsichtlich der stets notwendigen Abwägung mit berechtigten Interessen oder gar Allgemeininteressen[731] ist eine Sphärentheorie hinsichtlich personenbezogener Daten und Datensammlungen wie der digitalen Identität erkennbar.

730 So im Ergebnis auch *Herbst*, NVwZ 2016, 902 (905 f).
731 Vgl. BVerfGE 80, 367 (373); 115, 320 (357 ff).

c) Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Fernerhin bleibt vor dem gedanklich-historischen Hintergrund des Allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme zu betrachten. Sinnstiftend definierte das Bundesverfassungsgericht dieses Grundrecht als gegenüber Art. 10 Abs. 1, 13 Abs. 1 GG subsidiären Schutz vor Eingriffen in informationstechnische Systeme, fokussiert allerdings ebenfalls moderne Gefährdungen der Persönlichkeit.[732] Gelingt der Zugriff auf das Informationssystem, offenbart sich ein quantitativer wie qualitativer Datensatz: „Im Rahmen des Datenverarbeitungsprozesses erzeugen informationstechnische Systeme zudem selbsttätig zahlreiche weitere Daten, die ebenso wie die vom Nutzer gespeicherten Daten im Hinblick auf sein Verhalten und seine Eigenschaften ausgewertet werden können."[733] Kommt es im Wege des Eingriffs auf die umfangreiche Datenerhebung an, beispielsweise durch eine Kopie der gesamten Festplatte oder die Infiltration des Systems via Malware, ist eine Beeinträchtigung der Integrität und Vertraulichkeit des Systems zu bedenken.[734] Schließlich „ist [dann] die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen."[735].

Was das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (nachfolgend GGVIS[736]) genau schützt, lässt sich in informationeller Hinsicht als Systemsicherheit bzw. IT-Sicherheit bezeichnen. Datenschutz und Datensicherheit weisen hierzu oftmals Kongruenzen auf, wie Art. 25, 32 DSGVO erkennen lassen. Fällt der Blick hingegen auf Instrumente der Datensicherheit wie beispielsweise die Intrusion Detection[737] unter Verwendung

732 BVerfGE 120, 274 (303).
733 BVerfGE 120, 274 (305).
734 BVerfGE 120, 274 (313 f).
735 BVerfGE 120, 274 (314)
736 Namensgebend mit weiterer Erläuterung zu diesem Akronym siehe *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 22.
737 Hierzu *Deusch*/*Eggendorfer*, K&R 2018, 753 ff.

maschinellen Lernens, kann eine damit einhergehende Verarbeitung personenbezogener Daten und ein Abbilden von Benutzerverhalten – also ebenfalls ein Vorhalten digitaler Identitäten – prima facie auch entgegen datenschutzrechtlicher Prinzipien wirken. Denn: Auch eine Analyse dieser aggregierten Daten und mögliche falsche Schlussfolgerungen unterliegen Art. 22 Abs. 1, Abs. 2 DSGVO, obschon eine Profilbildung und der Einsatz von Intrusion Detection Systemen von Art. 6 Abs. 1 lit. f DSGVO gedeckt sein könnten.[738] Dennoch dient der Einsatz dieser Systeme dem Schutz der Daten hinsichtlich Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit der Daten[739]; mithin auch Funktionsfähigkeit des informationstechnischen Systems[740]. Weiterhin führt dieses technische Aufrüsten eigener Systeme dazu, den für das Grundrecht vorausgesetzten Vertrauenstatbestand[741] zu schaffen.

Für den informationellen Gehalt der digitalen Identität ist der Systemschutz des GGVIS nur mittelbar brauchbar. Durch das Vertrauen des Nutzers in die eigene Informationstechnik, insbesondere bei eigens eingerichteten Schutzmaßnahmen wie Firewall und Virenscanner, wird die namensgebende Integrität des Datenbestandes geschützt.[742] Innerhalb eines Systems tragen auch begrenzte Benutzerrechte und der Einsatz von digitalen Signaturen dazu bei.[743] Darunter ist mit Blick auf die initiierende Rechtsprechung des Bundesverfassungsgerichts allerdings nur die technische Integrität gemeint, nicht die informationelle Lesart iSe Datengehalts. Der Verlust und die Manipulation von Daten bzw. Informationen betrifft vielmehr das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG, welche wie ausgeführt die Verfügungsposition über die eigenen Daten und digitalen Identitäten umfasst. Demgemäß ist eine weitere Betrachtung auf die technische Betrachtung der digitalen Identität unter D.II. zu vertagen.

738 Hierzu ErwGr 49 DSGVO; *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 167; *Deusch/Eggendorfer*, K&R 2018, 753 (757 f). Vgl. auch *Ritter* in: Schwartmann et al., DSGVO/BDSG, Art. 32, Rn. 56.

739 *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 167.

740 EuGH, Urteil vom 19.10.2016, Az. C-582/14 – Breyer –, Rn. 60.

741 BVerfGE 120, 274 (314); *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 70.

742 *Herrmann*, GGVIS, S. 123 f; *Hornung*, CR 2008, 299 (302 f); *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 71 sowie gleichermaßen *Luch*, MMR 2011, 75 (75).

743 *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, S. 75.

d) Recht auf (Daten-)Eigentum und digitalen Nachlass, Art. 14 Abs. 1 GG

Im Gegensatz zur Prüfung des GGVIS drängt sich die Diskussion einer Einordnung der digitalen Identität von originären Grundrechtsträgern geradezu auf, spätestens seit Umsetzung der DSGVO und dem beschlossenen Vorhaben der Großen Koalition aus CDU/CSU und SPD hinsichtlich eines Dateneigentums[744] sowie mit Blick auf das Urteil des BGH in Sachen „Digitaler Nachlass“[745]. Daher soll an dieser Stelle die darin angedeutete und zunehmend stärkere Diskussion beider Punkte und der darin eingeschlossenen Probleme einer Kollision von digitalen Sachverhalten mit dem „analogen Recht“ diskutiert werden. So ist zunächst auf die Frage des Dateneigentum unter dem verfassungsrechtlichen Eigentumsbegriff einzugehen und zu untersuchen, ob eine geeignete Definition besteht oder die politisch beabsichtigte Neuregelung entsprechend geeignet und effektiv erscheint. Anschließend bleibt dabei unter dem Stichwort „Schutzgut“ zu erörtern, ob die Problematik nicht eher einen persönlichkeitsrechtlichen bzw. informationell-datenschutzrechtlichen Hintergrund hat und weniger eine vermögensrechtliche Einordnung erzwingt. Anschließend ist auf Basis des verfassungsrechtlichen Erbrechts zu skizzieren, ob auch in diesem Punkt ein verfassungsrechtlicher Schutz der digitalen Identität besteht und, sofern gegeben, wie weit dieser reicht. In beiden Betrachtungen werden aufgrund der Normprägung der Grundrechte aus Art. 14 Abs. 1 GG[746] die entsprechenden einfachgesetzlichen Vorschriften lediglich zu streifen sein.

aa) Recht auf Eigentum an (personenbezogenen) Daten

744 Das Dokument ist einsehbar unter https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1.

745 BGH, Urteil vom 12. Juli 2018 – Az. III ZR 183/17.

746 Zur Eigentumsfreiheit: Ausführlich *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 29 ff mit Conclusio in Rn. 47 f; *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 148; *Hufen*, Staatsrecht II, § 38, Rn. 7 f. Zur Gewährleistung des Erbrechts: *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 404; *Hufen*, Staatsrecht II, § 38, Rn. 7 f.

(1) Verfassungsrechtliche Definition Grundlegend für die Betrachtung ist der verfassungsrechtliche Eigentumsbegriff des Art. 14 Abs. 1 GG. Wo dem Wortlaut keine Einzelheiten zu entnehmen sind, verweist Art. 14 Abs. 1 GG zumindest auf die Rolle des Gesetzgebers und die Normprägung des Grundrechts: Sowohl hinsichtlich der Gewährleistung des Eigentums (S. 1) als auch weiterer Inhalts- und Schrankenbestimmungen (S. 2) kommt ihm die Regelungsprärogative zu. Dennoch weist das Grundrecht einen eigenen Gehalt auf, der sich in den Funktionen des Grundrechts[747] erstreckt und dadurch die Grundlage für die Prärogative bietet. So erkennt das Bundesverfassungsgericht als Eigentum „alle vermögenswerten Rechte [an], die dem Berechtigten in der Weise zugeordnet sind, daß [sic] er die damit verbundenen Befugnisse nach eigenverantwortlicher Entscheidung zu seinem privaten Nutzen ausüben darf“[748]. Wenngleich das Sacheigentum als „natürliches Eigentum“[749] dem Gesetzgeber ein Leitbild[750] vorgibt und dieses andere Varianten des Eigentums überdeckt[751], einigt sie abseits physischer Eigenschaften der abwehrrechtliche Einfluss durch Herrschafts-, Nutzungs- und Verfügungsbefugnisse[752]. Demgemäß steht die ausschließliche, erga omnes bestehende Rechtsposition im Vordergrund.[753] Die Ausgestaltung dieser Einzelheiten ist Teil der institutionellen Garantie des Art. 14 Abs. 1 GG[754] – Eigentum ist (einfachgesetzlich) geprägte Freiheit[755]. Das weite Verständnis des Art. 14

747 Zu den Funktionen im Einzelnen siehe *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 3 ff.

748 BVerfGE 83, 201 (208); 91, 294 (307); 112, 93 (107); 115, 97 (110 f).

749 *Depenheuer* in: Merten/Papier, HGr V, § 111, Rn. 47 sowie *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 59.

750 Hierzu *Depenheuer* in: Merten/Papier, HGr V, § 111, Rn. 50 f sowie *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 62 f, 34; *Axer* in: Epping/Hillgruber, BeckOK GG, Art. 14, Rn. 10; *Stern*, StaatsR IV/1, S. 2185 ff.

751 *Axer* in: Epping/Hillgruber, BeckOK GG, Art. 14, Rn. 11: Strukturkompatibilität.

752 BVerfGE 52, 1 (30); 83, 201 (208); als „erweiterten Eigentumsbegriff“ bezeichnend *Kimminich* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 14, Rn. 32. Zur Entsubstantialisierung des Eigentumsbegriffs siehe auch *Depenheuer* in: Merten/Papier, HGr V, § 111, Rn. 28 ff.

753 Vgl. *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 64.

754 *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 121 f; *Kloepfer*, VerfR II, § 72, Rn. 72.

755 BVerfGE 97, 360 (371) und *Depenheuer* in: Merten/Papier, HGr V, § 111, Rn. 9, 61 unter Verweis auf Äußerungen Paul Kirchhofs; *Kloepfer*, VerfR II, § 72, Rn. 16.

Abs. 1 S. 1 Alt. 1 GG bedeutet jedoch auch, dass Eigentum sich als „gespeicherte Freiheit“ manifestiert.[756] Seinem Telos als Freiheitsrecht nach bewahrt das Eigentumsrecht das Geleistete und ist Grundlage für eine Wertbemessung.[757] Schließlich schützt Art. 14 Abs. 1 GG jedes vermögenswerte Recht, nicht jedoch das Vermögen selbst.[758] Daraus lässt sich auch kein Recht auf Garantie eines bestimmten Wertes aus Art. 14 Abs. 1 GG ableiten.[759] Dennoch obliegt es wie erwähnt dem Staat, die Mindestvoraussetzungen für eine Wertstellung des Eigentums zu erfüllen – sei es aus Gründen der Institutsgarantie[760] oder zur Erfüllung seiner Schutzpflichten bzgl. multidimensionaler Grundrechtssachverhalte nach Maßgabe des Untermaßverbots[761].[762]

Mit Blick auf die digitale Identität ist nunmehr zu klären, ob es sich um „gespeichertes“ Eigentum iSd Verfassung handelt. Dafür spricht zunächst, dass die digitale Identität – abgesehen von Speichermedien – nicht haptisch begreifbar ist und hin zum immaterialgüterrechtlichen Teil des Art. 14 Abs. 1 GG tendiert. An einer digitalen Identität könnten Immaterialgüterrechte bestehen, beispielsweise durch die Nutzung einer digitalen Identität als Kunstfigur oder bei besonderen Formen des § 2 UrhG. Zudem entstehen dadurch, oder durch die aufgezeigten datenschutzrechtlichen Mittel, entsprechende Herrschafts- und Nutzungsrechte, die ebenfalls ausschließlich dem Urheber bzw. Datensubjekt zukommen. Die Nutzung der Datensätze der digitalen Identität ist regelmäßig nach Maßgabe der Beteiligten

756 *Stern*, StaatsR IV/1, S. 2130; *Leisner*, Eigentum, S. 3 (4), 7 (8), 9 ff.

757 Siehe nur *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 13 f; *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 2, vgl. zum Urheberrecht auch Rn. 315; *Meyer-Abich*, Der Schutzzweck der Eigentumsgarantie, S. 58 f. Vgl. auch BVerfGE 116, 96 (121); 143, 246 (Rn. 238).

758 BVerfGE 65, 196 (209); 72, 175 (195); 95, 267 (300); vgl. 30, 250 (271 f); *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 277; *Stern*, StaatsR IV/1, S. 2200 ff.

759 BVerfGE 105, 17 (30). Zur Eigentumswertgarantie siehe auch *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 116, 279 f.

760 So BVerfGE 20, 351 (355); 24, 367 (389); 26, 215 (222); 31, 229 (240); 42, 263 (294); 50, 290 (339 f); 58, 300 (339); *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 119, 121; *Wendt* in: Sachs, GG, Art. 14, Rn. 10; *Stern*, StaatsR IV/1, S. 2172 f.

761 *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 92 aE.

762 Zur unterschiedlichen Stoßrichtung beider Aspekte siehe *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 134.

möglich (vgl. Art. 6 Abs. 1 lit. a, 7 Abs. 2 DSGVO), auch kann die Berechtigung jederzeit entzogen werden (Art. 7 Abs. 3 S. 1 DSGVO). Insofern scheint der letzte Halbsatz der eingangs zitierten Definition des Bundesverfassungsgerichts erfüllt.

Problematisch ist jedoch das Kriterium des „vermögenswerten Rechts", das seit der Nutzung von personenbezogenen Daten und digitalen Identitäten zum Zwecke personalisierter Werbung und ähnlichen Praktiken stets umstritten ist. So stellt sich die Frage, ob das Datenschutzrecht auch einen vermögenswerten Gehalt hat oder diesen einbezieht. Aussagen wie „Aber nichts im Leben ist umsonst! Daher muss der Nutzer von Facebook davon ausgehen, dass er mit seinen Daten [...] zahlen wird."[763] oder das „Modell ‚Service gegen Daten'"[764] entfachen die Debatte stets erneut, indem sie Daten als Leistungs- und Tauschgegenstand gegen ein digitales Angebot qualifizieren. Für den verfassungsrechtlichen Eigentumsbegriff kommt es jedoch nicht auf diese tatsächliche Ebene der Wertzuordnung an. Vielmehr ist, unter Einbeziehung der Einrichtungsgarantie, zu betrachten, welche Rechtspositionen der Gesetzgeber mit entsprechenden Wertschöpfungs- und Herrschafts- bzw. Nutzungsrechten ausgestattet hat (auch: Zuweisungsgehalt).[765] Zusätzlich zum Zuweisungsgehalt bedarf es aber der zuvor erwähnten Ausschlussfunktion[766]. Das Datenschutzrecht kann für diese Einordnung nicht in Betracht kommen[767], da es schon von Verfassungs wegen dem Schutz des Grundrechts auf informationelle Selbstbestimmung dient und keine Zuordnung von Vermögenswerten vorsieht, vgl. Art. 1 Abs. 2 sowie Erwägungsgrund 1 DSGVO.[768]

763 So *Söbbing*, InTeR 2018, 182 (185).

764 *Krohm*/*Müller-Peltzer*, ZD 2017, 551 (551). Zum Entgelt-Charakter von Daten ebenso *Faust*, NJW-Beilage 2016, 29 (29); vgl. *Schweitzer*/*Peitz*, NJW 2018, 275 (277).

765 *Stern*, StaatsR IV/1, S. 2184, Fn. 305 mwN; *Eschenbach*, Der verfassungsrechtliche Schutz des Eigentums, S. 519.

766 *Eschenbach*, Der verfassungsrechtliche Schutz des Eigentums, S. 519 f.

767 Mit Blick auf das Datenschutzrecht ablehnend *Richter*/*Hilty*, Die Hydra des Dateneigentums – eine methodische Betrachtung, S. 241 (252). Dagegen ein vermögenswertes Ausschließlichkeitsrecht befürwortend *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 208 ff.

768 So iE auch OLG Lüneburg, Beschluss vom 26.02.2019 – Az. 11 LA 274/18 –, Rn. 16, 20; *Hoeren*, Big Data und Recht, S. 19 f; *Härting*, CR 2016, 646 (648); *Specht*, CR 2016, 288 (289); *Zech*, CR 2015, 137 (141); vgl. *Sattler*, JZ 2017, 1036 (1037) sowie *Dorner*, CR 2014, 617 (624).

So schließt auch das Bundesverfassungsgericht aus: „Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann.“[769] Ebenso tritt die Zuordnung der Herrschafts- und Nutzungsrechte nur relativ ein, wenn es sich um personenbezogene Daten handelt oder per se die Datenverarbeitung keine Grundlage aufweist. Die generalklauselartige Verarbeitungsgrundlage des Art. 6 Abs. 1 lit. f DSGVO[770] öffnet die Ausschließlichkeit derart, sodass bei überwiegenden Interessen des Betroffenen gerade kein Ausschließlichkeitsrecht, sondern ein bloßes Informations- und Auskunftsrecht besteht.[771] Diese und weitere Instrumente des Datenschutzes[772] wirken außerdem nur bereichsspezifisch,[773] im Gegensatz zum grundlegenden Zuordnungsprinzip des Eigentums. Abseits dessen kann über die eigene digitale Identität frei verfügt werden, weshalb eine Verwendung als Zahlungsmittel bzw. Tauschmittel grundsätzlich nicht rechtswidrig ist. Auch die zitierte Aussage des Bundesverfassungsgerichts spricht nicht dagegen.[774] Vielmehr ist dies im Wege datenschutzkonformer Verträge möglich, wie Art. 6 Abs. 1 lit. b DSGVO erkennen lässt. Dies unterstützt auch der Kern der informationellen Selbstbestimmung in Art. 2 Abs. 1 GG einschließlich der Privatautonomie.[775] Verstöße von Vertragspflichten zwischen Privaten regelt sodann das BGB durch Anwendung des allgemeinen Schuldrechts, handelt es sich beispielsweise um einen Datenkauf iSd §§ 433, 453 Abs. 1 Alt. 2 BGB[776]. Daneben kann sich auf das „sonstige Recht“ des § 823 Abs. 1 BGB berufen werden. Wohingegen zunächst

769 BVerfGE 65, 1 (44). Gleichermaßen EuGH, Urteil vom 20.12.2017, Az. C-434/16 – Nowak –, Rn. 45. In der Literatur ebenso *Heymann*, CR 2016, 650 (652 f); vgl. *Fezer*, ZD 2017, 99 (101).

770 Zur daraus entstehenden Rechtsunsicherheit *Buchner/Petri* in: Kühling/Buchner, DSGVO, Art. 6 DSGVO, Rn. 142 ff.

771 Vgl. *Dorner*, CR 2014, 617 (624 f). Ferner unter Würdigung weiterer Vorschriften ablehnend *Kühling*/*Sackmann*, vzbv-Gutachten, S. 13.

772 *Hornung*/*Goeble*, CR 2015, 265 (270).

773 So *Schulz*, PinG 2018, 72 (73).

774 *Specht*, CR 2016, 288 (292 f).

775 Vgl. BGHZ 26, 349 (354 f); *Stern*, StaatsR IV/1, S. 204; *Isensee* in: Isensee/Kirchhof, HStR VII, § 150, Rn. 6 f, 59 f; *Kühling*/*Sackmann*, vzbv-Gutachten, S. 14; als „kleines Dateneigentum“ bezeichnend *Esken*, Dateneigentum und Datenhandel, S. 73 (78 f).

776 Zur Möglichkeit eines Datenkaufs siehe *Stender-Vorwachs*/*Steege*, NJOZ 2018, 1361 (1363 f).

nur persönlichkeitsrechtliche Aspekte hierunter zu fassen waren, sind auch Beeinträchtigungen des Grundrechts auf informationelle Selbstbestimmung von § 823 Abs. 1 BGB umfasst. Dies wurde wohl nur differenzierend angenommen[777], ist jedoch angesichts der Wertstellung von Datensätzen im Allgemeinen sowie der Ausweitung der Immaterialgüterrechte von analogen Medien auf Datenbanken nur konsequent. Eine Kollision mit nunmehr datenschutzrechtlichen Haftungsansprüchen aus Art. 82 Abs. 1 DSGVO besteht gem. Erwägungsgrund 146 S. 4 DSGVO nicht.[778] Ein vermögenswertes Recht aus einem privatrechtlichen Sekundäranspruch abzuleiten scheint jedoch insofern unangebracht, als dass es sich dabei um kein aktives Recht handelt, auf das der Inhaber der digitalen Identität zurückgreifen kann. Sonst muss zur Geltendmachung des Anspruchs ein Schaden provoziert werden, der schon zur Unanwendbarkeit der Norm führt – nur die Schädigung eines anderen und durch einen anderen ist von § 823 Abs. 1 BGB umfasst. Ein originäres, vermögenswertes Recht iSd Art. 14 Abs. 1 GG oder ein auf (personenbezogene) Daten bezugnehmender Rechtsrahmen besteht de lege lata nicht. Ein vermögenswertes Recht an Daten de lege ferenda ist dadurch aber nicht unmöglich, sondern könnte bei Ausgestaltung des Instituts des Art. 14 Abs. 1 GG bis zu diesem Punkt der Betrachtung möglich sein.

(2) Bestehende Eigentumsbegriffe Ungehindert dessen bleibt zu fragen, ob nicht schon ein Eigentumsrecht an personenbezogenen Daten durch Legislative, Judikative oder in der rechtswissenschaftlichen Literatur qua Analogie herausgebildet wurde. In diesem Fall bestünde wiederum eine Schutzfähigkeit der digitalen Identität nach Art. 14 Abs. 1 GG, da eine konkrete Ein- bzw. Unterordnung als vermögenswertes Recht vorliegt. Sodann bedürfe es auch keiner Neuregelung einer Rechtsposition.

777 Siehe nur *Wagner* in: Säcker et al., MüKo BGB, Bd. VI, § 823, Rn. 332 ff; *Zech*, Information als Schutzgegenstand, S. 386 f; *Meier*/*Wehlau*, NJW 1998, 1585 (1588 f); *Hoeren*, MMR 2013, 486 (491); *Faustmann*, VuR 2006, 260 (262 f); ausführlich zum Integritätsschutz *Berberich*/*Golla*, PinG 2016, 165 (170 f); *Spindler* in: Gsell et al., BeckOGK BGB, § 823, Rn. 184 ff.

778 So auch *Boehm* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 82 DSGVO, Rn. 32.

Naheliegend ist die Betrachtung des Zivilrechts, da es das erwähnte Leitbild des verfassungsrechtlichen Eigentumsbegriffs kodifiziert. Ansatzpunkte für eine Einordnung finden sich schon in der Definition der beweglichen Sache gem. § 90 BGB, die intrinsisch die (physische) Beweglichkeit der Daten voraussetzt. Dies ist jedoch aufgrund der immateriellen Gestalt von Daten, also Informationen in Form von elektrischen oder physischen, maschinenlesbaren Zuständen der Hardware, nicht möglich.[779] Daten sind per se nicht-rival, nicht-exklusiv und nicht-abnutzbar.[780] Höchstens die Hardware als Datenträger fällt unter den Begriff des § 90 BGB[781], unabhängig des eigentlichen Datengehalts. Das Eigentum an der Hardware und an den Daten fällt damit auseinander bzw. nicht stets in der gleichen Person zusammen.[782] Die in der Literatur ungeachtet dessen vertretene Annahme, dass Daten Nutzungen (§ 100 BGB) und Früchte (§ 99 Abs. 2 BGB) darstellen könnten[783], übersieht die in § 99 Abs. 1 und Abs. 2 BGB vorgesehene Voraussetzung einer rechtlichen Zuordnung. Beides sind nur Derivate einer Sache

779 *Härting*, CR 2016, 646 (647); *Schulz*, PinG 2018, 72 (74); *Redeker*, CR 2011, 634 (638); *Markendorf*, ZD 2018, 409 (410); *Lehmann*, FS Schneider, S. 133 (134); aufgrund mangelnder Rivalität ablehnend *Zech*, CR 2015, 137 (141 f). Ausführlich auch *Berberich*, Virtuelles Eigentum, S. 87 ff.

780 Erstmals *Zech*, CR 2015, 137 (139) sowie ausführlich *Zech*, Information als Schutzgegenstand, S. 326 ff; darauf aufbauend *Heymann*, CR 2016, 650 (652 f, 655 f). Vgl. auch *Berberich*, Virtuelles Eigentum, S. 92 sowie spezifisch zu Accounts *Kutscher*, Der digitale Nachlass, S. 23 f.

781 Vgl. *Welp*, iur 1988, 443 (448); *Kutscher*, Der digitale Nachlass, S. 22 ff; *Faust*, Ausschließlichkeitsrecht an Daten?, S. 85 (86 f). Zu dabei entstehenden Problemen siehe *Berberich*, Virtuelles Eigentum, S. 93 ff. Anders dagegen mit Blick auf Flashspeicher *Haustein*, Möglichkeiten und Grenzen von Dateneigentum, S. 143 f.

782 Vgl. *Welp*, iur 1988, 443 (448).

783 Grundlegend hierzu bzgl. Geodaten *Grosskopf*, IPRB 2011, 259 (260) und *Bleckat*, RDV 2019, 114 (114 f), jedoch iE Geodaten als Früchte des Grundeigentums annehmend. Die Kollision mit dem Persönlichkeitsrecht wird von *Grosskopf* durch eine Einwilligung des Datensubjekts gelöst. Dabei wird jedoch das mangelnde Dateneigentum an personenbezogenen Daten mit dem fingierten Eigentum an (Maschinen-)Daten als Früchte einer Sache überschrieben – ungeachtet potentieller Folgeprobleme einer eigentumsrechtlichen Zuordnung. Diese Probleme de lege ferenda aufzeigend und daher eine Analogie zu §§ 99, 100 BGB ablehnend *Schulz*, PinG 2018, 72 (75). Den Ansatz von *Grosskopf* ablehnend *Zech*, CR 2015, 137 (142) mit ausführlicher aA in *Zech*, Information als Schutzgegenstand, S. 221 f sowie *Haustein*, Möglichkeiten und Grenzen von Dateneigentum, S. 169 f. und *Stresemann* in: Säcker et al., MüKo BGB, Bd. I, § 99, Rn. 5 aE.

oder eines Rechts, setzen also eine vom Gesetzgeber vorgesehene „Hauptrechtsposition“ voraus. Mit dem Verneinen des zivilrechtlichen Eigentumsbegriffs gem. §§ 903 S. 1, 90 BGB kann also auch kein Fall der §§ 99, 100 BGB vorliegen.[784] Hinzu tritt bei verfassungsrechtlicher Würdigung der Übertragung und Aufgabe von Eigentum, dass auch das datenmäßige – persönlichkeitsrechtlich geprägte – Dateneigentum vollends aufgegeben werden müsste. Die Aufgabe der Kontrolle über persönliche Daten mit entsprechender Nähe zum Kernbereich privater Lebensgestaltung sowie der Menschenwürde des Art. 1 Abs. 1 GG ist allerdings kritisch zu betrachten.[785] Fernerhin wird gelegentlich ein eigenständiges Dateneigentum aus § 823 Abs. 1 BGB im Rahmen der „sonstigen Rechte“ zuerkannt.[786] Dies ist jedoch nicht mit dem im Rahmen der (politischen[787]) Diskussion gemeinten Eigentumsrecht zu vergleichen, sondern bezieht sich lediglich auf einen deliktischen Schadensersatzanspruch auf Basis des Allgemeinen Persönlichkeitsrechts als sonstiges Recht iSd § 823 Abs. 1 BGB aE. Ein eigenständiges, als Teil der Eigentumsordnung anerkanntes Eigentumsrecht ist darin nicht zu sehen.

Während ein Dateneigentum nach den allgemeinen zivilrechtlichen Regelungen ausscheidet, ließe sich möglicherweise eine Parallele zu Regelungen des Immaterialgüterrechts ziehen. Dafür spricht prima facie die fehlende Haptik von Daten gleichermaßen wie bei Immaterialgüterrechten. Obschon das Leitbild des Art. 14 Abs. 1 GG ein anderes ist, war die Ausgestaltung von Verfügungs- und Verwertungsrechten derartiger Positionen zur Schaffung von Inhaltsbestimmungen iSd

784 So auch *Zech*, CR 2015, 137 (142). Aus weiteren Gründen ablehnend *Schulz*, PinG 2018, 72 (74); *Specht*, CR 2016, 288 (292); *Härting*, CR 2016, 646 (647). Vgl. hinsichtlich Nießbrauch und Pfandrecht *Faust*, Ausschließlichkeitsrecht an Daten?, S. 85 (96).

785 *Peifer*, GRUR 2002, 495 (500); BVerfGE 65, 1 (43).

786 Hierzu *Bartsch*, FS Schneider, S. 297 ff; *Wagner* in: Säcker et al., MüKo BGB, Bd. VI, § 823, Rn. 336 ff; *Spindler* in: Gsell et al., BeckOGK BGB, § 823, Rn. 184 ff; *Heymann*, CR 2016, 650 (651 f). Bloß auf die Schutzlücke hinweisend *Faust*, Ausschließlichkeitsrecht an Daten?, S. 85 (94 f). Lediglich hinsichtlich des GGVIS und Datenverlust betrachtend *Faust*, NJW-Beilage 2016, 29 (32); *Grützmacher*, CR 2016, 485 (489 f); *Härting*, CR 2016, 646 (649). Wohl ablehnend *Fezer*, Repräsentatives Dateneigentum, S. 32.

787 Vgl. hierzu nur *Determann*, ZD 2018, 503 (506 f) sowie die weitere Rezeption unter D.I.1.d)aa)(3).

Art. 14 Abs. 1 S. 2 GG notwendig.[788] Beispielsweise sind auch Werke iSd § 2 Abs. 2 UrhG gespeichertes Eigentum iSe gespeicherten, verkörperten geistigen Leistung. In der Literatur finden sich diverse Ansätze, eine brauchbare Parallele aus dem Urheberrecht aufzuzeigen. Bevorzugt wird der Ansatz, auf der Basis des Datenbankwerks nach § 4 Abs. 2 UrhG oder den Regelungen zum Schutz des Datenbankherstellers nach §§ 87a ff UrhG aufzubauen. So wird hinsichtlich des § 4 Abs. 2 UrhG und dem Begriff des Datenbankwerks diskutiert, ob er sich per definitionem der Begriff nicht schon für eine Anwendung auf Daten eignet.[789] Prinzipiell ist dies nachvollziehbar, setzt die Legaldefinition des § 4 Abs. 2 S. 1 UrhG doch als Unterfall des Sammelwerks[790] eine methodische, systematische Anordnung unter Verwendung elektronischer Mittel voraus. So ist sie schon bei einer einfachen, alphabetischen oder chronologischen Sortierung anzunehmen.[791] Dies darf jedoch nicht vollautomatisiert geschehen, sondern muss iSe persönlichen geistigen Schöpfung des § 2 Abs. 2 UrhG die Individualität und Persönlichkeit des Urhebers durchscheinen lassen.[792] Dagegen stellt das Recht des Datenbankherstellers gem. § 87a Abs. 1 S. 1 UrhG auf eine Investition von Zeit, Geld oder Mühe ab,[793] übernimmt jedoch wortgleich die übrigen Voraussetzungen an Datenbanken aus § 4 Abs. 2 1 UrhG[794]. Ebenso „wortgleich" sind beide hinsichtlich ihres Normzwecks und ihrer Prägung durch Investitionsmomente abzulehnen: In beiden Fällen wird nicht das einzelne Datum, sondern entsprechend dem Schutzzweck der Norm die Struktur- bzw. Investitionsleistung geschützt und

788 Vgl. hierzu zum geistigen Eigentum in der Dogmatik des Art. 14 GG *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 314 ff; *Stern*, StaatsR IV/1, S. 2195 f.

789 Vgl. *Dorner*, CR 2014, 617 (621).

790 § 4 Abs. 2 S. 1 Hs. 1 UrhG; *Ahlberg/Lauber-Rönsberg* in: Ahlberg/Götting/Lauber-Rönsberg, BeckOK UrhR, § 4 UrhG, Rn. 18.

791 *Thum/Hermes* in: Wandtke/Bullinger, Praxiskommentar UrhR, § 87a UrhG, Rn. 25.

792 *Marquardt* in: Wandtke/Bullinger, Praxiskommentar UrhR, § 4 UrhG, Rn. 8; *Schulze* in: Dreier/Schulze, UrhG, § 2, Rn. 8; *Auer-Reinsdorff*, FS Schneider, S. 205 (Rn. 42 ff). Vgl. auch *Zech*, CR 2015, 137 (141).

793 *Vohwinkel* in: Ahlberg/Götting/Lauber-Rönsberg, BeckOK UrhR, § 87a UrhG, Rn. 55; *Auer-Reinsdorff*, FS Schneider, S. 205 (Rn. 24-26).

794 Ähnlich auch *Auer-Reinsdorff*, FS Schneider, S. 205 (Rn. 39).

mit vermögenswerten Rechten versehen.[795] Dabei geht das Datum oder das Element einer Datenbank nicht in die Datenbankstruktur über bzw. verschmelzen sie nicht – ausgenommen die Datenbank zeichnet sich durch eine Vielzahl von Unterstrukturen und -verzweigungen aus. Auch dann ist aber nur die Eigenart der Verzweigung geschützt, nicht das verzweigte Datum selbst. Weitergehende Ansätze eines Eigentumsrechts aus dem Urheberrecht an Computerprogrammen gem. §§ 69a ff UrhG[796] oder originär aus § 2 Abs. 2 UrhG schlagen ebenfalls fehl. Gegen den Computerprogramm-Vorschlag spricht ebenso der Normzweck, welcher sich wie § 4 Abs. 2 und § 87a Abs. 1 1 UrhG dem Fruchtbarmachen der Investition menschlicher, technischer und finanzieller Mittel verschrieben hat[797].[798] Ein eigenständiger Schutz als persönliche geistige Schöpfung im Sinne des § 2 Abs. 2 UrhG kann dagegen nur dann Erfolgen, wenn die digitale Identität in ihrer Kombination aus Einzeldaten eine Prägung der Urheberpersönlichkeit feststellen lässt, zugleich aber nicht bloß die personenbezogenen Daten des Urhebers wiedergibt. Das Urheberrecht als solches würdigt mit der Schöpfung bzw. dem Werk lediglich einen besonderen Teil der Persönlichkeit, welcher durch Gestaltungsmittel verzerrt, verfremdet und ggf. entkoppelt werden kann.[799] Demnach ist der Ansatz nur brauchbar, wenn es sich bei der digitalen Identität um eine Kunstfigur im Sinne eines Alter Ego handelt. Zumindest findet sich darin die Parallele eines urheberrechtlichen Schutzes von einzelnen Romanfiguren eines Buches, welcher vom Bundesgerichtshof angenommen wurde.[800] Eine dahingehend vertiefte Auseinandersetzung von Kunstfiguren in der Digitalisierung bedarf jedoch

795 StRspr EuGH, Urteil vom 09. November 2004, Az. C-203/02, Rn. 31 ff; *Dorner*, CR 2014, 617 (621, 622); *Zech*, CR 2015, 137 (141, 143). Nur zu §§ 87a ff UrhG siehe *Specht*, CR 2016, 288 (293 f); *Ensthaler*, NJW 2016, 3473 (3475 f); *Grützmacher*, CR 2016, 485 (491); *Hoeren*, Big Data und Recht, S. 22 f; *Drexl* et al., GRUR Int. 2016, 914 (915 f). Vgl. auch BGH GRUR 1999, 923 (924) – Tele-Info-CD. Bei Teildatensätzen annehmend *Grützmacher*, CR 2016, 485 (488), was dem Inhaber einer digitalen Identität aber ebenfalls kein Eigentumsrecht zuordnen würde. Vielmehr vererbt sich die Investitionsleistung auch auf Datenbankteile.

796 Ohne eine Nennung weiterer Vertreter *Härting*, CR 2016, 646 (647); *Wolff* in: Laufhütte/Saan/Tiedemann, Leipziger Kommentar StGB, § 303a, Rn. 2.

797 ErwGr 2 RL 2009/24/EG – Computerprogramm-RL.

798 Ferner ablehnend aufgrund mangelnden Werkcharakters *Zech*, CR 2015, 137 (141).

799 Vgl. *Ernst*, Weg zum Digitalen Staat, S. 33 (50).

800 BGH GRUR 2014, 258 (Rn. 27) – Pipi Langstrumpf.

einer eigenen rechtswissenschaftlichen Betrachtung.[801] Ein gesonderter Schutz kraft Immaterialgüterrecht ist de lege lata nicht ersichtlich[802]; das Urheberrecht hat keinen persönlichkeitsrechtlichen Bezug.[803]

In Ermangelung einer geeigneten Zuordnung innerhalb der zivilrechtlichen Begrifflichkeiten wurden in der rechtswissenschaftlichen Literatur Stimmen laut, ein nach dem Vorbild bestehender Immaterialgüterrechte ausgeformtes Immaterialgüterrecht an Daten sui generis zu etablieren. Dieses „Recht des Datenerzeugers"[804] würde voraussetzten, dass der politisch beabsichtigte Zuordnungsgedanke in die Tat umgesetzt würde und dementsprechend neue Rechtsverhältnisse zwischen Akteuren möglich wären. Durch das „Verrechtlichen" des (alltäglichen) Umgangs mit Daten und Informationen im Zeitalter des Big Data könnten entsprechend Anreize zum Schaffen von Daten und Verarbeitungsmöglichkeiten (konkret: Algorithmen) gesetzt werden.[805] Außerdem würde ein Offenbarungsgedanke gefördert, geheime Informationsgüter bei Aussicht auf ein Entgelt offenzulegen.[806] Was *Zech* in seiner für die Diskussion um das Dateneigentum fundamentgebenden Publikation jedoch meint ist das Eigentumsrecht an technischen Daten ohne jeglichen Personenbezug, wie sich am Beispiel von Maschinendaten auf einem Bauernhof erkennen lässt. Dementsprechend räumt *Zech* leider nicht die Bedenken von *Dorner*[807] aus wie beabsichtigt[808]. Dies vermag aber auch nicht durch weitere, spätere Beiträge von *Ensthaler*[809] und *Fezer*[810] zu gelingen. *Ensthaler* widmet sich ebenfalls nur der Verwertung von Maschinendaten, wozu er § 950 BGB

801 Vgl. *Redeker*, CR 2011, 634 (636), welcher lediglich das Durchschlagen eines persönlichkeitsrechtlichen Schadens von der Kunstfigur auf die tatsächliche Person bespricht. Treffender dagegen, wenngleich ebenso oberflächlich, die Ausführungen zu Avatarpersönlichkeiten in *Berberich*, Virtuelles Eigentum, S. 104-105.

802 *Dorner*, CR 2014, 617 (622, 626).

803 Vgl. *Vohwinkel* in: Ahlberg/Götting/Lauber-Rönsberg, BeckOK UrhR, § 87a Abs. 1 UrhG, Rn. 4.

804 So bezeichnend *Zech*, CR 2015, 137 (144).

805 So *Zech*, CR 2015, 137 (144 f).

806 *Zech*, CR 2015, 137 (145).

807 Siehe *Dorner*, CR 2014, 617 (626).

808 So einleitend *Zech*, CR 2015, 137 (144).

809 *Ensthaler*, NJW 2016, 3473 ff.

810 *Fezer*, MMR 2017, 3 ff sowie *Fezer*, ZD 2017, 99 ff.

sowie das Datenbankrecht als Inspiration nutzt und ein unmittelbares Recht an Maschinendaten konstruiert.[811] Der Ansatz lässt sich allerdings nicht auf personenbezogene Daten übertragen, da sich bei einer solchen Regelung der sogleich zu diskutierende Kulminationspunkt zweier verfassungsrechtlicher Rechtsgüter – das Grundrecht auf informationelle Selbstbestimmung und die Eigentumsgarantie – findet. Weiter schlägt *Fezer* ein „repräsentatives Dateneigentum" als Abwehr- und Vermögensrecht des Datenproduzenten vor.[812] Dies soll (zunächst) nur verhaltensgenerierte Daten umfassen und daher personenbezogene Daten ausschließen[813], was vor dem Hintergrund der aktuell weiten Definition der Personenbeziehbarkeit von Daten allerdings fragwürdig erscheint. Beispielsweise ordnet der Europäische Datenschutzbeauftragte durch das Nutzerverhalten generierte Daten als personenbezogen ein und lehnt die Regulierung personenbezogener Daten als Eigentum ab.[814] Möglicherweise führte dies auch zum erkennbaren Dissens im erweiterten Vorschlag: Einerseits geht der Ansatz von „reflexiven Daten" als Gegenstand des Dateneigentums und Sammelbegriff für personenbeziehbare, verhaltensgenerierte und maschinengenerierte Daten aus[815] und bezeichnet personenbezogene Daten zwischenzeitlich als ein Segment der verhaltensgenerierten Daten[816], statuiert aber andererseits: „Regelungsgegenstand des Datenschutzrechts sind personenbezogene Daten, Regelungsgegenstand des Dateneigentumsrechts sind verhaltensgenerierte Daten."[817] So werden verschiedene Gegenstände und damit Rechtsmaterien vermischt, bei der Ausformung des repräsentativen Dateneigentums allerdings ohne erkennbare Abgrenzungsmerkmale voneinander getrennt. Daher geht letztgenannte Schlussfolgerung nur dann auf, wenn – wie sogleich unter D.I.1.d)aa)(3) zu erörtern – verhaltensgenerierte Daten als nicht-personenbezogene Daten zu

811 *Ensthaler*, NJW 2016, 3473 (3474). Zu den ökonomischen Aspekten eines Eigentums sui generis an Maschinendaten siehe *Kerber*, GRUR Int. 2016, 989 ff.

812 *Fezer*, MMR 2017, 3 (3); *Fezer*, ZD 2017, 99 (102). Umfangreich konzeptionell darlegend in *Fezer*, Repräsentatives Dateneigentum sowie gekürzt in *Fezer*, Digitales Dateneigentum – ein grundrechtsdogmatisches Bürgerrecht in der Zivilgesellschaft, S. 101 ff.

813 *Fezer*, ZD 2017, 99 (101).

814 Siehe *Buttarelli*, Opinion 4/2017, S. 3, 6.

815 *Fezer*, Repräsentatives Dateneigentum, S. 35 ff.

816 *Fezer*, Repräsentatives Dateneigentum, S. 40 f.

817 *Fezer*, Repräsentatives Dateneigentum, S. 46.

qualifizieren sind. Darüber hinaus wird die Aufgabe der Abgrenzung, Verwaltung und (dogmatisch sauberen) Einordnung der Daten nach Vorstellung von *Fezer* in die Hände einer sog. Datenagentur gelegt. Ihre Hauptaufgabe soll sein, „als Repräsentant der Bürger mit den Unternehmen und/oder deren Repräsentanten die Digitalisierungsbedingungen einer digitalen Generierung der Bürgerdaten und deren weitere Verwendung" zu verhandeln[818], unter Berücksichtigung datenschutzrechtlicher Prinzipien wie der Transparenz, der Datenportabilität sowie Interoperabilität[819]. Augenscheinlich wird auch an dieser Stelle trotz ausdrücklichem zivilrechtlichem Schwerpunkt[820] das Datenschutzrecht beliehen, auch wenn es sich nicht um personenbezogene bzw. -beziehbare Daten handelt und nach Ansicht von *Fezer* ein eigenständiges, vom Datenschutzrecht gelöstes Rechtsinstitut gelten müsse[821]. Folglich bleibt zweifelhaft, inwiefern das Konstrukt trotz seiner durch zivilrechtliche Ausgestaltung gestärkten Datensouveränität ebendiese unmittelbar bei den Grundrechtsträgern und Datensubjekten belässt. Weiter lässt sich daran zweifeln, dass die faktisch getrennte Eigentümerstellung hinsichtlich der Hardware und der darauf befindlichen Daten, sofern sie auseinanderfällt, unproblematisch durchsetzbar wäre.[822] Das Einräumen dinglicher Berechtigungen zu Lasten des Eigentums des anderen mag zwischen Privatpersonen noch zu regeln sein[823], bedeutet aber bei Cloud-Speichern in der Konsequenz selbige Rechtespositionen und entsprechendes Problempotential[824].[825] Letztendlich bleibt die Notwendigkeit eines eigenständigen Rechts am Dateneigentum und die (legislative) Auflösung eben aufgezeigter Konflikte erst abschließend zu diskutieren.

818 *Fezer*, Digitales Dateneigentum – ein grundrechtsdogmatisches Bürgerrecht in der Zivilgesellschaft, S. 101 (155); *Fezer*, Repräsentatives Dateneigentum, S. 77/78.

819 Siehe *Fezer*, Repräsentatives Dateneigentum, S. 80 ff.

820 *Fezer*, Repräsentatives Dateneigentum, S. 77: „Rechtskonstitution eines repräsentativen Dateneigentums als ein Bürgerrecht sui generis mit *zivilgesellschaftlicher Gestaltungskompetenz* der Bürger" – Hervorhebung im Original nicht enthalten.

821 Vgl. *Fezer*, Repräsentatives Dateneigentum, S. 33, 38, 46.

822 Vgl. *Ernst*, Weg zum Digitalen Staat, S. 33 (53 f).

823 Hierzu einen Vorschlag auf Basis der Rechtsprechung zum virtuellen Hausrecht darstellend *Berberich*, Virtuelles Eigentum, S. 105 ff.

824 *Kutscher*, Der digitale Nachlass, S. 28/29. Eine Lösung durch differenzierte Lese- und Schreibrechte aufzeigend *Martini* et al., MMR-Beil 2021, 3 (16 ff).

825 Aus weiteren Gründen zweifelnd *Stender-Vorwachs*/*Steege*, NJOZ 2018, 1361 (1365); *Kutscher*, Der digitale Nachlass, S. 27 f.

Schließlich könnte sich eine Analogie aus dem Strafrecht ergeben, welche den Ansatz von *Fezer* obsolet werden lässt. Nicht selten – und berechtigterweise – wurde in der rechtswissenschaftlichen Literatur der strafrechtliche Datenbegriff umgarnt.[826] Grundlage hierfür bildet der sog. Skripturakt: Zurückgehend auf *Welp*, ist darunter im Rahmen des § 202d bzw. § 303a StGB die Zuordnung des (strafrechtlichen) Datums zum Verfügungsbefugten qua initiierender Datenerstellung zu verstehen. Dateninhaber ist zunächst derjenige, der die Daten erzeugt und damit die Speicherung oder Übermittlung selbst unmittelbar bewirkt hat.[827] Dabei soll auch der Wille des Verfügungsberechtigten einbezogen werden[828]; ebenso dienen Schutzvorkehrungen wie Passwörter als Indiz für eine Befugnis[829]. Die Definition fängt insofern das von der Literatur[830] gesehene und im Rahmen des Regierungsentwurfs verworfene[831] Schutzgut auf, das sich im Schutz des formellen Datengeheimnisses und der dahinter stehenden Privatsphäre sowie der Verfügungsbefugnis als Ausprägung der informationellen Selbstbestimmung erschöpft. Mithin wird im Schutz des Datenbestandes selbst auch ein Aspekt des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gesehen.[832] Trotz dieser Prägung ist das Datengeheimnis formell, umfasst also nicht ausschließlich bestimmte Arten von Daten und ist

826 Allen voran – und wiederholt – *Hoeren*, MMR 2013, 486 ff sowie *Hoeren*, Big Data und Recht, S. 11 ff und zuletzt *Hoeren*, MMR 2019, 5 ff. Ferner *Grützmacher*, CR 2016, 485 (490 f); *Schulz*, PinG 2018, 72 (73 f); *Dorner*, CR 2014, 617 (618); *Markendorf*, ZD 2018, 409 (410 f).

827 *Welp*, iur 1988, 443 (447). Später auch von der Rechtsprechung übernommen, siehe OLG Nürnberg, Beschluss v. 23.01.2013 – Az. 1 Ws 445/12 –, Rn. 14. Dagegen lediglich auf ausdrücklich oder stillschweigend geäußerte Voraussetzungen bzw. Vereinbarungen des Verfügungsberechtigten abstellend *Hilgendorf*, JuS 1996, 509 (512).

828 *Heger* in: Lackner/Kühl, StGB-Kommentar, § 202a, Rn. 3; *Hilgendorf*, JuS 1996, 509 (512); *Kargl* in: Kindhäuser/Neumann/Paeffgen, StGB, § 202a, Rn. 7.

829 Vgl. LAG Köln, Urt. v. 15.12.2003 – Az. 2 Sa 816/03 –, Rn. 23 = NZA-RR 2004, 527.

830 So *Hilgendorf*, JuS 1996, 509 (511); *Golla*/*von zur Mühlen*, JZ 2014, 668 (670). Lediglich den formellen Geheimnisschutz anerkennend *Eisele* in: Schönke/Schröder, StGB-Kommentar, § 202a, Rn. 1; *Kargl* in: Kindhäuser/Neumann/Paeffgen, StGB, § 202a, Rn. 3; *Berghäuser*, JA 2017, 244 (245); *Popp*, JuS 2011, 385 (386).

831 So *Stuckenberg*, ZIS 2016, 526 (530).

832 Vgl. *Welp*, iur 1988, 443 (448); *Dorner*, CR 2014, 617 (618); *Schulz*, PinG 2018, 72 (73).

daher weit zu verstehen[833]. Er schließt ebenso personenbezogene Daten ein. Dies zum Anlass nehmend, formte sich in der Diskussion um das Dateneigentum die Übertragbarkeit der Grundsätze des Skripturaktes auf das zivilrechtliche Eigentum iSd § 903 BGB. Demnach ist ein Eigentumsrecht an Daten ebenso nach der Skriptur eines Datums auszurichten, das den Skribenten sowohl mit Vermögens- als auch Ausschließlichkeitsrechten ausstattet.[834] Indes, und trotz der bei Einbeziehung des Skriptur-Ansatzes erkennbaren Parallele zur Eigentümerstellung des § 903 BGB, erscheint es fraglich, ein Dateneigentum auf einer Definition aufzubauen, die aufgrund von Zweifeln an der Bestimmtheit des § 202a StGB geschaffen wurde[835]. Zwar ist es gerade die Arbeit der Wissenschaft und Rechtsprechung, weite Rechtsbegriffe zu konkretisieren. Dies kann jedoch nicht über den speziellen Bestimmtheitsgrundsatz des Art. 103 Abs. 2 GG hinweghelfen, auch bei einer engen Auslegung[836].[837] Die entsprechende Regelungsdichte bei Straftatbeständen muss die Legislative selbst herstellen; sie kann nicht auf Exekutive, Judikative oder die erkenntnissuchende Wissenschaft abgewälzt werden.[838] Wann eine Skriptur vorliegt, ist für den Bürger als Norm- und Verhaltensadressaten wohl kaum nachvollziehbar. Vielmehr bedarf es konkreter Regelungen, um den Anforderungen der Institutsgarantie des Art. 14 Abs. 1 GG gerecht zu werden. Sowohl die Inhalte als auch Schranken sind durch den Gesetzgeber festzulegen, Art. 14 Abs. 1 S. 2 GG. In der Tiefe vermag der Ansatz ebenso nicht überzeugen, berücksichtigt er nicht die mangelnde Rivalität, Exklusivität und Abnutzbarkeit von Daten.[839] Auch bei Zurückverfolgen des Skribenten bzw. des Moments der Erstspeicherung kann das Datum vervielfältigt und ggf. manipuliert werden; ein

833 *Singelnstein*, ZIS 2016, 432 (432, 434); *Stuckenberg*, ZIS 2016, 526 (531); *Berghäuser*, JA 2017, 244 (245).

834 *Hoeren*, MMR 2013, 483 (487 f, 490 ff); vgl. auch *Dorner*, CR 2014, 617 (618).

835 *Golla*/*von zur Mühlen*, JZ 2014, 668 (670); *Singelnstein*, ZIS 2016, 432 (435 f); *Grützmacher*, CR 2016, 485 (491 f); OLG Nürnberg, Beschluss v. 23.01.2013 – Az. 1 Ws 445/12 –, Rn. 11.

836 Hierzu OLG Nürnberg, Beschluss v. 23.01.2013 – Az. 1 Ws 445/12 –, Rn. 11.

837 Wegen fehlender zivilrechtsimmanenter Regelung ebenfalls ablehnend *Haustein*, Möglichkeiten und Grenzen von Dateneigentum, S. 77 ff.

838 *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 103 II, Rn. 87, 106 f.

839 *Stuckenberg*, ZIS 2016, 526 (532).

rechtliche Durchsetzbarkeit nach unberechtigter Vervielfältigung bleibt weiterhin fragwürdig. Überdies ist die Umsetzung der Theorie in technischer Hinsicht starken Zweifeln ausgesetzt: Um die Skribentenstellung auch außerhalb des Herrschaftsbereiches des Skribenten erkennen zu können, bedarf es einer eindeutigen und universellen Erkennbarkeit – insbesondere vor dem Hintergrund der Publizität des Sachenrechts[840].[841] Dies ließe sich beispielsweise als Präfix oder digitaler Fingerabdruck bewerkstelligen, der bei der Erstellung von Dokumenten und anderen Dateien stets implementiert wird. Jede Datei erhält auf diese Weise eine digitale Signatur, wobei einst auch der digitale Personalausweis hierzu genutzt werden sollte[842]. Exemplarisch: Geeigneter, da der breiten Öffentlichkeit zugänglich, erscheint sogar eine staatliche, dezentral verwaltete Blockchain, welche die originären Eigentumsrechte ebenso abbildet wie die abgegebenen bzw. erteilten Nutzungsrechte.[843] Das Frage nach der allgemeinen Zugänglichkeit und Verständlichkeit der Blockchain, ein potentielles Manipulationsrisiko aufgrund Sicherheitslücken oder durch einen Mehrheits-Angriff[844] sowie letztlich die dadurch entstehende Verknüpfung von personenbezogenen Daten mit Hash-Werten, welche dann nur noch als Pseudonyme fungieren[845], stehen dieser Idee entgegen. Maschinendaten, die mit dem personalisierten Public und Private Key verknüpft wurden und wegen des Blockchain-Ansatzes untrennbar bzw. unlöschbar sind, sind dann zugleich Gegenstand des Datenschutzrechts – das Grundrecht auf informationelle Selbstbestimmung und das Eigentumsrecht des Art. 14 Abs. 1 GG müssen dann in ein angemessenes Verhältnis gesetzt werden, um auf fruchtbarem Rechtsboden zu stehen. Unter anderem müsste das (datenschutzrechtliche) Recht auf Vergessenwerden, das bei einer Blockchain ohnehin problematisch ist[846], mit

840 Hierzu *Oechsler* in: Säcker et al., MüKo BGB, Bd. VII, § 932, Rn. 5 f; *Prütting*, Sachenrecht, 38 f.

841 Dies ebenso beispielhaft aufzeigend *Singelnstein*, ZIS 2016, 432 (433); *Specht*/*Rohmer*, PinG 2016, 127 (129).

842 Siehe die Unterschriftswirkung der elektronischen Signatur des Personalausweises gem. Art. 25 Abs. 2, 3 Nr. 23 eIDAS-VO, § 22 PAuswG sowie *Borges*, NJW 2010, 3334 (3335).

843 Dies vorschlagend *Markendorf*, ZD 2018, 409 (412 f).

844 Siehe hierzu *Pesch*, Cryptocoin-Schulden, S. 33 f.

845 Vgl. hierzu *Klar/Kühling* in: Kühling/Buchner, DSGVO, Art. 4 Nr. 1 DSGVO, Rn. 34.

846 Hierzu ausführlich *Martini*/*Weinzierl*, NVwZ 2017, 1251 ff.

der immerwährenden Publizitätswirkung in Einklang gebracht werden. Darüber hinaus setzen die genannten technischen Möglichkeiten für eine objektive Erkennbarkeit entsprechende Datei- und Betriebssysteme oder Verknüpfungen in bestehenden Systemen und nationale wie internationale Standards voraus, die allesamt bislang nicht ersichtlich sind. Ein Dateneigentum analog § 903 BGB auf Basis der Skriptur aufzubauen ist demnach ein labiles Gerüst, dessen Tragkraft auch in Zukunft nicht zu überzeugen vermag. Auch letzte „Baumaßnahmen" in dieser Hinsicht durch *Hoeren*, welcher das Dateneigentum gegen den Datenbesitz eintauscht[847] und damit den Ansatz von *Redeker*[848] aufgreift, können die Tragkraft oder argumentative Standfestigkeit nicht verbessern.[849] Schließlich fehlt es weiterhin an der Publizität und den weiteren dargelegten Möglichkeiten; auch der Besitz ist von der Prärogative des Art. 14 Abs. 1 S. 2 GG umfasst[850] und macht konkrete einfachgesetzliche Regelungen erforderlich.

Zusammenfassend ist in keiner der Disziplinen der Rechtswissenschaft ein brauchbarer Ansatz für ein Eigentum an personenbezogen Daten und damit auch digitalen Identitäten ersichtlich.[851]

(3) Notwendigkeit einer eigenständigen Regelung: Eine Frage des Schutzguts

Doch, ist die Diskussion tatsächlich ausgefochten und mit Geltung der Datenschutz-Grundverordnung überwunden? Der erneute Ansatz von *Hoeren* deutet das Gegenteil an. Für eine tatsächliche Antwort – und damit auch eine Antwort

847 *Hoeren*, MMR 2019, 5 ff, wobei der Autor lediglich den Begriff austauscht, in der Argumentation allerdings weitgehend gleich bleibt – vgl. *Hoeren*, MMR 2013, 486 (487 ff) sowie *Hoeren*, Big Data und Recht, S. 11-38. Dagegen wohl den von *Hoeren* gemeinten „blanken Besitz" prinzipiell befürwortend *Michl*, NJW 2019, 2729 (2730 ff). Im Ergebnis kehrt jedoch auch *Michl* zu den persönlichkeitsrechtlichen Interessen zurück.

848 Siehe *Redeker*, CR 2011, 634 (639).

849 Zur Zweifelhaftigkeit des digitalen Besitzes siehe vgl. *Kutscher*, Der digitale Nachlass, S. 28 f.

850 *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 323. Vgl. BVerfGE 89, 1 (5 f).

851 Mit gleichem Ergebnis *Schulz*, PinG 2018, 72 (74 f). Vgl. auch *Dorner*, CR 2014, 617 (626); *Drexl* et al., GRUR Int. 2016, 914 (914); *Determann*, MMR 2018, 277 (278).

auf die Frage der Notwendigkeit eines Dateneigentums – sind die jeweiligen Schutzgüter der Grundrechte vertiefend zu betrachten.

„Daten haben einen wirtschaftlichen Wert." – diese herrschende Ansicht wird so oder in anderer Formulierung vorgetragen, sei es unter Verweis auf unzählige Vergleiche mit Gold, Öl oder generell als zentrales Wirtschaftsgut.[852] Der Tatsache, dass personenbezogene Daten per se einen Gegenwert besitzen, wohnt insofern die normative Kraft des Faktischen inne.[853] Die (neue) Regelung des § 312 Abs. 1a BGB manifestiert diese Diskussion letztlich – wenn auch nicht synallagmatisch[854] –, zurückgehend auf ErwGr 24 und Art. 3 Abs. 1 UAbs. 2 RL (EU) 2019/770 (Digitale-Inhalte-Richtlinie). Ein tatsächlicher, ökonomischer Wert oder abstrakte Wertschöpfungsmaßstäbe sind nicht ersichtlich. Der Wert der Daten bemisst sich nicht an einer allgemeingültigen Währungsordnung; Daten haben je Vertragspartner und Vereinbarung einen unterschiedlichen Wert.[855] Dafür spricht auch, dass gelegentlich in Ermangelung von Rechtsgrundlagen auf die Privatautonomie und die vertragliche „Lizenzierung" der eigenen Daten abgestellt wird.[856] Daher erscheint die Einordnung in die Materie des Art. 14 Abs. 1 GG naheliegend, wo unkörperliche „Vermögensgüter" verschiedenen Vertragstypen des BGB – und so auch personenbezogene Daten – unterliegen könnten[857]. Demgemäß bedarf es prima facie einer Aktivierung des Schutzgutes für das konstitutive Handeln des Gesetzgebers. Dies wird in Belangen des Art. 14 Abs. 1 GG dann aktiviert, wenn

852 Siehe grundlegend *Wandtke*, MMR 2017, 6 (7 f) sowie *Bisges*, MMR 2017, 301 (301 f); *Dickmann*, RuS 2018, 345 (345); *Markendorf*, ZD 2018, 409 (411); *Fezer*, MMR 2017, 3 (3); *Schefzig*, DSRITB 2015, 551 (551); *Alexander*, K&R 2016, 301 (304); *Lehmann*, FS Schneider, S. 133 (133) – regelmäßig ohne Verweis oder unter Verweis auf erstere. Als zivilrechtlichen Leistungsgegenstand iSd §§ 241, 362 BGB einordnend *Langhanke*, Daten als Leistung, S. 97 f. Eine Wertzuordnung durch Datenverknüpfung aufzeigend *Bisges*, MMR 2017, 301 (302 f). Der Verfasser erhebt keinen Anspruch auf Vollständigkeit.

853 Vgl. *Wandtke*, MMR 2017, 6 (9).

854 *Martens* in: Hau/Poseck, BeckOK BGB, § 312, Rn. 10a.

855 Vgl. auch *Beise*, RDi 2021, 597 (600). Zu Faktoren der Wertbemessung siehe ausführlich *von Lewinski*, Wert von personenbezogenen Daten, S. 209 ff.

856 Vgl. zur sog. Datenlizenz *Schefzig*, DSRITB 2015, 551 ff; *Schwartmann*/*Hentsch*, PinG 2016, 117 (124).

857 So kann es sich um einen Kaufvertrag über unkörperliche Güter gem. §§ 453 Abs. 1 Alt. 2, 433 ff BGB oder einen Tauschvertrag gem. §§ 480, 433 ff BGB handeln – so *Markendorf*, ZD 2018, 409 (410); vgl. *Lehmann*, FS Schneider, S. 133 (134).

die Zubilligung eines Martkwertes durch die Gesellschaft erfolgt ist oder sich derart abzeichnet, als dass der Gesetzgeber entsprechende Inhalte manifestieren und Schranken zum Schutz bestehender (Grund-)Rechte festlegen muss.[858] Auf diese Weise gewährleistet der Gesetzgeber, einen Freiheitsraum in vermögensrechtlicher Hinsicht abzusichern und jedem Grundrechtsträger ein selbstbestimmtes Leben zu ermöglichen.[859] Diese objektive, garantierende Schutzfunktion schlägt sich subjektiv in Form des bereits dargestellten[860], personalen Freiheitsrechts zum „Schutz des Erworbenen"[861] nieder.[862] Zudem soll der Schutz des Gegenwärtigen zu zukünftigen Leistungen anspornen, da auch diese qua Gewährleistungsfunktion des Art. 14 Abs. 1 GG vom Gesetzgeber zumindest mit Entstehen zu schützen sind.[863] Das Schutzgut des Art. 14 Abs. 1 GG lässt sich folglich nicht in wenige Worte fassen, sondern ist entsprechend seiner Konzeption vielseitig, erstreckt sich über eine Vielzahl an Funktionen und einzelnen Gewährleistungen.[864] Sie erschöpfen sich jedoch in einer allumfassenden Verfügungsfreiheit über vermögenswerte Güter und Rechte, die als vermögensrechtliche Privatautonomie zu begreifen ist.[865]

Ähnlich zersplittert scheint das Schutzgut des Grundrechts auf informationelle Selbstbestimmung, blickt man auf die Zusammenfassung von *Veil*. Wohingegen das Bundesverfassungsgericht das Grundrecht bei seiner Taufe zum Schutz der

858 *Eschenbach*, Der verfassungsrechtliche Schutz des Eigentums, S. 597 f.

859 StRspr BVerfGE 24, 367 (389); 30, 292 (334); 53, 257 (290); 79, 292 (303 f); 97, 350 (370 f); 100, 1 (32); 102, 1 (15); 104, 1 (8 f); 115, 97 (110); 134, 242 (290 f, Rn. 167); 143, 246 (316 f, Rn. 195). Ferner *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 1; *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 2; *Eschenbach*, Der verfassungsrechtliche Schutz des Eigentums, S. 595 f.

860 Siehe D.I.1.d)aa)(1).

861 *Stern*, StaatsR IV/1, S. 2126 mwN in Fn. 2.

862 *Wendt* in: Sachs, GG, Art. 14, Rn. 12. Im Detail auch *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 3 ff; *Meyer-Abich*, Der Schutzzweck der Eigentumsgarantie, S. 25 ff.

863 Zu diesem Gedanken bereits ausführlich *Meyer-Abich*, Der Schutzzweck der Eigentumsgarantie, S. 26-28.

864 Im Einzelnen siehe *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 3 ff sowie 112 ff; ebenso tiefgehend *Stern*, StaatsR IV/1, S. 2128 ff zu den Kernelementen der Eigentumsgarantie.

865 Vgl. zum Aspekt der Privatautonomie *Isensee* in: Isensee/Kirchhof, HStR VII, § 150, Rn. 64.

Selbstbestimmung vor dem Hintergrund neuer technischer Gefährdungen schuf[866], scheint der darin verankerte Datenschutz nach Ansicht der Wissenschaft in einer Vielzahl von Formulierungen zu bestehen. So schützt der Datenschutz nicht nur die „informationelle Selbstbestimmung", sondern auch die „informationelle Unversehrtheit", „das Grundrecht auf e-privacy" und bzw. oder die „informationelle Gewaltenteilung" – um nur einige zu nennen.[867] Rekurrierend auf die ausführliche Darstellung der umfassten datenschutzrechtlichen Prinzipien als Teil des Grundrechts auf informationelle Selbstbestimmung[868] ist festzustellen, dass diese Aspekte ebenso Teil des Schutzgehalts bzw. des Schutzgutes sind. Schutzgut sind nicht nur die personenbezogenen Daten und die Selbstbestimmung über ihren Verbleib und ihre Nutzung.[869] Neben Auskunfts- und Informationsrechten sind auch Aspekte der Vertraulichkeit (Stichwort: e-privacy) sowie die datenmäßige Integrität im Sinne einer Richtigkeit des Datums (Stichwort: informationelle Unversehrtheit) umfasst. Dies leitet sich schon aus der Aussage des Bundesverfassungsgerichts ab: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und *wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag*, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."[870] Ein Abschätzen und Überschauen der Verarbeitung der eigenen Daten – auch einer digitalen Identität – erfordert Transparenz ebenso wie die Richtigkeit der Informationen. Weiter fungiert die „Richtigstellung" als Mittel der Selbstdarstellung der Person, was letztlich auf die persönlichkeitsrechtliche Prägung des Grundrechts

866 BVerfGE 65, 1 (41 f).

867 Weitere Antworten auf die Frage nach dem Schutzgut nennend *Veil*, Schutzgutmisere des Datenschutzrechts (Teil I), Abschnitt „Die Schutzgutdebatte".

868 Siehe D.I.1.b).

869 So BVerfGE 65, 1 (43): „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

870 BVerfGE 65, 1 (43).

zurückzuführen ist.[871] Demgemäß ist das Schutzgut des Grundrechts auf informationelle Selbstbestimmung ebenso facettenreich, findet seinen Kulminationspunkt allerdings in der Selbstbestimmung als Handlungsfähigkeit und Mitwirkungsfähigkeit des Individuums als Teil des freiheitlich-demokratischen Gemeinwesens.[872] Diese ist wiederum als informationelle Privatautonomie zu verstehen.

Letztendlich ist das Konstrukt des Dateneigentums, das vornehmlich durch die Politik und rechtswissenschaftliche Literatur geprägt wurde, in die aufgezeigte Dualität einzuordnen. Hält man die Datenschutz-Grundverordnung in ihrer aktuellen Form für den Ursprung der Debatte, könnte zumindest Erwägungsgrund 7 S. 2 DSGVO dafür sprechen: „Natürliche Personen sollen die Kontrolle über ihre eigenen Daten besitzen." Das Begriffspaar „Kontrolle besitzen" kann zu dem Trugschluss führen, dass das Datenschutzrecht oder die Grundverordnung ein eigentumsgleiches Verhältnis von Daten bezwecken bzw. forcieren wollten. Dieses Begriffspaar fand jedoch schon vorher seine Verwendung, wenngleich die Regelung noch nicht in Kraft war, und stellt wohl den eigentlichen Ursprung der Diskussion dar: Am 28.3.2017 eröffnete der damalige Bundesverkehrsminister Alexander Dobrindt mit einem sog. Datengesetz, Daten dem Sacheigentum gleichzustellen und eine entsprechende Eigentumsordnung einzuführen. Ebenso soll ein Zuordnungssystem des Eigentums konzipiert werden.[873] Dies ist allerdings aus den zuvor ausführlich dargestellten Gründen kaum möglich.[874] Ungehindert dessen statuiert der Grundriss des erhofften Gesetzes im Gleichklang mit dem Titel des Entwurfes „Strategiepapier Digitale Souveränität": „Der Schlüssel dazu ist die Datensouveränität des Einzelnen." Im Fokus des Entwurfes steht folglich die Souveränität des Individuums bezüglich Informationen, welche mangels Trennung sowohl personenbezogene wie nicht-personenbezogene Daten einbezieht.

871 *Ambrock* in: Jandt/Steidle, Datenschutz im Internet, A.II., Rn. 17 aE; *Herbst* in: Kühling/Buchner, DSGVO, Art. 5, Rn. 18; *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 5, Rn. 49 f.

872 So BVerfGE 65, 1 (43). Im Ergebnis zur Schutzgut-Debatte des Datenschutzrechts so auch *Bock*, Schutzgut des Datenschutzrechts (Teil I) sowie *Bock*, Schutzgut des Datenschutzrechts (Teil II).

873 Siehe https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html.

874 Siehe D.I.1.d)aa)(2).

Begreift man diesen Entwurf sowie die politische Aussage als Grundstein der nationalen Diskussion um das Dateneigentum, muss die Datensouveränität als Kern der Idee gesehen werden. Datensouveränität bzw. digitale Souveränität meint – ganz im Lichte der informationellen Selbstbestimmung – die Kenntnis und eigenverantwortliche Verfügung über den Verbleib und die Nutzung von Daten.[875] Sie entspricht einem persönlichen Verfügungs-[876] und Abwehrrecht[877], synonym der aufgezeigten informationellen Privatautonomie[878]. Diese kann sich unter anderem in Einwilligungen äußern, allerdings auch in der Information des Inhabers bzw. Datensubjekts. Damit weist die Idee deutliche Bezüge zur Volkszählungs-Rechtsprechung des Bundesverfassungsgerichts auf – mit den Worten des Gerichts ausgedrückt: „Im Mittelpunkt [...] stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt.“[879] Folglich besteht schon in der Grundlage der Diskussion eine erkennbare Tendenz in Richtung der informationellen Privatautonomie, obschon der Begriff ursprünglich als Platzhalter für rechtspolitische Forderungen verwendet wurde[880].

Diesem Ergebnis lässt sich nun entgegenhalten, dass der aktuelle Stand der Technik Anonymisierungsmöglichkeiten bietet und zumindest an für Statistiken und Heuristiken aufbereiteten Daten ein Eigentumsrecht im Sinne einer Wertschöpfungs- und Beteiligungsmöglichkeit bestehen sollte. Kern der informationellen Selbstbestimmung sind schließlich nur personenbezogene Daten. Diese Argumentation wurde nach erstmaligem Aufkommen der Debatte greifbar von Andrea Nahles in Form eines Daten-für-Alle-Gesetzes vorgeschlagen, mit Fokus auf eine Datenteilungspflicht für als Quasi-Monopol anzusehende Akteure.[881] Wohingegen sich

875 Zum Begriff siehe *Krüger*, ZRP 2016, 190 (190 f); *Seidel*, ZG 2014, 153 (155 f); *Beise*, RDi 2021, 597 (598); mit technischer Prägung auch *Broadnax* et al., DuD 2018, 74 (76 f). Inhaltlich kongruent, aber als Datenhoheit definierend *Martini* et al., MMR-Beil 2021, 3 (3, 16 ff). Dagegen ausschließlich institutionell verstehend *Karl*/*Hummert*, DuD 2021, 223 (224).

876 So *Stern*, StaatsR IV/1, S. 204. Vgl. auch *Kühling/Raab* in: Kühling/Buchner, DSGVO, Einführung, Rn. 26.

877 *Faust*, Ausschließlichkeitsrecht an Daten?, S. 85 (88).

878 Im Ergebnis so auch *Beise*, RDi 2021, 597 (598).

879 BVerfGE 65, 1 (41).

880 So *Richter*/*Hilty*, Die Hydra des Dateneigentums – eine methodische Betrachtung, S. 241 (251).

881 Siehe *Nahles*, Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, S. 2 ff.

Louven[882] berechtigterweise kritisch zu kartellrechtlichen Aspekten äußert, blieb die datenschutzrechtliche Rezeption aus[883]. Dies ist jedoch nicht zu verstehen als verfassungs- und datenschutzrechtliche Konformität der Absicht einer weiteren Variation des Dateneigentums. Ein vermögenswertes Recht an anonymisierten und nicht-personenbezogenen Daten oder ein freier Verkehr letzterer[884] kann nur hinsichtlich des letzteren Falles unproblematisch für das Datenschutzrecht sein, da diese Daten in Form bloßer Maschinendaten (tendenziell) keinen Personenbezug aufweisen. Sobald die Datenverarbeitung der Maschine bzw. des Geräts auf einer menschlichen Interaktion basiert, besteht zumindest die Möglichkeit einer Personenbeziehbarkeit durch Mustererkennung unter mehreren Benutzern, unter Umständen auch weitere Schlüsse wie Vorlieben, Tag-Nacht-Rhytmus, etc.[885] Beispielsweise lässt sich dies aus Smart Metern bzw. deren Maschinendaten und dem Verlauf der Stromnutzung anhand der Tageszeit ablesen. Bei Zusammenführung verschiedener Datensätze ergeben sich mithin Lebenssachverhalte, die dem Schutz des Grundrechts auf informationelle Selbstbestimmung unterliegen.[886] Auch wenn die Daten nach dem Diskussionspapier anonymisiert sein mögen, entspricht dies nur einer Risikominimierung.[887] Folglich gilt das zu anonymen und anonymisierten digitalen Identitäten ausgeführte hinsichtlich einer datenschutz- und grundrechtskonformen Verarbeitung im Lichte des Erforderlichkeitsprinzips.[888] Insgesamt ist der Ansatz des Diskussionspapiers im Kern konkreter, doch setzt er ebenfalls an den falschen Punkten an und übersieht das Potential der Personenbeziehbarkeit, das durch die geforderte Datenteilungspflicht noch erhöht werden könnte[889]. Das zumindest teilweise Einbeziehen datenschutzrechtlicher Aspekte kann jedoch als Fortschritt gewertet werden, wobei die mangelnde

882 Siehe Beitrag auf Telemedicus vom 13.02.2019 unter http://tlmd.in/a/3392.
883 Einzig *Geminn*, ZD-aktuell, 06492.
884 So *Nahles*, Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, S. 4.
885 *Buchmann*, DuD 2015, 510 (510 f).
886 *Buchmann*, DuD 2015, 510 (511); *Braun*, ZD 2018, 71 ff.
887 Vgl. *Hammer* in: Jandt/Steidle, Datenschutz im Internet, B. IV., Rn. 293; *Datenschutzkonferenz des Bundes und der Länder*, Das Standard-Datenschutzmodell (Version 2.0b), S. 16.
888 Siehe D.I.1.b)(2).
889 Derart *Geminn*, ZD-aktuell, 06492.

technische Auseinandersetzung den notwendigen State of the Art zum wirksamen Grundrechtsschutz vermissen lässt.

Somit bleibt nur die Möglichkeit des Gesetzgebers, ein vermögenswertes Recht an maschinengenerierten Daten ohne eine menschliche Einwirkung einzurichten. Dies erfordert jedoch aufgrund möglicher Kollisionen mit dem Grundrecht auf informationelle Selbstbestimmung, dass geeignete Sicherungsmaßnahmen von den Herstellern zur getrennten Verarbeitung und Speicherung personenbezogener wie nicht-personenbeziehbarer Maschinendaten vorgesehen werden. Dementsprechend ist die Forderung nach nationalen wie internationalen Standards für datenverarbeitende Systeme ebenso wie eine klarstellende Regelung zu anonymen wie anonymisierten Daten zu wiederholen.[890] Hinsichtlich der finalen Einordnung in die informationelle oder vermögensrechtliche Privatautonomie bleibt an der eigentlichen Idee des Dateneigentums in Form eines Ansatzes der Datensouveränität festzuhalten, der mit dem Grundrecht auf informationelle Selbstbestimmung bereits in Art. 2 Abs. 1 iVm 1 Abs. 1 GG verfassungsrechtlich verankert ist. Rein vermögensrechtliche Aspekte wie Konditionen zur Vertragsgestaltung über personenbezogene Daten, die wie erwähnt mit Blick auf Art. 6 Abs. 1 lit. b DSGVO nicht verschlossen erscheint, kann und sollte der Gesetzgeber zum Schutz personenbezogener Daten in diesen besonderen Konstellationen ganzheitlich regeln.[891] Insofern besteht eine dienende Funktion des Datenschutzrechts[892], die sich am gesamtgesellschaftlichen Interesse an Datenschutz sowie -integrität ausrichtet und im verfassungsrechtlichen Rahmen zu gewährleisten ist.[893] Dafür spricht vor allem die fehlende Anwendbarkeit des sog. Koppelungsverbots gem. Art. 7 Abs. 4 DSGVO für zweiseitige Geschäfte, da die Verankerung in Art. 7 DSGVO lediglich

890 Siehe hierzu bereits unter D.I.1.b)(2).

891 Vgl. *Richter*/*Hilty*, Die Hydra des Dateneigentums – eine methodische Betrachtung, S. 241 (259).

892 *Buchner*, DuD 2010, 39 (43).

893 Die Begrifflichkeit der „dienenden Funktion" stammt aus der Materie des Rundfunkrechts und geht auf BVerfGE 57, 295 (319 f) zurück. Nach Rechtsprechung bedarf es dazu eines objektiven Prinzips der Gesamtrechtsordnung (hier: informationelle Selbstbestimmung bzw. Privatautonomie), welcher subjektive Elemente zugleich bedingt und durch sie gestützt wird. Letzteres ist durch die einfachgesetzlich ausgestalteten Rechte sowie Verpflichtungen der Verantwortlichen gegeben.

zur Anwendung für die Einwilligung führt.[894] Die vermögensrechtliche Privatautonomie wird allerdings durch die informationelle Privatautonomie tangiert bzw. ist sie in diese einzubetten. Jede vermögenswerte Datenverarbeitung als Folge der informationellen Privatautonomie – beispielsweise mittels Einwilligung[895] –, die zu Lasten des Datenschutzes und zu einem erhöhten Risiko führt, ist durch den Gesetzgeber zu regeln und etwaigen Gefahren vorzubeugen. Bei dieser Ausgestaltung sind daher mögliche Kollisionen mit kollidierendem Verfassungsrecht zu vermeiden. Beispielsweise ist die Informationsfreiheit gem. Art. 5 Abs. 1 S. 1 Alt. 2 GG[896] und die multilaterale Sicht auf personenbezogene Daten zu berücksichtigen. Letztere tritt bei Verflechtungen personenbezogener Daten auf, die bei einem ausschließlich wirkenden Dateneigentum unlösbar werden.[897]

Der aus Sicht des Datenschutzes beabsichtigte freie Datenverkehr[898] würde dann eher gehindert als der Datenschutz gefördert. Insgesamt verbietet sich eine Eigentumsordnung für personenbezogene Daten folglich schon unter Berücksichtigung verfassungsrechtlicher Wurzeln bzw. Schutzgüter.[899]

894 Hierzu *Engeler*, ZD 2018, 55 (56, 58 f) sowie *Faust*, Ausschließlichkeitsrecht an Daten?, S. 85 (89 f). Zur Einwilligung in die vermögensrechtliche Nutzung von Daten siehe ferner *Kühling*/*Sackmann*, vzbv-Gutachten, S. 25 ff.

895 Für die weitere Regulierung und Fokussierung auf dieses Mittel der Selbstbestimmung *Kühling*/*Sackmann*, ZD 2020, 24 (29/30).

896 Hierzu *Specht*, CR 2016, 288 (294).

897 So *Determann*, ZD 2018, 503 (508).

898 Vgl. Art. 1 Abs. 1 sowie ErwGr 6 S. 5 DSGVO.

899 Dagegen ein Eigentumsrecht an Daten nach Art. 14 Abs. 1 GG mit positiver Einordnung in dessen Schutzgut einzig *Stranz*, Eigentumsrecht an personenbezogenen Daten, S. 55 f, 163 f; *Fezer*, Repräsentatives Dateneigentum, S. 61 f parallel zur. Ähnlich auch *Wiebe*/*Schur*, ZUM 2017, 461 (465), wobei dies als Leistungsschutzrecht ausgestaltet werden soll. *Boehm*, ZEuP 2016, 358 (386) weist dagegen – zutreffend – auf die notwendige gesetzliche Ausgestaltung hinsichtlich Inhalt und Reichweite hin, sofern man an diesem Ansatz festhielte; „Ein Immaterialgüterrecht sui generis für Daten ist nur denkbar, wenn die gesetzliche Normierung in diesem Bereich nicht abschließend ist." Erst dann könne sich eine rechtssichere bilaterale bzw. vertragliche Konstruktion etablieren – so iE auch *Kraul*, GRUR-Prax 2019, 478 (479 f).

(4) Ergebnis Die Eigentumsgarantie des Art. 14 Abs. 1 S. 1 Alt. 1 GG ist demgemäß in vielerlei Hinsicht ungeeignet und nicht auf die Idee des Dateneigentums anwendbar.[900] Dies ergibt sich sowohl aus der mangelnden Eröffnung des Schutzbereiches als auch bei vertiefter Betrachtung des Schutzguts. Um die aufgezeigte Nähe zum Grundrecht auf informationelle Selbstbestimmung aufzulösen, müsste man personenbezogene bzw. persönliche Daten als verselbstständiges, von der Person abgelöstes Gut betrachten können.[901] Dies ist allerdings aus praktischen wie technischen Erwägungen nicht möglich. Vielmehr empfiehlt es sich, von der Terminologie Abstand zu nehmen[902] und zum eigentlichen Schutzgut – der bereits erläuterten informationellen Selbstbestimmung – und dem Ansatz der Datensouveränität überzugehen. In der Folge findet sich die digitale Identität ebensowenig vom Schutz des Art. 14 Abs. 1 S. 1 Alt. 1 GG umfasst.

bb) Der digitale Nachlass Im Folgenden bleibt neben dem Eigentum eine weitere Garantie des Art. 14 Abs. 1 GG zu betrachten, die vor dem Hintergrund des Dateneigentums ebenso von Bedeutung ist. Artikel 14 Abs. 1 S. 1 Alt. 2 GG garantiert das Erbrecht, das, wie schon die Eigentumsgarantie, der Prärogative des Gesetzgebers zur Ausgestaltung von Inhalt und Schranken des Erbrechts iSd Art. 14 Abs. 1 S. 2 GG[903] unterliegt. Dementsprechend offen ist die Definition des Schutzgehalts, insbesondere des Schutzgegenstands. Seinem Gehalt nach umfasst die verfassungsrechtliche Erbrechtsgarantie subjektive Abwehrrechte ebenso wie

900 Den Ansatz des Dateneigentums ebenso ablehnend *Ernst*, Weg zum Digitalen Staat, 33 ff; *Dorner*, CR 2014, 617 ff; *Peschel*/*Rockstroh*, MMR 2014, 571 ff; *Heun*/*Assion*, CR 2015, 812 ff; *Boehm*, ZEuP 2016, 358 (384 ff); *Grützmacher*, CR 2016, 485 ff; *Härting*, CR 2016, 646 ff; *Specht*/*Rohmer*, PinG 2016, 127 ff; *Heymann*, CR 2016, 650 ff; *Berberich*/*Golla*, PinG 2016, 165 ff; *Schwartmann*/*Hentsch*, PinG 2016, 117 ff; *Kim*, GRUR Int. 2017, 697 ff; *Steinrötter*, MMR 2017, 731 ff; *Determann*, ZD 2018, 503 ff; *Schulz*, PinG 2018, 72 ff; *Raue*, NJW 2019, 2425 (2425); *Kühling*/*Sackmann*, ZD 2020, 24 (26 ff). Vgl. mit insolvenzrechtlichem Bezug *Hoffmann*, JZ 2019, 960 (965, 966 f).

901 Vgl. *Zech*, Information als Schutzgegenstand, S. 218 f.

902 So auch *Hoffmann*, JZ 2019, 960 (965, Fn. 75).

903 Hierzu *Leisner* in: Isensee/Kirchhof, HStR VIII, § 174, Rn. 14; *Wendt* in: Sachs, GG, Art. 14, Rn. 199a f.

die Institutsgarantie als objektive Komponente des Grundrechts.[904] Sie beziehen sich jedoch nicht auf einen eigenen Schutzgegenstand, sondern knüpfen als besondere Form der Privatautonomie an der Eigentumsgarantie des Art. 14 Abs. 1 GG an.[905] Hauptzweck des Erbrechts ist mithin, bereits zu Lebzeiten über den Verbleib des Erworbenen bestimmen und so auch prämortal auf den eigentlich postmortalen Sachverhalt einwirken zu können.[906] Insofern strahlt die Privatautonomie über den Tod hinaus. Mit dem Ableben erlischt die Rechtspersönlichkeit und die Verfügungsposition geht auf den Erben über, kann allerdings durch prämortale Handlungen wie ein Testament durch den Willen des Erblassers beeinflusst werden. Das Verfassungsrecht gibt den Regelungsgegenstand so nicht vor[907], ebenso wie sich das Bundesverfassungsgericht[908] oder die rechtswissenschaftliche Literatur einer Erläuterung entbehrt. Dies mag daran liegen, dass die Norm des Art. 14 Abs. 1 S. 2 GG diese Aufgabe dem Gesetzgeber überlässt, also mit Rücksicht auf die besagte Prärogative keine Notwendigkeit besteht. Dann würde aber die höchstrichterliche Erläuterung zum Eigentumsbegriff[909] gleichermaßen obsolet. Vielmehr spricht für die mangelnde Notwendigkeit, dass Eigentums- und Erbrechtsgarantie einheitlich zu betrachten sind. So sagt nicht nur die Konjunktion im Wortlaut des Art. 14 Abs. 1 S. 1 GG – „Eigentum *und* Erbrecht werden gewährleistet" – etwas über die inhaltliche Verknüpfung aus.[910] Weiter wirkt die gemeinsame Positionierung in Art. 14 Abs. 1 1 GG sowie die Geltung des S. 2 für beide Gehalte des S. 1 als Indiz.[911] Es erscheint daher nicht verwerflich, die Vererblichkeit vermögenswerter Rechte iSd eigentumsrechtlichen Definition

904 *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 516 f, 518 f.

905 *Isensee* in: Isensee/Kirchhof, HStR VII, § 150, Rn. 65.

906 *Wendt* in: Sachs, GG, Art. 14, Rn. 193; *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 513 f; *Stern*, StaatsR IV/1, S. 2320, 2324 f.

907 So auch BVerwGE 35, 278 (287).

908 Siehe nur BVerfGE 19, 202 (206), in der das BVerfG lediglich Ansprüche aus der Rentenversicherung als beschränkbaren Gegenstand des Erbrechts anerkennt. Darin zeigt sich die Parallele zum vermögenswerten Recht des Art. 14 Abs. 1 S. 1 Alt. 1 GG.

909 Siehe hierzu D.I.1.d)aa)(1) mwN.

910 Vgl. BVerfGE 93, 165 (174).

911 *Leisner* in: Isensee/Kirchhof, HStR VIII, § 174, Rn. 1 ff; *Stern*, StaatsR IV/1, S. 2320.

des Bundesverfassungsgerichts als Schutzgegenstand der Erbrechtsgarantie des Art. 14 Abs. 1 S. 1 Alt. 2 GG anzunehmen.[912]

Der so rein durch das Verfassungsrecht hergeleitete Schutzgegenstand ist allerdings durch die Wirkung des Art. 14 Abs. 1 S. 2 GG zu erweitern, sodass auch hier die einfachgesetzlichen Regelungen und die Ausgestaltung des Erbrechts einzubeziehen sind. Dementsprechend bleibt mit Blick auf § 1922 Abs. 1 BGB das Vermögen bzw. jedes vermögenswerte Recht vom Schutz der Erbrechtsgarantie umfasst. Im Gegensatz dazu deuten § 2047 Abs. 2 und § 2373 S. 2 BGB an, dass auch nicht-vermögenswerte Gegenstände wie persönliche Briefe oder Familienbilder Teil der Erbmasse sind.[913] Diese Lesart wird ferner durch die Rechtsprechung des Bundesgerichtshofes bestätigt.[914] Der Schutzgegenstand des Erbrechts erstreckt sich so grundsätzlich sowohl auf vermögenswerte als auch nicht-vermögenswerte Rechte oder Gegenstände und reicht damit weiter als der Eigentumsbegriff des Art. 14 Abs. 1 S. 1 Alt. 1 GG. Dies scheint zunächst widersprüchlich, betrachtet man die Verknüpfung von Eigentums- und Erbgarantie. Die Erweiterung des Erbrechts fußt allerdings nicht auf der bloß vermögensrechtlichen Privatautonomie, sondern fängt als Ausdruck der Selbstbestimmung[915] auch die informationelle Privatautonomie auf und ermöglicht auch in dieser Hinsicht das Erben von vertraulichen Briefen und Tagebüchern.

Die eben dargestellte Differenzierung zwischen vermögenswerten und nicht-vermögenswerten Gütern als Teil des verfassungsrechtlichen Erbrechts mag daher zunächst trivial oder gar obsolet erscheinen; die Erbrechtsgarantie ist wie dargestellt umfassend. Vor dem Hintergrund der digitalen Identität und dessen Einordnung in das Erbrecht des Art. 14 Abs. 1 S. 1 Alt. 2 GG entspinnt sich jedoch ein bis zuletzt umstrittenes Problemfeld, wie bereits unter B.II.2.a) angedeutet wurde. So ist fraglich, ob und wie die digitale Identität aufseiten des Erblassers

912 So auch *Leisner* in: Isensee/Kirchhof, HStR VIII, § 174, Rn. 4, 14.
913 Vgl. *Lohmann* in: Hau/Poseck, BeckOK BGB, § 2047, Rn. 3.
914 BGH, Urteil vom 12.7.2018, Az. III ZR 183/17, Rn. 49.
915 BVerfGE 99, 341 (351); *Stern*, StaatsR IV/1, S. 2325; *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 412; *Leisner* in: Isensee/Kirchhof, HStR VIII, § 174, Rn. 18; *Isensee* in: Isensee/Kirchhof, HStR VII, § 150, Rn. 65.

verfassungsrechtlich geschützt ist, er also auch hierüber als Inhaber prämortal verfügen kann. Die Frage nach dem Umgang und Verbleib dieser als Teil der digitalen Erbmasse wird in der Rechtswissenschaft unter dem Begriff des digitalen Nachlasses diskutiert. Diese Bezeichnung ist bislang nicht durch den Gesetzgeber oder die Rechtsprechung[916] definiert worden, sondern lediglich durch die rechtswissenschaftliche Literatur geprägt. Initiatorisch wirkte dabei die Stellungnahme des Deutschen Anwaltvereins zur Thematik, welcher mit dem Begriff des digitalen Nachlasses die „Gesamtheit des digitalen Vermögens" bzw. vermögenswerter Rechte beschreibt und „auch die Gesamtheit aller Accounts und Daten des Erblassers im Internet" erfasst.[917] Er sei aufgrund seines bloß deskriptiven Charakters weit zu verstehen.[918] Durch seine Endlosigkeit werden allerdings personenbeziehbare Datensätze mit rein maschinellen Datensätzen vermengt, wenn unter anderem auch lokale Datensätze des Smart Home einbezogen werden[919]. Die Suchformel[920] trägt also zum Entstehen der rechtlichen Grauzone, einer Melange aus vermögenswerten und nicht-vermögenswerten bzw. persönlichkeitsrechtlichen Rechten und Rechtsgütern, bei. Selbige findet sich prima facie in der Definition des verfassungsrechtlichen Erbrechts wieder, was für eine Lösbarkeit des Problems der Vererblichkeit digitaler Güter sprechen mag. Allerdings wird die prämortale Disponibilität über höchstpersönliche, nicht-vermögenswerte Nachlassgegenstände seit dem Mephisto-Urteil des Bundesgerichtshofes stets infrage gestellt: Nichtvermögenswerte Rechte und Güter, welche höchstpersönlichen Bezug oder Inhalt haben, sind unauflöslich an die Person gebunden und daher unverzichtbar und

916 Auch das Urteil des BGH vom 12.7.2018, Az. III ZR 183/17 zum Übergang eines Facebook-Nutzerkontos bei Tod des Kontoinhabers greift den Begriff lediglich im Rahmen der Unvererblichkeit durch den Verweis auf die rechtswissenschaftliche Literatur auf, siehe Rn. 47 ff.

917 *Deutscher Anwaltverein*, Stellungnahme zum Digitalen Nachlass, Glossar: Digitaler Nachlass. Abweichend und konkreter *Deusch*, ZEV 2014, 2 (2 f) sowie *Uhrenbacher*, Digitales Testament und digitaler Nachlass, S. 160 f.

918 So *Lange*/*Holtwiesche*, ZErb 2016, 125 (125); *Klas*/*Möhrke-Sobolewski*, NJW 2015, 3473 (3473); *Alexander*, K&R 2016, 301 (302); *Ludyga*, ZEV 2018, 1 (1 f); *Herzog*, NJW 2013, 3745 (3745).

919 Diese hinzuzählend *Alexander*, K&R 2016, 301 (302).

920 *Sorge*, MMR 2018, 372 (373).

unveräußerlich.[921] Abspaltbare, generell der Öffentlichkeit bekannte Bestandteile der Persönlichkeit wie der Name oder die äußerliche Gestalt können dagegen kommerziell verwertet werden.[922] Bestehen beispielsweise Markenrechte als vermögenswerte Rechte an den Bestandteilen, so wären diese auch übertragbar.

In der verfassungsrechtlichen Parallelwertung lässt sich erkennen, dass die Erbgarantie in der Position des Erben keinen personellen Ersatz für den Erblasser sieht. Vielmehr tritt der Erbe lediglich zur Erfüllung und Auflösung der zurückbleibenden Rechtsgeschäfte ein; bestimmte, genuine Rechte nimmt der Erblasser „mit ins Grab".[923] Zu differenzieren wäre damit anhand der Disponibilität des Grundrechts. Disponible Grundrechte unterliegen prinzipiell der Vererblichkeit kraft Testament – vorausgesetzt, die disponible (Grund-)Rechtsposition ist nicht Teil eines überindividuellen Guts bzw. eines funktionierenden demokratischen Prozesses oder dient der Integration des Gemeinwesens[924]. Ebenso indisponibel ist die Menschenwürde des Art. 1 Abs. 1 GG.[925] Demgemäß kann der Erbe den Achtungsanspruch und Ehrschutz des Erblassers nur verteidigen, aber nicht wie eine eigene Verletzung geltend machen; er ist keine erbbare Rechtsposition.[926] Bezieht man dies wiederum auf den digitalen Nachlass, so bedarf es auch an dieser Stelle einer Prüfung der Erbmasse auf disponible, vermögenswerte Anteile oder nicht disponible, höchstpersönliche Güter, welche von der Erbmasse auszuschließen wären.

Für diese Prüfung haben sich mit Aufkommen der Thematik *Hoeren*[927] und *Martini*[928] ausgesprochen. Beide begründen dies mit der durch das Grundrecht auf informationelle Selbstbestimmung entstehenden Vor- bzw. Reflexwirkung,

921 BGHZ 50, 133 (137). Hieran anschließend BGH GRUR 2000, 709 (712 ff) – Marlene Dietrich – sowie vgl. BGH NJW 2007, 684 (Rn. 10 ff) – kinski-klaus.de.
922 BGH GRUR 2000, 709 (713).
923 So beispielsweise für das Namensrecht – siehe BGH NJW 2007, 684 (Rn. 8).
924 *Robbers*, JuS 1985, 925 (927 f).
925 Vgl. BVerfGE 88, 203 (252); *Bethge*, Die verfassungsrechtliche Zulässigkeit des Grundrechtsverzichts, S. 38 ff; *Bleckmann*, JZ 1988, 57 (58).
926 Vgl. BGHZ 50, 133 (137).
927 *Hoeren*, NJW 2005, 2113 (2114).
928 *Martini*, JZ 2012, 1145 (1152).

zu Lebzeiten über den Verbleib der Daten verfügen zu können.[929] Zum Schutz des Grundrechtsträgers, insbesondere seines Vertrauens in die Datenverarbeitung, muss vor der Erbschaft treuhänderisch der Inhalt des Kontos geprüft werden. Nur auf diese Weise kann der postmortale Persönlichkeitsschutz gewahrt werden. Der dabei entstandene Terminus der „Infektion"[930] von Nutzerkonten durch höchstpersönliche Inhalte und der Trennungsansatz an sich wurden jedoch überwiegend von der Literatur[931] und letztlich auch durch den Bundesgerichtshof[932] abgelehnt. So führt das Gericht gegen diese Differenzierung die erwähnte Sicht des Gesetzgebers in § 2047 Abs. 2 und § 2373 S. 2 BGB an, welche expressis verbis nicht-vermögenswerte Güter einbezieht.[933] Zudem sind digitale wie analoge Inhalte nach dem BGB Teil der Erbmasse; auf das Trägermedium kommt es nicht an.[934] Würde der die Infektion befürwortenden Ansicht dessen ungeachtet gefolgt werden, ergeben sich kaum zu bewältigende praktische Probleme an der Umsetzung der Überprüfung der Daten, sei es aufgrund der kaum möglichen Einschätzung der Höchstpersönlichkeit oder der personellen Befugnis hierzu.[935] Dieser, nunmehr durch den Bundesgerichtshof geprägten Ansicht, ist zumindest hinsichtlich der Umsetzbarkeit der Prüfung zu folgen. Auch scheint es unmöglich, die Erkennung der Infektion auf den jeweiligen Diensteanbieter, welcher den Account bzw. die digitale Identität des Verstorbenen aufbewahrt, abzuwälzen.[936] Es erscheint mithin fraglich, ob bzw. wie diese diffizile Einschätzung durch eine

929 Anders *Sorge*, MMR 2018, 372 (376), welcher die Reflexwirkung zum Erhalt der Datensouveränität kraft Erbe aufseiten des Erblassers sieht und besagten Reflex aus dem Übergang vermögensrechtlicher Rechtsstellungen schließt. Diese Wenn-Dann-Kopplung vermischt allerdings datenschutzrechtliche bzw. informationelle und vermögens- bzw. eigentumsrechtliche Schutzrichtungen, sodass auch diesbezüglich die obige Schutzgut-Diskussion aufgegriffen werden könnte.

930 So *Deutscher Anwaltverein*, Stellungnahme zum Digitalen Nachlass, S. 24 f. Hierzu auch *Kutscher*, Der digitale Nachlass, S. 105 f.

931 Siehe nur *Uhrenbacher*, Digitales Testament und digitaler Nachlass, S. 157 ff; *Kutscher*, Der digitale Nachlass, S. 113 f; *Leeb*, K&R 2014, 693 (695 f); *Steiner*/*Holzer*, ZEV 2015, 262 (262 f); *Alexander*, K&R 2016, 301 (304 f); *Gomille*, ZUM 2018, 660 (664); *Seidler*, NZFam 2020, 141 (143) – mwN auch BGH MMR 2018, 740 (Rn. 48).

932 BGH MMR 2018, 740 (Rn. 47 ff).

933 *Herzog*, NJW 2013, 3745 (3748).

934 BGH MMR 2018, 740 (Rn. 50).

935 BGH MMR 2018, 740 (Rn. 51).

936 *Alexander*, K&R 2016, 301 (305).

letztwillige Verfügung gelöst werden könnte. Dieser Ansatz wird in der Literatur häufiger genannt, jedoch kaum mit praktischen Erwägungen oder Hinweisen zur Umsetzung bedacht.[937] Die Löschung qua Testament erscheint nur schwer durchsetzbar, wenn ein Notar oder eine andere Vertrauensperson als Testamentsvollstrecker iSd § 2197 BGB unter Nutzung der Zugangsdaten des Erblassers alle digitalen Identitäten eigenhändig löscht[938]. So geht die Weitergabe der Zugangsdaten an Dritte je nach AGB mit einer Vertragsverletzung aufseiten des Nutzers einher.[939] Dabei nützt es nichts, die Zugangsdaten der digitalen Identität iSv personalisierten Zugriffsschranken gegen Übergriffe durch Dritte mit einem „elektronischen Schlüssel" gleichzusetzen.[940] Selbige Problematik entsteht, wenn sich eines „digitalen Bevollmächtigten"[941] bedient wird. Auf diese Weise wird die vom Bundesgerichtshof und der Literatur angeführte Problematik bloß personell verschoben. Bislang nicht diskutiert wurde eine Ernennung des Diensteanbieters der zu löschenden digitalen Identität zum Testamentsvollstrecker gem. § 2197 Abs. 1 BGB. Schließlich können auch juristische Personen als Testamentsvollstrecker fungieren[942] und ein Nebeneinander mehrerer Vollstreckungsbefugter ist qua § 2197 Abs. 1 BGB nicht ausgeschlossen. Das Amt des Testamentsvollstreckers kann jedoch gem. § 2202 Abs. 2 S. 1 BGB abgelehnt werden, was an der Durchsetzbarkeit einer Löschung zweifeln lässt. Zudem würde die Schar an Testamentsvollstreckern mit Blick auf die alltägliche Nutzung digitaler Identitäten den eigentlichen Zweck der Norm ausdünnen. Der Testamentsvollstrecker dient der „fremdnützigen, unparteiischen und sachkundigen Willensvollstreckung"[943] und setzt den mutmaßlichen und/oder ausdrücklichen Willen des Erblassers nach

937 So *Brisch/Müller-ter Jung*, CR 2013, 446 (448); *Willems*, ZfPW 2016, 494 (510 f). Ähnlich auch *Herzog*, NJW 2013, 3745 (3750). Einzig mit Empfehlungen für die Praxis *Steiner/Holzer*, ZEV 2015, 262 (265 ff).

938 Vgl. *Brinkert/Stolze/Heidrich*, ZD 2013, 153 (156); *Martini*, JZ 2012, 1145 (1152).

939 *Alexander*, K&R 2016, 301 (307) unter Verweis auf BGHZ 180, 134 (139 f, Rn. 17 f); vgl. auch die Gegenüberstellung von Facebook, Yahoo! und GMX in *Willems*, ZfPW 2016, 494 (496/497).

940 So *Alexander*, K&R 2016, 301 (303, 305).

941 Hierzu *Steiner/Holzer*, ZEV 2015, 262 (265).

942 *Lange* in: Hau/Poseck, BeckOK BGB, § 2197, Rn. 28. Vgl. auch §§ 2210 S. 3, 2163 Abs. 2 BGB.

943 *Zimmermann* in: Säcker et al., MüKo BGB, Bd. X, Vor § 2197, Rn. 2.

dessen Tod um. Diese, mit entsprechendem Vertrauen aufgeladene Position dient daher weniger der Umsetzung datenschutzrechtlicher Defizite und mehr der Willensmäßigkeit der Umsetzung des Testaments bei potentiellen Erbstreitigkeiten.[944] Wenngleich die Eignung dieses Ansatzes vielmehr einer zivilrechtlichen Diskussion außerhalb dieser Untersuchung bedarf, kann zumindest von der mangelnden Eignung des Ansatzes zur Umsetzung der informationellen Selbstbestimmung über den Tod hinaus ausgegangen werden.

Darüber hinaus ist die datenschutzrechtliche Komponente des digitalen Nachlasses zu betrachten. Sowohl der Bundesgerichtshof[945] als auch die Literatur[946] haben sich damit auseinandergesetzt, ob und wie das Datenschutzrecht, und damit auch die informationelle Selbstbestimmung des Erblassers gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG, mit dem berechtigten Interesse des Erben iSd Art. 14 Abs. 1 S. 1 Alt. 2 GG[947] kollidiert. Zutreffend ist, dass das Datenschutzrecht nach Erwägungsgrund 27 S. 1 DSGVO die Anwendung auf Verstorbene ausschließt.[948] Ebenso schließt das Bundesverfassungsgericht die Anwendbarkeit des Allgemeinen Persönlichkeitsrechts nach dem Tod aus, da es sodann an der Handlungsfähigkeit mangele.[949] Dennoch halten es Stimmen der überwiegenden Ansicht für möglich, die Löschung der Daten des Erblassers problemlos umsetzen zu können.[950] Dabei wird jedoch grundlegend übersehen, dass die dafür notwendigen Anspruchsgrundlagen schon nicht anwendbar sind: Grundsätzlich ergibt sich ein Löschungsanspruch für mit persönlichen – ergo personenbezogenen – digitalen

944 Ähnlich kritisch *Deusch*, ZEV 2014, 2 (7).
945 BGH, Urteil vom 12.7.2018, Az. III ZR 183/17, Rn. 64 ff.
946 *Martini*, JZ 2012, 1145 ff sowie *Martini*/*Kienle*, JZ 2019, 235 (237 ff); *Alexander*, K&R 2016, 301 (303 ff); *Gomille*, ZUM 2018, 660 (664 f); *Klas*/*Möhrke-Sobolewski*, NJW 2015, 3473 (3745 f); *Sorge*, MMR 2018, 372 (375).
947 Vgl. BGH, Urteil vom 12.7.2018, Az. III ZR 183/17, Rn. 77 f; *Gomille*, ZUM 2018, 660 (666).
948 So auch BGH, Urteil vom 12.7.2018, Az. III ZR 183/17, Rn. 67.
949 BVerfGE 30, 173 (194); Beschluss vom 25.2.1993, Az. 1 BvR 151/93 = NJW 1993, 1462 – Heinrich Böll; Beschluss vom 25.8.2000, Az. 1 BvR 1168/04 = NJW 2001, 594 f – Willy Brandt; Beschluss vom 5.4.2001, Az. 1 BvR 932/94 = NJW 2001, 2957 (2958) – Wahlkampfäußerung der DVU. Vgl. auch *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 31; *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2 I, Rn. 226.
950 *Steiner*/*Holzer*, ZEV 2015, 262 (265).

Identitäten aus Art. 17 Abs. 1 DSGVO. Diese Anspruchsgrundlage entfällt jedoch aufgrund des Erwägungsgrundes 27 S. 1 DSGVO, auch wenn dieser nur eine Auslegungshilfe darstellt. Überdies ist das Datenschutzrecht aus Sicht des Erben unanwendbar, da dieser in der datenschutzrechtlichen Terminologie nicht Anspruchsberechtigter bzw. Betroffener iSd Art. 4 Nr. 1 DSGVO ist.[951] Wenn das Datenschutzrecht also entfällt, ist zumindest auf zivilrechtliche Generalklauseln zurückzugreifen. Soweit kein Anspruch aus § 37 Abs. 1 S. 1 KunstUrhG oder § 98 Abs. 1 UrhG im Falle eines Bildes vorrangig ist, bietet sich ein Anspruch aus §§ 1004 Abs. 1 S. 1 analog, 823 Abs. 1 BGB iVm Art. 2 Abs. 1 iVm 1 Abs. 1 GG an. Danach könnte die Löschung des Accounts durch einen Anspruch auf Untersagung der weiteren oder Beseitigung der störenden – da grundrechtsbelastenden – Datenverarbeitung erreicht werden. Wohingegen es an der sachlichen Einordnung des Löschungsanspruchs in Art. 2 Abs. 1 iVm 1 Abs. 1 GG nicht scheitern mag[952], ist jedoch konsequent zum oben ausgeführten auch hier die personelle Anwendbarkeit des Art. 2 Abs. 1 iVm 1 Abs. 1 GG ausgeschlossen. Folglich kann mit dieser Argumentation höchstens vonseiten der Angehörigen auch abseits der Erbenstellung die Verunglimpfung des postmortalen Persönlichkeitsrechts des Erblassers geltend gemacht werden. Diese greift jedoch nur ein, wenn die Beeinträchtigung des Achtungsanspruchs entsprechend öffentlich wahrnehmbar ist, die Herabwürdigung sich also in der Öffentlichkeit ergibt.[953] Hierüber geben allerdings weder der Bundesgerichtshof noch die Literatur Aufschluss über die Durchsetzbarkeit dieser Verpflichtung, die vor dem Hintergrund uneinheitlicher allgemeiner Geschäftsbedingungen zu bezweifeln ist.

In der Gesamtschau kann das Urteil des Bundesgerichtshofes zum digitalen Nachlass hinsichtlich einer digitalen Identität nur mäßig überzeugen, wenn es neue Lebenssachverhalte unter nur unvollständig anwendbare Regelungen subsumiert. Zuletzt sei sich daher eines Vorschlags bemüht, um eine mögliche Richtschnur für den weiteren Diskurs zu bieten.

951 Vgl. *Martini*/*Kienle*, JZ 2019, 235 (237).
952 Hierzu bereits unter D.I.1.b)aa).
953 *Leipold* in: Säcker et al., MüKo BGB, Bd. X, § 1922, Rn. 158. Auch BGHZ 50, 133 (137).

Als besagte Richtschnur lassen sich die bereits dargestellten Werkzeuge hinsichtlich persönlichkeitsrechtlicher Gehalte verwenden: Die Sphärentheorie sowie der Erforderlichkeitsgrundsatz, welche bereits im Datenschutzrecht angewendet werden und nach der hier vertretenen Ansicht des postmortalen Datenschutzes weiterhin Anwendung fänden. Vor dem fließenden Übergang zwischen Öffentlichkeits-, Privats- und Intimsphäre sollten nicht die Inhalte im Einzelnen, sondern die Nutzungsweise von Teilaspekten oder des gesamten Accounts betrachtet werden. Danach bietet es sich zumindest an, die Nutzung eines sozialen Netzwerkes in öffentlich zugängliche Teile mit vermögensrechtlichem Hintergrund (Bilder, Postings, etc.)[954] und private, nur dem Nutzer zugängliche Aspekte (Privatnachrichten, versteckte Angaben, etc.) einzuordnen. Im Erbfall kann dann von Seiten des Diensteanbieters problemlos Zugang zu öffentlich gemachten Informationen gewährt werden, wohingegen auf nächster Stufe die potentiell privaten Daten auf ein erforderliches Maß zu beschränken sind. So muss nicht zwangsläufig den Erben der komplette Datensatz mit Klarnamen freigegeben, sondern könnte auf nicht relevante Aspekte reduziert werden. Darüber hinaus werden durch dieses Vorgehen die Persönlichkeitsrechte Dritter berücksichtigt, die auf die Vertraulichkeit der Kommunikation hinsichtlich des Inhalts und der Empfangsperson iSd Art. 10 Abs. 1 GG vertraut haben. Auf diese Weise wird die Kategorisierung nicht vom eigentlichen Inhalt der Daten abhängig gemacht, sondern von der Typik des (einzelnen) Angebots. Alternativ könnte vor dem Hintergrund beider, eingangs genannter Prämissen ein Konstrukt aus rechtlichen Einwirkungsmöglichkeiten und (verpflichtenden) technischen Minimalanforderungen zur Umsetzung des digitalen Nachlasses geschaffen werden. Beispielsweise könnte eine Anwendung zur Markierung der Datensätze geschaffen werden, um einer Vertrauensposition oder den Erben deren Verwendung und Verbleib mitzuteilen – ähnlich einem „letzten digitalen Willen“. So könnte auch die Einordnung weg vom privatrechtlichen Diensteanbieter und hin zum Datensubjekt und der Datensouveränität bewegt werden.

954 Vgl. BGH GRUR 2000, 709 (712); auch *Lange*/*Holtwiesche*, ZErb 2016, 157 (160 f).

Die eben dargestellten Ansätze sind allerdings ebenso streitbar wie der Zwiespalt zwischen der Lösung des Bundesgerichtshofes und der weiterhin konträren Ansicht. So moniert *Martini* weiterhin die mangelnde Berücksichtigung des Datenschutzrechts in der Entscheidung des Bundesgerichtshofes.[955] Insgesamt ist also festzuhalten, dass der digitale Nachlass sich mit Bestimmtheit in vermögensrechtlicher Hinsicht einordnen lässt. Dagegen sind persönlichkeitsrechtliche Belange digitaler Identitäten wie Nutzeraccounts nur uneinheitlich in die Erbgarantie des Art. 14 Abs. 1 S. 1 Alt. 2 GG oder zumindest in die Reflexwirkung des Grundrechts auf informationelle Selbstbestimmung zu integrieren. Weiter spiegelt sich diese unbefriedigende Lösung in der Diversität von Allgemeinen Geschäftsbedingungen der Diensteanbieter wider[956], die sich letztendlich negativ auf die informationelle Selbstbestimmung des Erblassers auswirkt. Diese unklare Rechtslage sollte allerdings nicht auf die Judikative abgewälzt werden. Vielmehr ist es iSd Rechtsstaatsprinzips des Art. 20 Abs. 2, Abs. 3 GG sowie nach Wesentlichkeitslehre und Untermaßverbot Aufgabe des Gesetzgebers, grundlegende Leitlinien für das digitale Vermächtnis zu entwerfen.[957] Diesen Weg eröffnet schließlich Erwägungsgrund 27 S. 2 DSGVO expressis verbis. Die Umsetzung eines postmortalen „Recht auf Vergessenwerdens“[958] ist prima facie nicht ausgeschlossen, bedenkt man die einstige Regelung des § 4 Abs. 1 S. 2 BlnDSG a.F.[959] und die Erweiterung des Datenschutzrechts auf Verstorbene vor Umsetzung der DSGVO. Möglicherweise könnte sich dann aber die bereits ausgeführte Schutzgut-Debatte[960] ausweiten, sofern die Erbgarantie nicht wie hier vertreten auch informationelle Aspekte in sich trägt. Weiter ist trotz (vorerst) gescheiterten Verhandlungen gespannt auf die ePrivacy-VO zu blicken.[961] Zur Berücksichtigung der prämortalen Reflexwirkung des Grundrechts auf informationelle Selbstbestimmung kann de

955 Siehe *Martini*/*Kienle*, JZ 2019, 235 (237 ff).
956 Vgl. *Alexander*, K&R 2016, 301 (306); *Seidler*, NZFam 2020, 141 (144).
957 So auch *Deutscher Anwaltverein*, Stellungnahme zum Digitalen Nachlass, S. 90; *Deusch*, ZEV 2014, 2 (5).
958 Dies bloß fragend *Alexander*, K&R 2016, 301 (307).
959 § 4 Abs. 1 S. 2 BlnDSG a.F.: „Entsprechendes gilt für Daten über Verstorbene, es sei denn, dass schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.“
960 Siehe hierzu D.I.1.d)aa)(3).
961 Hierzu bereits *Martini*/*Kienle*, JZ 2019, 235 (240 f).

lege lata daher nur in dubio pro libertate gelten; ein uneingeschränkter Zugriff auf die digitale Identität des Erblassers kann nur bei entsprechender letztwilliger Verfügung gewährt werden[962].

cc) Ergebnis In Summe ergibt sich damit für die Garantien des Art. 14 Abs. 1 GG eine nur geringe Anwendbarkeit für digitale Identitäten.

Das Konstrukt des Dateneigentums, das die verknüpften Daten digitaler Identitäten einschließt, wurde in seinen einzelnen intradisziplinären Begriffs- und Lösungsvorschlägen dargestellt und die mangelhafte Anwendbarkeit herausgestellt. Vor diesem Hintergrund konnte sodann dargelegt werden, dass die eigentliche Suche nach einer geeigneten Eigentumsordnung unter Verwendung bestehender Modelle obsolet ist: Ein Dateneigentum widerspricht schon seinem Zweck und Inhalt nach der Eigentumsgarantie des Art. 14 Abs. 1 Alt. 1 GG. Demgemäß erübrigt sich die weitere Diskussion dieser Idee; sie muss auf den Ansatz der Datensouveränität bzw. digitalen Souveränität ausgerichtet werden.

Im Rahmen der Erbgarantie bleibt entgegen der Ansicht des Bundesgerichtshofes die Reflexwirkung des Grundrechts auf informationelle Selbstbestimmung des Erblassers einzubeziehen. Folglich ist entweder eine geeignete technische Lösung zur Regelung des digitalen Nachlasses im Vorhinein zu entwerfen und/oder zu etablieren. Dies stellt insbesondere aufgrund der international und außereuropäisch organisierten Diensteanbieter eine große Herausforderung dar. Andererseits muss sich weiterhin mit den trotz des Urteils fortbestehenden, kollidierenden Interessen auseinandergesetzt werden. Auch wenn eine Differenzierung nach Angebotszweck unter der Prämisse datenschutzrechtlicher Prinzipien nicht einfacher als bisherige Vorschläge erscheint, sollte diese multipolare grundrechtliche Konfliktlage weiterhin rechtswissenschaftlich betrachtet werden.

962 So auch *Brinkert*/*Stolze*/*Heidrich*, ZD 2013, 153 (155); *Martini*, JZ 2012, 1145 (1152) sowie *Martini*/*Kienle*, JZ 2019.

e) Berufsfreiheit, Art. 12 Abs. 1 GG

Zuletzt sei vor dem Hintergrund der Frage nach einem Dateneigentum auch eine gegenläufige These einzubeziehen, die sich jüngst im amerikanischen Raum gebildet hat. Mit der Frage „Should we treat data as labor?" stellten die Autoren des gleichnamigen Papers[963] die Theorie vor, jede Weitergabe von Daten bei der Nutzung von Diensten im Internet oder auch anderen Angeboten mit automatisierter Datenverarbeitung als Arbeit anzusehen. Diese Idee fußt auf der Ansicht, dass die Weitergabe von Daten an Diensteanbieter zur weiteren Datengenerierung von künstlichen Intelligenzen oder anderen Rechenprozessen führt, welche sich ausschließlich zu Gunsten des Diensteanbieters auswirken. Gerade künstliche Intelligenzen im Sinne des Machine Learnings[964] sind darauf angewiesen, auf Basis von (menschlichen) Daten zu Lernen und die Daten dementsprechend zu verarbeiten. Ohne eine Datenzufuhr ist dies nicht möglich. Somit wird die Leistung der künstlichen Intelligenz oder jeder anderen Recheneinheit mit der Datenweitergabe verknüpft, deren gemeinsames Resultat die Arbeitsleistung ist. Der Ansatz ist damit konträr zu der im Bereich des Dateneigentums geführten Diskussion. (Personenbezogene) Daten als Arbeitsleistung anzuerkennen führt – so die Autoren – zum Verbleib des Besitzes der Daten beim Individuum, dem als Anreiz bzw. Gegenleistung auch ein Arbeitslohn gewährt wird. Das Individuum, auch Datenarbeiter genannt, kann so den gegenwärtigen Beruf ablegen und aus der Datenarbeit psychologische (z.B. Selbstbewusstsein, Hingabe) wie finanzielle Gewinne erzielen. Demgegenüber erscheint das Modell von Daten als Vermögen bzw. Eigentum negativ behaftet, verbleibt der Vermögenswert der Daten bei den Diensteanbietern (z.B. durch Weiterverkauf der Daten an Werbetreibende) und ergibt sich mangels eines angemessenen Ausgleichs auch eine Dysbalance zwischen Dateninhaber und Diensteanbieter. Zumindest ist der „kostenlose" Zugang in letzterem Modell nicht als angemessene Gegenleistung zu werten.

963 Siehe im Folgenden *Ibara* et al., Should We Treat Data as Labor.
964 Zum Begriff siehe Kapitel B.IV.1. sowie ausführlich *Herberger*, NJW 2018, 2825 (2825 ff).

Die Diskussion ist untrennbar mit der Figur der digitalen Identität verknüpft. Um als Datenarbeiter die Arbeitsleistung zu erbringen und eine angemessene Gegenleistung zu erhalten bedarf es – so auch das Paper[965] – einer allumfassenden Datenerhebung über die analoge Identität, sodass die erhobenen Daten möglicherweise auch der digitalen Gesamtidentität entsprechen. Insofern bliebe zu überprüfen, ob der gemeinsame Verarbeitungsvorgang von Mensch und Maschine als Beruf im Sinne des Art. 12 Abs. 1 GG angesehen werden kann.

Unter dem Beruf des Art. 12 Abs. 1 GG ist nach gefestigter Auffassung in Rechtsprechung[966] und Literatur[967] jede auf Dauer angelegte Tätigkeit zur Schaffung und Erhaltung einer Lebensgrundlage zu verstehen. Auf ein Erlaubtsein des Berufes kommt es nicht an.[968] Mithin ist der Begriff des Berufes weit auszulegen, um einen möglichst weiten Schutz zu garantieren[969] und auch moderne Berufsbilder zu umfassen. So kommt es nicht auf die Schwere oder den aktiven/passiven Charakter der Arbeit an, weshalb auch „Fernsehen“ oder „Musik hören“ als Arbeit angesehen werden könnten. Insofern besteht für den Grundrechtsträger ein „Berufserfindungsrecht“.[970] Im Gegensatz dazu ist der reine Müßiggang allerdings von der Handlungsfreiheit des Art. 2 Abs. 1 GG geschützt; es fehlt hierbei schon an einer Entlohnung.[971] Prinzipiell würde die Datenarbeit nach dem dargelegten Modell auf die Schaffung und Erhaltung einer Lebensgrundlage gerichtet sein, soll doch das aktuell bestehende Nebeneinander von Berufstätigkeit und Nutzung „kostenloser“ Angebote aufgelöst werden. Allerdings würde auch das Nebeneinander eine Eröffnung des Schutzbereichs in diesem Punkt nicht hindern, da auch

965 *Ibara* et al., Should We Treat Data as Labor, S. 3.
966 BVerfGE 7, 377 (379); 102, 197 (212); 105, 252 (265); 111 10 (28).
967 Siehe nur *Mann* in: Sachs, GG, Art. 12, Rn. 43 ff; *Kloepfer*, VerfR II, § 70, Rn. 23 ff.
968 Siehe nur BVerfGE 115, 276 (300 f). Ausführlich *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 56.
969 BVerfGE 14, 19 (22); 68, 272 (281).
970 *Stern*, StaatsR IV/1, S. 1788; *Scholz* in: Maunz/Dürig, GG-Kommentar, Art. 12, Rn. 276; *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 57.
971 Vgl. *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 8. Dennoch kann nicht ausgeschlossen werden, dass auch mit Müßiggang im Wortsinn ein Beruf ausgeübt werden kann, beispielsweise als Kurs in Geh-Meditation.

Neben- und Zweitberufe als solche unter den Begriff fallen[972]. Weiterhin spricht für die Idee der Datenarbeit, dass durch die Berufsausübung iSd Art. 12 Abs. 1 GG stets auch die Fähigkeit des Menschen gefördert wird, die Voraussetzungen für eine individuelle wie gesamtgesellschaftliche Reputation zu schaffen[973]. Zudem erscheint das neue Berufsbild nicht sozialschädlich. Der Öffnung der Berufsfreiheit für die Datenarbeit steht demnach nichts entgegen.

Der somit eröffnete Schutzbereich der Berufsfreiheit ist umfangreich definiert. Nicht nur die dem Wortlaut des Art. 12 Abs. 1 GG entnehmbaren Kategorien von Beruf und Arbeitsplatz sind umfasst, also sowohl die Organisationsform als auch die eigentliche Grundform des grundrechtlich geschützten Handelns[974]. Weiter sind auch die freie Wahl des Arbeitsplatzes, die Arbeitskraft und ihr Aufrechterhalten, Arbeitsmittel und ihre Nutzung sowie das Recht auf einen angemessenen Arbeitsertrag Teil des Art. 12 Abs. 1 GG.[975] Betreffend die Vorstellung des Datenarbeiters, ergibt sich ein Schutz sowohl der gerechten Entlohnung (insbesondere unter Einbeziehung des Art. 1 Abs. 1 GG[976]) als auch ein Schutz der „digitalen Arbeitskraft". Gleichwohl die Digitalisierung das traditionelle Berufsbild ändert, so ändert sich nicht die für Art. 12 Abs. 1 GG typisch-ökonomische Konstellation tendenziell schwächeren Arbeitnehmer und dem aus seiner Machtposition gewährenden Arbeitgeber. Auf diese Konstellation wird sogleich noch vertiefter einzugehen sein.

Zuvor ist es allerdings unvermeidlich, die Beschränkung der Berufsfreiheit beim vorliegenden Konstrukt näher herauszubilden. In der Konsequenz tangiert die Tätigkeit eines Datenarbeiters bei Einspeisung und Anreicherung personenbezogener Daten das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Fraglich ist daher, ob sich das Berufsbild auf Schrankenebene auch in die Verfassungsordnung einpassen lässt. Die Berufsfreiheit ist expressis

972 BVerfGE 110, 141 (156 f).
973 So *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 3.
974 *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 7.
975 *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 7 ff, 54 ff; *Kloepfer*, VerfR II, § 70, Rn. 32 f, 40 f.
976 Vgl. BVerfGE 137, 34; *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 13.

verbis nicht schrankenlos gewährt, da Art. 12 Abs. 1 S. 2 GG auf die Beschränkung durch oder aufgrund eines Gesetzes hinweist. Überdies können aber auch verfassungsimmanente Schranken gelten. Dazu bedarf es allerdings eines „aktivierenden" Gesetzes, welches dem Schutz eines verfassungsrechtlichen Rechtsguts dient.[977] Nicht fern liegt im Falle der digitalen Identität das nationale wie unionsrechtliche Datenschutzrecht, das vorwiegend die informationelle Selbstbestimmung schützt – vgl. Art. 1 Abs. 1 DSGVO. Die typischen Anforderungen an Schranken bzw. Eingriffe in die Berufsfreiheit überschauend bleibt hinsichtlich der Schranken eine Einordnung des Eingriffs durch aktivierende Gesetze zu prüfen, um den Prüfungsmaßstab für die weitere Betrachtung zu ermitteln. Diesbezüglich ist festzustellen, dass es sich bei den Regelungen zum Datenschutz höchstens mittelbar um Normen mit einer berufsregelnden Tendenz handelt. Beispielsweise nimmt der Datenschutz durch Vorgaben zur Minimalisierung der Datensammlung entsprechend Einfluss und begrenzt die Verwertbarkeit der abgebildeten digitalen Identität. Es dürfen auch im datenbasierenden Beschäftigungsverhältnis gem. Art. 88 Abs. 1 DSGVO iVm § 26 Abs. 1 S. 1 BDSG nur jene Daten verarbeitet werden, die für die Tätigkeit erforderlich sind. Nicht erforderlich sind einzelne Daten der digitalen Identität so lange, wie sie nicht für die Verarbeitung durch die künstliche Intelligenz und deren voraussichtlichen Einsatzzweck nötig sind; das Vorhalten von Daten darüber hinaus entfällt.[978] Dementsprechend nimmt das Datenschutzrecht nur beiläufig Einfluss auf das zu untersuchende Berufsbild, wenn es nur mittelbar die Regelung einzelner Vorgaben an das Berufsbild bestimmt. Im Vordergrund des Datenschutzrechts steht die Verfügungshoheit über die den Datenarbeiter selbst betreffenden Daten, unabhängig seines Berufes. Insofern ist von einer objektiv berufsregelnden Tendenz auszugehen.[979] Für die weitere Prüfung

977 *Ruffert* in: Epping/Hillgruber, BeckOK GG, Art. 12, Rn. 84 unter Verweis auf BVerwGE 87, 37 (45); *Kloepfer*, VerfR II, § 70, Rn. 74.

978 Schon dies widerspricht dem Konzept von *Ibara* et al., wo das Herrschaftsrecht bzw. „Eigentumsrecht" an Daten beim Identitätsinhaber verbleiben soll. Dies wäre dann nicht möglicherweise mehr gewährleistet, wenn die Daten über den Verarbeitungsprozess hinaus gespeichert würden. Sicherer und zweckmäßiger erscheint es, die künstliche Intelligenz erneut bei jedem Arbeitsvorgang mit den Daten zu speisen.

979 Zum Begriff siehe *Ruffert* in: Epping/Hillgruber, BeckOK GG, Art. 12, Rn. 55 mwN; *Kloepfer*, VerfR II, § 70, Rn. 57.

dürften Regularien, die den Umgang mit den eigenen Daten auch im Beschäftigtenkontext betreffen, lediglich als Regelungen zur Berufsausübung im Rahmen der Drei-Stufen-Theorie zu qualifizieren sein. Für eine Rechtfertigung reichen sodann vernünftige Erwägungen des Gemeinwohls aus.[980]

Vor diesem Hintergrund ist zu diskutieren, inwiefern die freie Berufswahl und -ausübung des Datenarbeiters zum Schutz seiner digitalen Identität eingeschränkt werden kann. Wie soeben eingeführt, konfligiert hier die Berufsfreiheit mit dem Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Spezifische Kollisionen könnten sich beispielsweise dann ergeben, wenn die Wertigkeit der digitalen Identität bzw. eingespeister Daten mit einer stark schwankenden Entlohnung einhergeht oder gar die Qualität der Daten in Abhängigkeit zur Person steht. Auch einer Diskrminierung aufgrund verschiedener Sexualität oder Gesundheitsgrade ist (gedanklich) keine Grenzen gesetzt. In diesen Fällen durchwirkt allerdings der Gleichheitsgrundsatz des Art. 3 Abs. 1 GG bzw. Art. 21 Abs. 1 GrC mit seinem Diskriminierungsverbot etwaige zivilrechtliche Verträge im Rahmen der mittelbaren Drittwirkung. Möglicherweise könnte dieses Risiko beim Berufsbild der Datenarbeit auch die Schutzpflicht des Gesetzgebers auslösen, wenn bestehende Gesetze – insbesondere Art. 22 DSGVO – ihre Wirkung verfehlen. Den Beschäftigungskontext betreffend ist der Gesetzgeber ohnehin nach Art. 88 Abs. 1 DSGVO zur Regelung des Beschäftigtendatenschutzes angehalten. Aber auch in dieser Hinsicht bestehen Bedenken bei der Gewährleistung einiger datenschutzrechtlicher Prinzipien: Die Ansammlung der Daten in einem für die Theorie von *Ibara* et al. erdachten Modell widerspricht grundlegend dem Gedanken der Datenminimierung gem. Art. 5 Abs. 1 lit. c sowie der Speicherbegrenzung iSe Erforderlichkeit gem. Art. 5 Abs. 1 lit. e DSGVO, wobei beide im Licht des (Unions-)Grundrechts der informationellen Selbstbestimmung zu lesen sind bzw. diesem dienen. Ebenso finden sich diese Prinzipien in deren Schutzgehalt.[981]

Gewichtige Zweifel an einer einfachen Umsetzung des Berufsbildes lassen sich zudem hinsichtlich einer rechtskonformen Einwilligung in die Datenverarbeitung

980 Siehe BVerfGE 7, 377 (405).
981 Siehe D.I.1.b)aa).

finden. Die Verarbeitungsgrundlage der Datenarbeit dürfte regelmäßig der Arbeitsvertrag sein, der sich Art. 6 Abs. 1 lit. b DSGVO zuordnen ließe. Jede weitere, auch nur vorübergehend über den Vertragstypus hinausgehende Verarbeitung bedürfe der Einwilligung. Dies ist auch dann der Fall, wenn zum Zeitpunkt der Einstellung nicht bekannt ist, für welche Verarbeitungs- und Analysezwecke die Informationen des Datenarbeiters verwendet werden sollen. Sodann ist zu überprüfen, ob und wie eine Datenarbeit auf Grundlage einer Einwilligung die dahingehende Berufsfreiheit beschränkt.

Grundsätzlich – sowohl nach dem durch die Rechtsprechung des Bundesverfassungsgerichts geprägten Selbstbestimmungsrechts[982] als auch die datenschutzrechtliche Konkretisierung[983] – setzt eine Einwilligung eine informierte und freiwillige positive Willensbekundung voraus. Zur Umsetzung der Anforderungen dient insbesondere die Pflicht zur Transparenz über den Verwendungszweck und die einzelnen Verarbeitungsvorgänge.[984] Daraus resultiert jedoch, dass der Datenarbeiter nicht zur Abgabe der digitalen Identität an seinen Arbeitgeber durch Anreize oder andere Mittel mit Zwangswirkung genötigt wird. So könnte sich an eine sukzessive Abgabe der Daten denken lassen, die mit steigender Bezahlung oder einmaligen Boni vergütet wird. In einem solchen Fall ist möglicherweise die bis zuletzt strittige Lesart und Anwendung des sog. Kopplungsverbots bei Einwilligungen (Art. 7 Abs. 4 DSGVO) einzubeziehen, die sich mit der Verknüpfung der Weitergabe von Daten über den Vertragsgegenstand hinaus[985] mit einer „Entlohnung“ – z.B. einem kostenfreien Angebot – auseinandersetzt.

Exemplarisch sei daher die Situation der Datenarbeit derart ausgestaltet, als dass ein Basis-Arbeitsvertrag dazu dient, weitere und über den Verarbeitungszweck

982 In Ansätzen BVerfGE 65, 1 (42 f): „Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten.“

983 Siehe Art. 4 Nr. 11, 7 sowie ErwGr 32, 42 DSGVO.

984 Zu dem Merkmalen der Einwilligung siehe bereits D.I.1.b)bb)(3).

985 Zum umgrenzten Anwendungsfall des Kopplungsverbots siehe *Engeler*, ZD 2018, 55 (57 f).

des Basis-Arbeitsvertrags hinausgehende Aufträge auf Einwilligungsbasis abzusichern. In Ansehung des sog. Kopplungsverbots des Art. 7 Abs. 4 DSGVO ist insbesondere dann von einer freiwillig erteilten Einwilligung der einzelnen Aufträge auszugehen, wenn die Erbringung einer Dienstleistung oder die Erfüllung eines Vertrages unter Würdigung des Gesamtkontexts nicht von einer zusätzlichen Einwilligung abhängig ist. Mit anderen Worten: Die Einwilligung darf nicht zu einer „Take it or leave it"-Situation führen.[986] Dies ist insbesondere der Fall, wenn „zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht"[987]. Dies ebenfalls für das Verhältnis zwischen (Daten-)Arbeitgeber und (Daten-)Arbeitnehmer anzunehmen erscheint nicht abwegig. Schließlich prägt ein solches Missverhältnis auch die grundrechtliche Stärkung des Arbeitnehmers durch Art. 12 Abs. 1 sowie 9 Abs. 3 GG.[988] Allerdings spricht der Wandel des Unionsgesetzgebers gegen ein solches Verständnis, da dieser sich gegen eine ausdrückliche Aufnahme in die Erläuterungen zur Freiwilligkeit in Erwägungsgrund 43 der DSGVO entschloss[989]. Stattdessen verweist die Öffnungsklausel des Art. 88 DSGVO auf § 26 BDSG, der in Abs. 2 spezifische Vorgaben zur Freiwilligkeit der Einwilligung ähnlich zum Kopplungsverbot enthält. Diese ist insofern erforderlich, da sich die Auslegungsgrundsätze des Art. 7 Abs. 4 DSGVO von einseitigen Einwilligungen nicht auf mehrseitige Rechtsgeschäfte wie Verträge übertragen lassen.[990] Verfolgt man den utopischen Ansatz nach *Ibara* et al. stringent, basiert die Verarbeitung wohl auf Arbeitsverträgen und ist damit Gegenstand des Beschäftigtendatenschutzes. Auf nationaler Ebene ist im Rahmen des § 26 BDSG anzunehmen, dass es sich bei den Akteuren im diskutierten Modell unproblematisch um Beschäftigte des § 26 Abs. 8 BDSG

986 *Klement* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 7, Rn. 56; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 107 f; *Buchner*, DuD 2016, 155 (158). Vgl. ErwGr 43 S. 2 DSGVO; *Bräutigam*, MMR 2012, 635 (640); *Krüger*, ZRP 2016, 190 (191).

987 ErwGr 43 S. 1 DSGVO.

988 Vgl. *Scholz* in: Maunz/Dürig, GG-Kommentar, Art. 12, Rn. 91 f; *Cornils* in: Epping/Hillgruber, BeckOK GG, Art. 9, Rn. 38.

989 *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7, Rn. 77.

990 *Engeler*, ZD 2018, 55 (58 f).

handelt und § 26 Abs. 1, Abs. 2 BDSG Anwendung findet. Damit dürfen personenbezogene Daten, also auch Daten der digitalen Identität, für die Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Begründung eines Beschäftigungsverhältnisses oder nach Begründung für dessen Durchführung erforderlich ist. Erfolgt die Verarbeitung auf Basis einer Einwilligung, treten weitere Prüfpflichten hinsichtlich eines Abhängigkeitsverhältnisses hinzu (§ 26 Abs. 2 S. 1, 2 BDSG). Im Falle der beschriebenen Datenarbeit sind diese unumgänglich. Im Zuge der jeweiligen Erforderlichkeitsprüfung sind allerdings die datenschutzrechtlichen Grundprinzipien iSd Art. 5 DSGVO einzubeziehen, sodass dennoch die o.g. Maßstäbe der Datenminimierung und Speicherbegrenzung zu beachten sind. Daher sind die digitalen Identitäten der Datenarbeiter nach Möglichkeit nicht als Gesamtidentitäten anzulegen, sondern zweckgebunden (vgl. Art. 5 Abs. 1 lit. b DSGVO) und nur mit den notwendigen Daten vorzuhalten. Hierüber ist der Beschäftigte entsprechend zu informieren, vgl. Art. 12 Abs. 1, 13 DSGVO. Erfolgt die Verarbeitung personenbezogener Daten im Rahmen der Beschäftigung hingegen qua Einwilligung, so sind die Maßstäbe des § 26 Abs. 1, Abs. 2 BDSG anzuwenden. Das Ungleichgewicht zwischen Arbeitgeber und Arbeitnehmer, das gerade durch die finanzielle wie rechtliche Bindung entsteht, wird allerdings ausdrücklich gem. § 26 Abs. 2 S. 2 BDSG ausgeschlossen. Damit wirkt es sich nicht negativ auf die Prüfung der Freiwilligkeit einer Einwilligung nach § 26 Abs. 2 S. 1 BDSG aus. In der Gesamtschau erscheint die Erhebung der digitalen Identität als Basis des Beschäftigungsverhältnisses wider Erwarten datenschutzkonform möglich, wenn die auftragsbezogene Einwilligung zur Erfüllung des Beschäftigungsverhältnisses erfolgt und die übrigen datenschutzrechtlichen Vorgaben hinreichend berücksichtigt werden.

Aus der vorangehenden Erläuterung ergibt sich auf Basis der einfachgesetzlichen Ausgestaltung der informationellen Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG eine Kollisionslage mit der Berufsfreiheit des Art. 12 Abs. 1 GG. Diese ist insbesondere auf das Machtgefälle zwischen Arbeitgeber und Arbeitnehmer zurückzuführen, das sich so verfassungsrechtlich widerspiegelt. Entgegen der sonst hohen Gewichtung des Datenschutzes als persönlichkeitsrechtliches Interesse gegenüber unternehmerischen Freiheiten wie Art. 12 Abs. 1 GG lässt

sich die eingangs dargestellte Theorie von *Ibara* et al. wohl mit geltenden verfassungsrechtlichen Grundsätzen vereinbaren. Gerade die freie Betätigung und grundrechtlich geschützte Privatautonomie des Individuums[991], mit seinen Daten frei verfügen[992] sowie auch ihren Wert als Tauschware oder „in barer Münze" nutzen zu können, unterstützt diese These. Der Staat darf (und kann) trotz seiner Beschützerfunktion im Rahmen der Schutzpflichtenerfüllung nicht jegliche Gefährdung des Grundrechtsträgers ausschließen. Vor diesem liberalen Gedanken verschließt sich der europäische Gesetzgeber nicht, wie auch der Entwurf der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte in Art. 3 Abs. 1 sowie Erwägungsgrund 13 andeuten.[993] Trotzdem ist auch in diesen Fällen auf privatrechtlicher Ebene das Verfassungsrecht im Wege von Generalklauseln zu berücksichtigen, sodass sich die Datenarbeit einer Ausbeutung durch „digitalen Sell-Out" verschließt. Dies würde nicht nur das Grundrecht auf informationelle Selbstbestimmung ad absurdum führen, sondern auch dem Grundsatz der Menschenwürde widersprechen.[994] Darüber hinaus wird die Selbstbestimmung des Datenarbeiters durch die des Arbeitgebers als ebenso privater Akteur begrenzt; ein Unterwerfen widerstrebt der Privatautonomie.[995] Ansätzen der Diskriminierung von Daten und Arbeitnehmern oder der zwanghaften Abgabe einer Einwilligung, ohne dass dies für das Beschäftigungsverhältnis erforderlich ist, ist mittels Schutzpflichtenerfüllung entgegenzuwirken. Unter anderem müsste der Gesetzgeber auch die Spezifika des Datenschutzes und Daten in technischer Hinsicht für derartige Arbeitsverhältnisse regeln, um nicht gegen das Untermaßverbot zu verstoßen. So müssten die mangelnde Rivalität und Exklusivität der Daten ebenso berücksichtigt werden, wobei dies rein technisch kaum überwindbar erscheint und zu entsprechenden Folgeproblemen führen würde. Ohnehin müsste der Gesetzgeber die aus Art. 12 Abs. 1 GG folgende, spezifische

991 *Isensee* in: Isensee/Kirchhof, HStR VII, § 150, Rn. 7, 50 ff, 57 f sowie zu Art. 12 Abs. 1 GG in Rn. 63.

992 Vgl. *Jandt* in: Jandt/Steidle, Datenschutz im Internet, B.II., Rn. 27.

993 Der Entwurf der Richtlinie ist abrufbar unter https://ec.europa.eu/transparency/regdoc/rep/1/2015/DE/1-2015-634-DE-F1-1.PDF (Abruf am 13.10.2018).

994 Zur besonderen Rolle der Menschenwürde als Grenze der Datenerhebung siehe *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 34 f.

995 Vgl. *Isensee* in: Isensee/Kirchhof, HStR VII, § 150, Rn. 17, 104.

Variante der Privatautonomie wegen seiner Inhaltsoffenheit ausformen müssen.[996] Die (zurecht) mangelnde Eigentumsordnung würde wenig hierzu beitragen können, insbesondere wenn künstlichen Intelligenzen als nicht entwirrbares Bündel an Datensätzen digitaler Identitäten und automatisierter Entscheidungen erzeugen. Zwar ergibt sich eine Parallele zum Gesamthandseigentum iSe Gesellschaft bürgerlichen Rechts nach § 705 ff BGB, die dann aber in Anbetracht des eigentlich relevanten Schutzguts[997] auszuschließen ist. Geeigneter scheint eine Parallele zur Investitionsleistung des Datenbankschutzrechts gem. § 87a Abs. 1 UrhG.[998] Diese existiert jedoch gerade wegen mangelnder Eigengehalte der Datenbanken für Maschinendaten; kumulierter personenbezogene Daten sind hierüber nicht zu schützen. Andernfalls würden das Investitionsrecht des KI-Programmierers und der Dateninvestoren kollidieren oder gar verschmelzen. Letztere Situation ist von der Rechtswissenschaft bislang ungeklärt. Gleichermaßen ungeklärt bleibt, ob im Rahmen dieser Utopie nicht auch tatsächliche Schranken des Marktes eintreten und es zu einer Übersättigung des Datenmarktes kommt – Daten verlieren plötzlich an Wert, möglicherweise kommt es zu einer Inflation. Diese eher dystopischen Züge wären jedoch eher Gegenstand eigenständiger Forschung und aufgrund ihrer mangelnden Nachweisbarkeit nicht mehr Teil dieser Arbeit.

Zusammenfassend gilt damit ein Schutz der Erstellung der digitalen Identität, sofern sich dieses als Berufsbild abzeichnet und die wiederholende Datenspeisung an sich darunter zu fassen ist. Dabei sind jedoch entsprechende Schranken durch den Gesetzgeber zum Schutz des Grundrechts auf informationelle Selbstbestimmung vorzusehen und datenschutzrechtliche wie verfassungsrechtliche Prinzipien spezifisch zu regeln. Ebenso vertretbar wäre es aber auch, das Aufkommen dieses Berufsbildes nach *Ibara* et al. zu unterbinden und einer Anreizschaffung der „digitalen Ausbeutung“ vorzuwirken. Die Prärogative liegt ganz beim Gesetzgeber. Allerdings nicht geschützt ist jede alltägliche Erstellung einer digitalen Identität,

996 Zum gesetzgeberischen Gestaltungsspielraum dahingehend siehe *Isensee* in: Isensee/Kirchhof, HStR VII, 63, 85 f.

997 Siehe D.I.1.b)aa)(3).

998 Derart *Specht*/*Rohmer*, PinG 2016, 127 (131); ausführlich *Schwartmann*/*Hentsch*, PinG 2016, 117 ff. Diese und weitere Parallelen zum Urheberrecht grundweg ablehnend *Fezer*, Repräsentatives Dateneigentum, S. 32.

beispielsweise zur Nutzung eines Angebots. Diese unterfällt wiederum der Ausübung der informationellen Selbstbestimmung des Art. 2 Abs. 1 iVm 1 Abs. 1 GG.

f) Conclusio für natürliche Personen

Die digitale Identität natürlicher Personen ist in informationeller Hinsicht vorwiegend durch die dahingehend ausgerichteten Grundrechte geschützt, namentlich das Grundrecht auf informationelle Selbstbestimmung und ggf. mittelbar das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Letzteres betrifft indes einen systemgerichteten Schutz und kommt dem informationellen Schutz nur mittelbar zugute. Im Grundrecht der informationellen Selbstbestimmung geht die digitale Identität jedoch vollumfänglich auf, indem sie in all ihren Facetten in Quantität und Qualität sowie Persönlichkeitssphären umfasst ist. Problembehaftet sind dabei die Grenzfälle der Facetten, namentlich anonyme bzw. anonymisierte digitale Identitäten. Diesen ist jedoch als bewusst mangelndes Dasein von personenbezogenen Daten grundrechtlicher Schutz zu gewähren. Die politischen Bestrebungen zur Einrichtung eines Dateneigentums als Anhaltspunkt für die Eigentumsgarantie des Art. 14 Abs. 1 S. 1 Alt. 1 GG können dagegen nicht überzeugen, sowohl hinsichtlich der definitorischen Einordnung als auch bei näherer Betrachtung des eigentlichen Schutzguts. Das durch das Dateneigentum eigentlich forcierte Ziel der digitalen Souveränität wird vielmehr durch die informationelle Selbstbestimmung des Art. 2 Abs. 1 iVm 1 Abs. 1 GG aufgefangen. Letztlich ebenso gewagt ist die Einspeisung von Daten zur Anreicherung einer digitalen Identität zum Zweck der Erwerbstätigkeit in die Berufsfreiheit des Art. 12 Abs. 1 GG. Wenngleich die Berufswahlfreiheit ein Berufserfindungsrecht enthält, so fehlen dennoch spezifische Rahmenregelungen zur Vorbeugung datenschutzrechtlich wie grundrechtlich schwerwiegender Folgen. In dieser Hinsicht bleiben legislative wie gesellschaftliche Prozesse abzuwarten.

Dieses Ergebnis bedeutet allerdings mitnichten, dass die digitale Identität lediglich ihren Schutz aus dem Grundrecht auf informationelle Selbstbestimmung

gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG ableiten kann. Wie dargestellt, finden sich in diesem Grundrecht die grundlegenden und maßgeblichen Parameter für den selbstbestimmten Umgang mit der digitalen Identität im Rahmen des eingangs erläuterten Lebenszyklus[999]. Einzelne, grundrechtsspezifische Handlungen, die analog auch diesem Grundrecht zugeordnet würden, sind dann der jeweiligen digitalen Dimension des Grundrechts zuzuordnen. Das Grundrecht auf informationelle Selbstbestimmung erweist sich somit als Auffanggrundrecht. Insofern sei auf den Überblick der jeweiligen digitalen Dimensionen aller Grundrechte von *Hoffmann* et al. verwiesen, da eine Betrachtung aller möglicher Handlungsvarianten durch digitale Identitäten den inhaltlichen Rahmen dieser Arbeit überschreiten würde.

2. Zur digitalen Identität juristischer Personen iSd Art. 19 Abs. 3 GG

Nach der ausführlichen Betrachtung der digitalen Identität natürlicher Personen und deren grundrechtliche Einordnung bedarf es unter Rekurs auf B.III. ebenfalls einer Einordnung der dargestellten digitalen Unternehmensidentität in das grundrechtliche Gesamtgefüge. Aufgrund der für juristische Personen des Privatrechts vorzunehmenden Einschränkung auf die bloß wesensmäßig anwendbaren Grundrechte iSd Art. 19 Abs. 3 GG beschränkt sich die nachfolgende Betrachtung auf die Berufsfreiheit des Art. 12 Abs. 1 GG, die relevanten Aspekte des Rechts am eingerichteten und ausgeübten Gewerbebetrieb aus Art. 14 Abs. 1 GG sowie Bezüge zu Art. 2 Abs. 1 iVm 1 Abs. 1 GG – also die potentiell geeigneten Grundrechte für einen „zweckgebundenen Schutz des Rufes“[1000].

999 Siehe B.II.2.
1000 *Quante*, Das allgemeine Persönlichkeitsrecht juristischer Personen, S. 102.

a) Zum verfassungsrechtlichen Unternehmenspersönlichkeitsrecht

Insbesondere wegen genannter Bezüge bedarf es vor der tiefergehenden Betrachtung der Darstellung verfassungsrechtlicher Bezüge der (digitalen) Unternehmensidentität bzw. -persönlichkeit. Hierunter ist nach hiesiger Auffassung die intern und extern gelebte, vereinheitlichte Handlungsweise eines Unternehmens zu verstehen, zumeist festgelegt in Leitfäden und ähnlichen zwingenden Vereinbarungen.[1001] Diese leitet sich jedoch bislang aus praktischen wie ökonomischen Erwägungen ab und findet sich in der verfassungsrechtlichen Literatur kaum oder nur oberflächlich: Während die Unternehmenspersönlichkeit als solche selten umfassend besprochen wird, finden sich zumindest Ansätze in der persönlichkeitsrechtlichen Kommentierung des Grundgesetzes[1002]. Ebenso hat sich das Bundesverfassungsgericht bislang nicht hierzu geäußert[1003], sondern die Thematik lediglich partiell gestreift – beispielsweise in Bezug auf Mithöreinrichtungen und das Recht am eigenen Wort aus Art. 2 Abs. 1 GG[1004] oder zum Schutz vor unzulässiger und rufschädigender Information der Öffentlichkeit iRd Art. 12 Abs. 1 GG[1005]. Eine umfängliche Betrachtung jüngeren Datums gelingt *Koreng*, wenn auch das Konstrukt der Unternehmenspersönlichkeit abgelehnt und dazu im Widerspruch eine persönlichkeitsrechtliche Auffangfunktion des Art. 2 Abs. 1 GG gegenüber Art. 12 Abs. 1, 14 Abs. 1 GG angenommen wird.[1006] Letzteres wurde zwar später vom Bundesverfassungsgericht bestätigt, indem Art. 2 Abs. 1

1001 Siehe B.III. mwN.

1002 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 33 f; *Enders* in: Epping/Hillgruber, BeckOK GG, Art. 19, Rn. 40 f; *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 103; *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I GG, Rn. 383 f; *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 39. Ferner auch *Stern*, StaatsR IV/1, S. 246 f; *Kube* in: Isensee/Kirchhof, HStR VII, § 148, Rn. 75.

1003 Siehe nur BVerfG NJW 2010, 3501 (3502, Rn. 25): „Auch der vorliegende Fall gibt keinen Anlass, diese Fragen abschließend zu beantworten." Ebenso offenlassend BVerfG NJW 2001, 502 (505).

1004 BVerfGE 106, 28 (43 f).

1005 Vgl. BVerfGE 105, 252 (265 ff); 148, 40 (50 ff, Rn. 26 ff).

1006 *Koreng*, GRUR 2010, 1065 (1069).

gegenüber Art. 12 Abs. 1 GG in Sachen der Unternehmenspersönlichkeit als subsidiär erklärt wurde.[1007] Zurück bleibt jedoch besagter Widerspruch, trotz einer nicht bestehenden bzw. abzulehnenden Unternehmenspersönlichkeit zumindest vom Allgemeinen Persönlichkeitsrecht abstammende (selbstständige) Teilrechte anzuerkennen – beispielsweise das Namensrecht, das Recht der persönlichen Ehre oder das Recht auf Geheim- und Privatsphäre.[1008] Somit ist man verfassungsrechtlich zumindest prima facie gewillt, für Unternehmen ein unternehmensbezogenes Persönlichkeitsrecht herauszubilden, sei es aus Art. 12 Abs. 1, 14 Abs. 1 oder 2 Abs. 1 GG.

Diese oberflächliche Übereinstimmung der Ansichten in der Literatur kann jedoch nicht ausreichen, um die Thematik des Unternehmenspersönlichkeitsrechts auch in der Tiefe aufzufangen. Die formelhafte Begrenzung auf persönlichkeitsrechtliche Aspekte des Art. 2 Abs. 1 GG muss schon aus definitorischen Gründen um die zivilrechtlichen Stimmen aus Rechtsprechung und Literatur erweitert werden, die das Unternehmenspersönlichkeitsrecht weitaus umfassender im Rahmen des § 823 Abs. 1 BGB betrachten. Anfangs scheint die dogmatische Einordnung des Unternehmenspersönlichkeitsrechts nach Ansicht des BGH unproblematisch. In stetiger Rechtsprechung sind persönlichkeitsrechtliche Ausprägungen bei der Fassung des Schutzbereiches qua Abwägung herausgebildet worden, jedoch beschränkt auf bloßen Funktionsschutz.[1009] Eine genaue, dogmatisch saubere Zuordnung wurde aber kaum vorgenommen, weshalb sie in der (zivilrechtlichen) Literatur fortan diferriert. Einerseits soll das Unternehmenspersönlichkeitsrecht

1007 BVerfGE 148, 40 (63, Rn. 62). Ebenso *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 103. Differenzierend dagegen *Wilms*/*Roth*, JuS 2004, 577 (579).

1008 Neben *Koreng*, GRUR 2010, 1065 (1067 ff, 1069) ebenso *Brauer*, Das Persönlichkeitsrecht der juristischen Person, S. 40, 42 ff. Zu den einzelnen Rechtspositionen unter Befürworten einer Unternehmenspersönlichkeit *Prinz* in: Fezer/Büscher/Obergfell, UWG, S 7, Rn. 93 ff; *von Lilienfeld-Toal*, Das allgemeine Persönlichkeitsrecht juristischer Personen des Zivilrechts, S. 58 ff; *Klippel*, JZ 1988, 625 (631 ff).

1009 BGH NJW 2008, 2110 (2111, Rn. 7 sowie 2112, Rn. 12) – Gen-Milch; BGHZ 166, 84 (111 ff, Rn. 106 ff) – Deutsche Bank AG; NJW 2005, 2766 (2769 f) – Angedrohter Pressebericht; NJW 1994, 1281 (1282) – Jahresabschluss; BGHZ 98, 94 (95 f) – BMW; BGHZ 81, 75 (77 f) – Carrera; BGHZ 78, 24 (25 f) – Medizin-Syndikat I; NJW 1975, 1882 (1884) – Geist von Oberzell.

aus dem (verfassungsrechtlichen) Allgemeinen Persönlichkeitsrecht gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG abgeleitet werden, jedoch – so auch hier – ohne den Menschenwürde-Aspekt des Art. 1 Abs. 1 GG. Damit reduziert sich die Herleitung auf ein Durchwirken des Art. 2 Abs. 1 GG in die Generalklausel des § 823 Abs. 1 GG.[1010] Andererseits wird vorgeschlagen, das Unternehmenspersönlichkeitsrecht aus Wesen und Interessen der juristischen Person[1011], ihrem sozialen Geltungsanspruch als Parallele zu Art. 1 Abs. 1 GG[1012] oder dem „Geist der Gründer"[1013] herzuleiten. Von diesem Standpunkt entfernter wird die Unternehmenspersönlichkeit der Fallgruppe des Rechts am Unternehmen bzw. am eingerichteten und ausgeübten Gewerbebetrieb untergeordnet; es bedürfe keiner weiteren Generalklausel.[1014]

Mithin sind sich die zivilrechtlichen Stimmen über einen positiven Schutz einig, scheitern aber an der dogmatisch nachvollziehbaren Begründung. So ist ungewiss, ob der Schutz eher dem vermögensrechtlichen Standpunkt des Rechts am Unternehmen in seiner Gesamtheit oder dem durch das unternehmerische Handeln in der Öffentlichkeit erzeugte Persönlichkeitsbild zuzurechnen ist. Zudem wird die einwandfreie Einordnung in beiden Disziplinen dadurch erschwert, dass ein Loslösen beider Richtungen voneinander kaum möglich ist. Denklogisch-kausal kann ein Schaden der Unternehmenspersönlichkeit und der Reputation sich auf das Unternehmen in seiner vermögensrechtlichen Gestalt auswirken, und umgekehrt. Dennoch hat der BGH sich dafür entschieden, das unternehmensbezogene Persönlichkeitsrecht als eigenständiges Schutzgut des § 823 Abs. 1 BGB

1010 *Leßmann*, AcP 170 (1970); *Wilms*/*Roth*, JuS 2004, 577 (578). Vgl. auch BVerfGE 95, 220 (242); 106, 28 (43 f).

1011 *Gierke*, Das Wesen der menschlichen Verbände, S. 10 f, 12; *Klippel*, JZ 1988, 625 (629 f): „Verbandspersönlichkeitsrecht"; *Westermann*, Steht der Genossenschaft das „Allgemeine Persönlichkeitsrecht" zu?, S. 345 (352 f): Eigenart als Kulminationspunkt des Menschlichen; *Kraft*, FS Hubmann, S. 201 (217 f).

1012 So *Wronka*, Das Persönlichkeitsrecht juristischer Personen, S. 98, 104 f. Selbigen aus Art. 2 Abs. 1, 12 Abs. 1, 19 Abs. 3 GG folgernd *Ziegelmayer*, GRUR 2012, 761 (762). Lediglich erwähnend *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 103.

1013 *Hubmann*, Persönlichkeitsrecht, S. 333, allerdings differenzierend nach wesensmäßiger Anwendbarkeit.

1014 *Quante*, Das allgemeine Persönlichkeitsrecht juristischer Personen, S. 128 ff; vgl. *Peifer*, Individualität im Zivilrecht, S. 470.

herauszubilden; es steht damit neben dem Recht am Unternehmen bzw. am eingerichteten und ausgeübten Gewerbebetrieb.[1015] Die Abgrenzung der (zivilrechtlichen) Schutzbereiche wird dabei anhand einer Abwägung der konfligierenden Interessen im Einzelfall[1016] vorgenommen, sodass neben jeweiligen Interessen auch objektive Faktoren wie die Rechtsform des Unternehmens einzubeziehen wären[1017]. Ebenso ist das Rangverhältnis der beiden Generalklauseln einzubeziehen; das Unternehmenspersönlichkeitsrecht genießt grundsätzlich Vorrang.[1018] Ein vollständiges Loslösen geschieht folglich nicht auf abstrakter Ebene, sondern ausschließlich kontextbezogen.

Schlussendlich soll es gelingen, die Argumentationsstruktur des Zivilrechts auf die verfassungsrechtlichen Schutzgüter zu übertragen und einen sowohl dogmatisch als auch für die weitere Betrachtung sinnvollen Maßstab zu entwickeln. Dass das zivilrechtliche und verfassungsrechtliche Persönlichkeitsrecht in der Sache zu unterscheiden sind[1019], steht diesem Vorhaben nicht entgegen. In beiden rechtswissenschaftlichen Disziplinen pendelt die materielle Einordnung des Unternehmenspersönlichkeitsrechts zwischen einer vermögensrechtlichen – Art. 14 GG – und persönlichkeitsrechtlichen bzw. privatautonomen – Art. 2 Abs. 1 ohne 1 Abs. 1 GG[1020], nach *Gostomzyk* auch iVm Art. 12 Abs. 1 GG[1021] – Grundlage, die ohnehin durch den BGH fallgruppenspezifisch bestimmt wird. Als erster Schritt muss vor dem Hintergrund der aufgezeigten – und wohl erfolglosen –

1015 BGH NJW 2008, 2110 (2112, Rn. 12).

1016 Vgl. BGH NJW 2008, 2110 (2112, Rn. 12); BGHZ 45, 296 (307); 65, 325 (331); 138, 311 (318); 166, 84 (109); *Wagner* in: Säcker et al., MüKo BGB, Bd. VI, § 823, Rn. 370 f; *Hubmann*, Persönlichkeitsrecht, S. 159 ff.

1017 Zum rechtsformabhängigen Schutzumfang ausführlich *von Lilienfeld-Toal*, Das allgemeine Persönlichkeitsrecht juristischer Personen des Zivilrechts, S. 118 ff.

1018 Hierzu *Prinz* in: Fezer/Büscher/Obergfell, UWG, S 7, Rn. 105.

1019 Siehe nur BVerfGE 34, 269 (280 f) worin die Differenzierung deutlich gemacht wird. Das zivilrechtliche Persönlichkeitsrecht stellt nur eine konkretisierte Form verfassungsgerichtlicher Rechtsprechung dar, die sich durch Generalklauseln anhand von Fallgruppen manifestiert. Ebenso *Murswiek/Rixen* in: Sachs, GG, Art. 2, Rn. 67.

1020 *von Lilienfeld-Toal*, Das allgemeine Persönlichkeitsrecht juristischer Personen des Zivilrechts, S. 132 f; *Korneeva*, Das Persönlichkeitsrecht des Unternehmens, S. 120 f. Zur wirtschaftlichen Handlungsfreiheit siehe nur BVerfG NJW 1994, 1784 (1784).

1021 Siehe *Gostomzyk*, NJW 2008, 2082 (2084); *Ziegelmayer*, GRUR 2012, 761 (762); *Söder* in: Gersdorf/Paal, BeckOK InfoMedienR, § 823 BGB, Rn. 83.

Suche einer dogmatischen Einordnung des Unternehmenspersönlichkeitsrechts von einer absoluten Einordnung abgerückt werden. Hierfür spricht zunächst, dass das Unternehmenspersönlichkeitsrecht zunächst nicht als „Wunderwaffe" dienen soll[1022]. Ziel dieser neuen Ausformung ist genauer, trotz bestehender einfachgesetzlicher Regelungen auch den Schutz des Unternehmens gegenüber neuen Gefahren reflektieren und im Rahmen von (zivilrechtlichen) Generalklauseln abbilden zu können.[1023] Selbige Auffangfunktion ist bereits für natürliche Personen durch die persönlichkeitsrechtliche Rechtsprechung des BGH und letztlich auch des BVerfG etabliert worden. Demgemäß könnte auch die einzelfallbezogene Bestimmung des unternehmensbezogen anzuwendenden Grundrechts ähnlich der Vorgehensweise des BGH angewandt werden. Dazu bedarf es nicht der Abwägung einzelner Grundrechtsgüter im Vorfeld der Schutzbereichsprüfung, sondern vielmehr einer wertenden Gesamtbetrachtung.[1024] Eine ganz ähnliche, rechtsgüterbezogene Betrachtung in Form eines Ausschlussverfahrens wurde durch das Bundesverfassungsgericht stets bei der Prüfung der Grundrechte zum Schutz vor invasiven Datenerhebungen (Stichwort: Online-Durchsuchung) bei der Abstufung von Art. 13 Abs. 1, 10 Abs. 1 sowie 2 Abs. 1 iVm 1 Abs. 1 GG vorgenommen.[1025] Zweitens ist es erforderlich, für den ersten Schritt grundlegend von einer Selbstständigkeit der einzelnen Grundrechte bzw. relevanten persönlichkeitsrechtlichen Ausprägungen des Art. 2 Abs. 1 iVm 1 Abs. 1 GG auszugehen. Wie bereits dargelegt, sind das Grundrecht auf informationelle Selbstbestimmung und das GGVIS als eigenständige Grundrechte zu begreifen.[1026] Vor dem aufgezeigten Hintergrund ist diese Verselbständigung, soweit es sich um ausreichend etablierte Grundrechte handelt, auch auf weitere Aspekte des Art. 2 Abs. 1 iVm 1 Abs. 1 GG auszuweiten.[1027] Auf diese Weise werden mögliche Probleme bei überlappenden

1022 *Gostomzyk*, NJW 2008, 2082 (2084).
1023 Vgl. *Westermann*, Steht der Genossenschaft das „Allgemeine Persönlichkeitsrecht" zu?, S. 345 (345).
1024 Vgl. hierzu ausführlich *Hubmann*, Persönlichkeitsrecht, S. 159 ff.
1025 Siehe BVerfGE 120, 274 (302 ff).
1026 Siehe D.I.1.a).
1027 *Brauer*, Das Persönlichkeitsrecht der juristischen Person, S. 27; vgl. auch *Hubmann*, Persönlichkeitsrecht, S. 173 f, welcher das Allgemeine Persönlichkeitsrecht als „Muttergrundrecht" bezeichnet. Ablehnend dagegen *Koreng*, GRUR 2010, 1065 (1068).

Schutzbereichen vermieden; ein durch Fallgruppen begünstigtes Entstehen von Rangverhältnissen gelingt dogmatisch sauberer. Andernfalls stünde das expressis verbis bloß *allgemeine* Persönlichkeitsrecht mit eigenen Topoi nicht als selbstständiges „Muttergrundrecht", sondern nur als Gefäß für spezifische Fallgruppen zur Anwendung. Mit Blick auf die initiale Rechtsprechung des Bundesverfassungsgerichts zur Sphärentheorie kann dem jedoch nicht zu folgen sein.[1028] Nur so wird auch dem Wesen des *allgemeinen* Persönlichkeitsrechts entsprochen.[1029] Drittens liegt der Grundstein des (zwei- bzw. mehrseitigen) Unternehmenspersönlichkeitsrechts bereits in Art. 2 Abs. 1 GG verankert, weshalb diesem eine Auffangfunktion zukommt. Schließlich schützt er sowohl die zulässigen persönlichkeitsrechtlichen Aspekte für juristische Personen iSd Art. 19 Abs. 3 GG als auch die unabhängig des Persönlichkeitsrechts zu schützende wirtschaftliche Handlungsfreiheit.[1030] Welche Lesart anzuwenden gilt ist schließlich einzelfallbezogen im Rahmen der Schutzbereichsprüfung zu ermitteln.

Im Fortgang sind damit die benannten Grundrechte als Dreiklang zu begreifen, die gemeinsam das Unternehmenspersönlichkeitsrecht sowohl in seiner vermögenswerten als auch informationellen Gestalt abbilden. Dazu werden sie jeweils in ihrer unternehmensbezogenen Schutzrichtung vertieft und in Bezug zur digitalen Identität gesetzt.

b) Berufsfreiheit, Art. 12 GG

Der Berufsfreiheit des Art. 12 Abs. 1 GG kommt schon ihrem Wesen nach für juristische Personen iSd Art. 19 Abs. 3 GG eine fundamentgebende Rolle zu. Ihre wesensmäßige Anwendbarkeit auf unternehmerische Sachverhalte ist nach ganz

1028 BVerfGE 27, 1 (6); 27, 344 (350 ff); 33, 367 (376 f); 49, 286 (298); 54, 148 (153 f mwN); 101, 361 (382); 120, 180 (199).

1029 Hierzu *Brauer*, Das Persönlichkeitsrecht der juristischen Person, S. 27.

1030 Zu diesem Zirkelschluss *Meissner*, Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht, S. 47.

h.M. gegeben[1031], weshalb sich die weitere Betrachtung in der Art und Weise des grundrechtlichen Schutzes erschöpft. Die „Unternehmerfreiheit“[1032] bzw. „Unternehmensfreiheit“[1033] ist damit ebenso weit und offen definiert in Berufswahl und -ausübung. Der Bereich der Berufswahl erscheint jedoch faktisch mangels höchstpersönlichem Charakter[1034] kaum beachtenswert. Einzig die Komponente der Berufswahl könnte als Berufs*feld*wahl verstanden werden. Sodann gilt das schon natürlichen Personen zuerkannte Berufserfindungsrecht[1035] auch korporativ, wenn mit neuen Branchen zugleich neue Berufsbilder erschlossen werden. Die demgemäß im Fokus stehende Berufsausübungsfreiheit ist entsprechend vielgestaltig; sie reicht von der Wahl der Rechtsform eines Unternehmens[1036] über die wirtschaftliche Betätigung und Leitung[1037] bis hin zur Außendarstellung[1038] und dem Geschäfts- und Betriebsgeheimnisschutz[1039]. Sie schützt also „jede Tätigkeit, die mit der Berufsausübung zusammenhängt und dieser dient“[1040], „soweit diese Tätigkeit ihrem Wesen und ihrer Art nach in gleicher Weise von einer juristischen wie von einer natürlichen Person ausgeübt werden kann.“[1041] In Hinblick auf den Lebenszyklus der digitalen Identität einer juristischen Person, welcher

1031 StRspr seit BVerfGE 21, 261 (266), siehe auch 30, 292 (312); 50, 290 (363 f); 65, 196 (210); 74, 129 (148); 95, 173 (181); 105, 262 (265); 106, 275 (298); 115, 205 (229); 134, 204 (222); 135, 90 (109 f); 148, 40 (50 f, Rn. 26 f). *Stern*, StaatsR IV/1, S. 1832 sowie *Stern*, StaatsR III/1, S. 1126 f; *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 49; *Manssen* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 12, Rn. 268; *Mann* in: Sachs, GG, Art. 12, Rn. 37; *Scholz* in: Maunz/Dürig, GG-Kommentar, Art. 12, Rn. 106 aE; *Ruffert* in: Epping/Hillgruber, BeckOK GG, Art. 12, Rn. 38; *Bethge*, Grundrechtsberechtigung juristischer Personen, S. 37.

1032 So BVerfGE 50, 290 (363).

1033 Hierzu *Stern*, StaatsR IV/1, S. 1819 ff.

1034 Vgl. BVerfGE 21, 201 (232).

1035 *Stern*, StaatsR IV/1, S. 1788; *Scholz* in: Maunz/Dürig, GG-Kommentar, Art. 12, Rn. 276; *Schneider* in: Merten/Papier, HGr V, § 113, Rn. 57.

1036 BVerfGE 21, 227 (232).

1037 Vgl. BVerfGE 50, 290 (363).

1038 BVerfGE 85, 97 (104); 85, 248 (256); 94, 372 (389); 105, 252 (266); 106, 181 (192); 112, 255 (262); 148, 40 (50 ff, Rn. 27 f).

1039 Grundlegend BVerfGE 115, 205 (230 ff).

1040 StRspr BVerfGE 85, 248 (256); 94, 372 (389). Als Teilfreiheiten aufschlüsselnd *Mann* in: Sachs, GG, Art. 12, Rn. 79.

1041 StRspr BVerfGE 21, 261 (266); 22, 380 (383); 30, 292 (312); 50, 290 (363); 65, 196 (209 f); 74, 129 (148 f); 105, 252 (265); 148, 40 (50).

ebenso[1042] in der Erschaffung[1043], Ausgestaltung und ggf. Auflösung selbiger besteht, erscheint der Schutzbereich zunächst eröffnet. Seine weite Formulierung schließt auch der Digitalisierung entspringende, neue Betätigungsfelder ein; er ist technologieneutral. Hierfür spricht auch das erwähnte Berufserfindungsrecht. Der Schutz des Art. 12 Abs. 1 GG ist damit per se eröffnet.

Die vollumfängliche, digitale Betrachtung der unternehmerischen Betätigungsfreiheit des Art. 12 Abs. 1 GG lässt entsprechend weite Spielräume, wobei nachfolgend zwei Aspekte en détail zu betrachten sind: Die Außendarstellung sowie das Geheimnisschutzinteresse des Unternehmens.

Der Aspekt der Außendarstellung des Unternehmens ist nach einhelliger Ansicht Teil der Berufsausübungsfreiheit des Art. 12 Abs. 1 GG.[1044] Gemäß der bereits erwähnten Formel der Berufsausübung schließt dies auch jede Tätigkeit ein, die unmittelbar oder mittelbar mit der Außendarstellung zusammenhängt. Einzig im Glykol-Urteil des Bundesverfassungsgerichts tritt die verbraucherbezogene Außendarstellung hervor: „Ein am Markt tätiges Unternehmen setzt sich der Kommunikation und damit auch der Kritik der Qualität seiner Produkte oder seines Verhaltens aus. [...] In den Schutz der Berufsausübungsfreiheit ist nämlich die auf die Förderung des beruflichen Erfolgs eines Unternehmens gerichtete Außendarstellung einschließlich der Werbung für das Unternehmen oder für dessen Produkte eingeschlossen“.[1045] Der weite Schutzumfang der Berufsfreiheit setzt sich folglich auch in diesem Aspekt fort, bezieht also die qua Digitalisierung entstehenden (und entstandenen) Möglichkeiten der Präsentation eines Unternehmens ein. Insofern ist die digitale Identität als Instrument bzw. Parser zwischen der internen Unternehmenskommunikation und der externen Wahrnehmung durch die Öffentlichkeit faktisch als auch in seinen Details umfasst. Dies ist jedoch, wie

1042 Zum Lebenszyklus der digitalen Identität einer natürlichen Person siehe B.II.

1043 Eine Parallele zur Koalitionsfreiheit des Art. 9 Abs. 1 GG findet sich hingegen nicht, da in der Ausdefinierung einer nicht-rechtsfähigen Persönlichkeit schon kein Gründungsakt liegen kann. Darüber hinaus existiert keine geeignete Rechtsform, unter den die Handlung zu subsumieren wäre. Gegenüber Art. 12 Abs. 1 GG ist Art. 9 Abs. 1 GG formaler Natur – so *Baumann*, BB 1997, 2281 (2285).

1044 Siehe Fn. 1038.

1045 BVerfGE 105, 252 (266).

sogleich[1046] erläutert wird, im Kern iSe status positivus bzw. status activus zu begreifen. Als status negativus muss stets zwischen dem materiellen Gehalt (z.B. Reputation) und der bloßen Ausgestaltung der Unternehmenspersönlichkeit differenziert werden. Artikel 12 Abs. 1 GG schützt lediglich letzteres.[1047]

Der Aspekt des verfassungsrechtlichen Schutzes von Betriebs- und Geschäftsgeheimnissen stellt sich dagegen hinsichtlich der grundrechtlichen Verortung diffizil dar: Herrschend ist bis zuletzt die Ansicht, dass derartige Interessen sowohl dem Schutz des Art. 12 Abs. 1 als auch des Art. 14 I GG unterliegen; „[e]in Schutz von Betriebs- und Geschäftsgeheimnissen durch Art. 14 Abs. 1 GG geht jedenfalls nicht weiter als der durch Art. 12 Abs. 1 GG“[1048].[1049] Die Ansicht des BVerwG scheint dagegen zunächst auf einem älteren Urteil des BVerfG[1050] zu fußen, da sie das unternehmerische Geheimhaltungsinteresse stets in der wirtschaftlichen Handlungsfreiheit des Art. 2 Abs. 1 GG verortet.[1051] In Entscheidungen jüngeren Datums hat sich das BVerwG allerdings ebenso der herrschenden Ansicht angeschlossen und geht von einem Schutz durch Art. 12 und 14 GG aus.[1052] Demgegenüber wird in der rechtswissenschaftlichen Literatur vereinzelt der Schutz ausschließlich[1053] oder zumindest schwerpunktmäßig[1054] in der wettbewerblichen Komponente des Art. 12 GG gesucht. Derlei Ansichten übersehen allerdings die Ambivalenz eines Eingriffs in das Geheimhaltungsinteresse des Unternehmens. Gemäß der herrschenden Ansicht ist daher nicht einwandfrei zu entscheiden, ob Art. 12 Abs. 1 oder 14 Abs. 1 GG einschlägig ist, sondern anhand des Eingriffs und

1046 Sub D.I.2.d).
1047 Vgl. BVerfGE 148, 40 (50, Rn. 27; 53, Rn. 34): kein Anspruch auf Sicherung der Reputation.
1048 BVerfGE 115, 205 (248). Vgl. auch Beschl. v. 12.10.1989 – 1 BvR 1347/88; 30, 292 (174).
1049 So auch *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2 I, Rn. 172; *Kloepfer*/*Greve*, NVwZ 2011, 577 (579).
1050 BVerfG, Beschl. v. 12.10.1989 – 1 BvR 1347/88 –, Rn. 27 f nach juris.
1051 BVerwGE 30, 191 (198); 60, 154 (158 f); 65, 167 (174). Mittelbar da auf Schaden an Wettbewerbsposition beschränkend BVerwG, Urt. vom 28.05.2009 – 7 C 18/08 –, Rn. 14 nach juris. Ausführlich hierzu *Stern*, StaatsR IV/1, S. 898 ff.
1052 BVerwG, Beschl. v. 19.1.2009 – 20 F 23/07 –, Rn. 11 nach juris = NVwZ 2009, 1114 (1116); Beschl. v. 8.2.2011 – 20 F 13/10 –, Rn. 16 nach juris; E 150, 383 (Rn. 28); E 151, 341 (Rn. 41).
1053 *Wolff*, NJW 1997, 98 (100 f).
1054 *Stern*, StaatsR IV/1, S. 1822 f.

der Folgen das Grundrechtsgut – wie bereits zum Dreiklang der Unternehmenspersönlichkeit[1055] erläutert – zu ermitteln. Insofern ist die Wettbewerbsfreiheit des Art. 12 Abs. 1 GG (ggf. iVm Art. 3 Abs. 1 GG) iSe aktiven und freien Teilnahme vom vermögenswerten Gehalt eines Betriebs- und Geschäftsgeheimnisses gem. Art. 14 Abs. 1 GG zu unterscheiden.[1056] Dabei soll der offener definierte Schutz der Berufsfreiheit den Schutz des Art. 14 Abs. 1 GG nicht aushöhlen.[1057] Zwangsläufig führt die Kombination beider Grundrechte aber zu einem flexibleren bzw. materiell breiteren Grundrechtsschutz, bei dem sich die Güter des Art. 12 und 14 GG bloß teilweise überdecken. Ein Erweitern dieser zwei Horizonte um die (subsidiäre)[1058] wirtschaftliche Handlungsfreiheit des Art. 2 Abs. 1 GG trägt wohl nur gering zum Schutzumfang bei, stützt beispielsweise iSd Theorie von *Gostomzyk* den Wettbewerbsaspekt des Art. 12 Abs. 1 GG.[1059] In der Summe ergibt sich damit keine andere Position. Vor dem Hintergrund des eingangs dargestellten Trias verfassungsrechtlicher Schutzgüter mit Unternehmensbezug passt sich der mehrseitige Schutz von Betriebs- und Geschäftsgeheimnissen ein.

Nunmehr bleibt die digitale Identität eines Unternehmens in den vorangehend erläuterten Kontext einzuordnen. Obschon die dargelegten Ansichten sich abseits einer Legaldefinition entwickelt haben[1060], ist sich nach der mit dem Geschäftsgeheimnisgesetz (GeschGehG) am 24.4.2019 in Kraft getretenen Definition des Betriebs- und Geschäftsgeheimnisses zu richten. Gemäß § 2 Nr. 1 GeschGehG bedarf es einer ausreichend gesicherten und der Öffentlichkeit unzugänglichen bzw. nur bestimmten Personen zugänglichen Information, an der ein berechtigtes

1055 Sub D.I.2.a).

1056 *Bullinger*, NJW 1978, 2173 (2176); *Wolf*, Der Schutz des Betriebs- und Geschäftsgeheimnisses, S. 126 ff, 82 f. Vgl. auch *Stern*, StaatsR IV/1, S. 1928 f; allgemein postulierend BVerfGE 30, 292 (335).

1057 Vgl. BVerfGE 115, 205 (248).

1058 *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2 I, Rn. 172.

1059 Vgl. *Mann* in: Sachs, GG, Art. 12, Rn. 194 unter Hinweis auf die stetig hilfsweise Anwendung des Art. 2 Abs. 1 ggü. 12 Abs. 1 GG durch das BVerfG mwN in Fn. 611; *Axer*, FS Isensee (2002), S. 121 (121 f).

1060 Zuvor wurde der Geheimnisbegriff im Rahmen der stetigen Rechtsprechung zu § 17 UWG ausdefiniert, siehe nur BGH GRUR 2018, 1161 (Rn. 28) mwN. Im Detail hierzu *Gennen* in: Conrad/Grützmacher, Recht der Daten und Datenbanken im Unternehmen, § 13, Rn. 12 ff.

Interesse an der Geheimhaltung besteht. Die einstige Trennung zwischen dem wissensbezogenen Geschäftsgeheimnis- und dem technik- und produktbezogenen Betriebsgeheimnisbegriff[1061] ist aufgrund ihrer mangelnden Praxisrelevanz aufgelöst worden.[1062] Die gemeinsame, offene und relativ zu bestimmende[1063] Fassung benennt nun auch expressis verbis den fiktiven Wert einer Information; es bedarf („nach wie vor“[1064]) keiner tatsächlichen Wertstellung. Vielmehr entsteht der Wert durch die tatsächliche und durch Vorkehrungen (z.B. Verschwiegenheitsklauseln) gesicherte Geheimhaltung, § 2 Nr. 1 GeschGehG: „daher“.[1065] Insofern indiziert die Auflösung der Geheimhaltung den potentiellen (wirtschaftlichen) Wissensvorsprung eines Mitbewerbers nach Aufdecken des Unternehmensgeheimnisses.[1066] Dies ist mit Blick auf den Schutz der unternehmerischen digitalen Identität insoweit nützlich, als dass auch „belanglose“ unternehmensbezogene Informationen geschützt wären. Das Kriterium des Unternehmensbezugs lässt sich verfassungsrechtlich allenfalls aus dem Kriterium der berufsregelnden Tendenz des Art. 12 Abs. 1 GG folgern[1067], wenn auch selbiges mit Fassung des GeschGehG fallen gelassen wurde.[1068] Der Schutz der Inhalte der digitalen Identität erstreckt sich damit primär ausschließlich auf Interna, beispielsweise geplante Postings oder interne Maßstäbe für die Öffentlichkeitsarbeit und -kommunikation. Diese sind aufgrund ihrer Natur zwar teilöffentlich, was dem Schutz allerdings nicht abträglich ist.[1069] Er erstreckt sich auf strategisch wertvolle Güter für Wettbewerb

1061 BVerfGE 115, 205 (230).
1062 So *Ohly*, GRUR 2019, 441 (442).
1063 *Ohly*, GRUR 2019, 441 (443).
1064 So *Dann*/*Markgraf*, NJW 2019, 1774 (1775).
1065 Ausführlich *Ohly*, GRUR 2019, 441 (443); *Schuster*, CR 2020, 726 (727).
1066 Vgl. *Wolf*, Der Schutz des Betriebs- und Geschäftsgeheimnisses, S. 128 ff.
1067 Vgl. BVerfGE 97, 228 (254): „Art. 12 Abs. 1 GG entfaltet seine Schutzwirkung vielmehr nur gegenüber solchen Normen oder Akten, die sich entweder unmittelbar auf die Berufstätigkeit beziehen oder die zumindest eine objektiv berufsregelnde Tendenz haben.“ – so stRspr E 95, 276 (302); 98, 218 (258). In der Folge erfordert auch die Schutzrichtung einen Unternehmensbezug, um eine Abgrenzung gegenüber anderen Grundrechten (z.B. Art. 5 Abs. 1 S. 2 oder 2 Abs. 1 GG) zu ermöglichen. Vgl. Unternehmensbezug als Abgrenzungskriterium *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2, Rn. 224.
1068 Zum früheren Kriterium siehe *Schnabel*, CR 2016, 342 (343). Zur nunmehr relevanten Problematik der Mischung von persönlichen und unternehmensbezogenen Informationen *Ohly*, GRUR 2019, 441 (443).
1069 Vgl. *Drexl* et al., GRUR Int. 2016, 914 (916 f, insbes. Rn. 25).

(Facette des Art. 12 Abs. 1 GG) und Reputation (Facette des Art. 14 Abs. 1 GG). Diese können bei entsprechender Verwendung wettbewerbs- wie unternehmensschädigend wirken.[1070] Folglich reicht diese Schutzrichtung nur für die „innere" digitale Identität, wobei der genaue Schutzgegenstand kontextbezogen ermittelt werden muss.

Der unternehmensbezogene Schutz der Berufsfreiheit gem. Art. 12 Abs. 1 GG schließt die digitale Identität folglich nur als Mittel der Repräsentation ein, nicht aber in seinem informationellen Gehalt. Ähnlich oberflächlich erweist sich der Schutz im Rahmen von Betriebs- und Geschäftsgeheimnissen über Art. 12 Abs. 1 GG. Persönlichkeitsrechtliche Aspekte der digitalen Identität juristischer Personen finden hingegen kaum bzw. nur mittelbaren Schutz.

c) Der Gewerbebetrieb des Art. 14 Abs. 1 GG

Schon aufgrund seiner Verflechtung mit Art. 12 Abs. 1 GG ist der Schutzbereich des Art. 14 Abs. 1 GG in die Betrachtung einzubeziehen. Im Unternehmenskontext des Art. 19 Abs. 3 GG[1071] nimmt die (bereits dargestellte[1072]) Eigentumsfreiheit wenig Raum ein[1073], sondern weicht dem qua Rechtsprechung ausgeformten Recht am eingerichteten und ausgeübten Gewerbebetrieb. Der eigentliche Gehalt dieses Aspekts einschließlich seiner definitiven Anerkennung als Schutzobjekt des Art. 14 Abs. 1 GG ist jedoch fast ausschließlich durch die zivilrechtliche

1070 BT-Drs. 19/4724, S. 24 unter Verweis auf RL (EU) 2016/943, ErwGr 14. Vgl. auch *Ohly*, GRUR 2019, 441 (443); *Schnabel*, CR 2016, 342 (346); *Kloepfer/Greve*, NVwZ 2011, 577 (579) mwN.

1071 Ganz h.M. – BVerfGE 4, 7 (12, 17); 23, 153 (163); 35, 348 (360); 53, 336 (345); 66, 116 (130); 126, 112 (135 f); 143, 246 (312, Rn. 182). *Leisner* in: Isensee/Kirchhof, HStR VIII, § 173, Rn. 33; *Stern*, StaatsR IV/1, S. 2215 f sowie *Stern*, StaatsR III/1, S. 1127; *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 189; *Wendt* in: Sachs, GG, Art. 14, Rn. 16.

1072 In Bezug auf die digitale Identität natürlicher Personen sub D.I.1.d).

1073 Dies ist ebenso auf den engen isolierten Anwendungsbereich der unternehmerischen Eigentumsgarantie zurückzuführen: Für eine diesbezügliche Prüfung bedürfte es einer eigenständigen Rechtsstellung der Elemente der (unternehmensbezogenen) digitalen Identität. Da es bereits an dieser für natürliche Personen mangelt, lässt sich diese nur schwerlich bei juristischen Personen iSd Art. 19 Abs. 3 GG erkennen. Von einer Prüfung als vermögenswertes Recht des Unternehmens wird daher abgesehen.

Rechtsprechung des BGH erfolgt.[1074] Das BVerfG hält sich, bis auf wenige bestätigende Urteile, bis dato zurück und lässt die Frage offen, „ob – eigentumsrechtlich gesehen – das Unternehmen [nur] eine tatsächliche, nicht aber eine rechtliche Zusammenfassung der zu seinem Vermögen gehörenden Sachen und Rechte ist, die an sich schon vor verfassungsrechtlichen Eingriffen geschützt ist."[1075] Die daher bestehenden, aus dem Wortlaut einiger verfassungsrechtlicher Urteile herausgelesenen Zweifel an der Rechtsfigur[1076] sind an dieser Stelle jedoch nicht zu vertiefen. Stattdessen ist sich den befürwortenden Stimmen des Rechts am eingerichteten und ausgeübten Gewerbebetrieb anzuschließen[1077] respektive auf die Notwendigkeit mit Blick auf den Schutz der Unternehmenspersönlichkeit hinzuweisen[1078]. Das damit in der Eigentumsfreiheit aufgehende und weitreichende[1079] Schutzgut erweitert schließlich den unternehmerischen Eigentumsschutz um tatsächlich bestehende, wertbestimmende Faktoren[1080] – beispielsweise einzelne eigentumsrechtliche Positionen des Betriebs (Grundstücksrechte, Einrichtungsgegenstände, Anlagen, Wahrenvorräte, etc.), den Kundenstamm, Betriebs- und Geschäftsgeheimnisse[1081] oder auch den Ruf des Unternehmens.[1082] Es umfasst

1074 BGHZ 23, 157 (162); 45, 150 (154); 48, 58 (60 f); 133, 265 (267). Darüber hinaus BVerwG 121, 382 (391); 143, 249 (268 f). Umfassend darstellend *Kimminich* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 14, Rn. 77 ff.

1075 So *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 134 unter Verweis auf BVerfGE 51, 193 (221 f); 66, 116 (145); 68, 193 (222 f); 96, 375 (397); 105, 252 (278); 123, 186 (259); 143, 246 (331, Rn. 240). Überdies 84, 212 (323); 87, 363 (394). Nur vgl. E 17, 232 (247 f).

1076 Hierzu im Einzelnen *Kimminich* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 14, Rn. 79 ff; *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 134; *Stern*, StaatsR IV/1, S. 2189 ff; *Koreng*, GRUR 2010, 1065 (1067); *Hagen*, GewArch 2005, 402 (403 f).

1077 *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 134 sowie *Depenheuer* in: Merten/Papier, HGr V, § 111, Rn. 63 f. Wohl auch *Kimminich* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 14 GG, Rn. 79 f.

1078 Siehe hierzu nur *Ziegelmayer*, GRUR 2012, 761 (762 ff).

1079 Hierzu *Kimminich* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 14, Rn. 85.

1080 Vgl. BVerfGE 74, 129 (148); *Friauf/Wendt*, Eigentum am Unternehmen, S. 29.

1081 Ausführlich *Wolf*, Der Schutz des Betriebs- und Geschäftsgeheimnisses, S. 103 f. Ablehnend dagegen *Wolff*, NJW 1997, 98 (100 f).

1082 *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 200; *Hagen*, GewArch 2005, 402 (406 f). Vgl. auch BGHZ 23, 157 (162 ff).

iSe methodischen Gesamtbetrachtung[1083] „alles das, was in seiner Gesamtheit den wirtschaftlichen Wert des konkreten Betriebes ausmacht“[1084] – sowohl funktional als auch organisatorisch[1085]. Der spezifische Mehrwert des Betriebes als organische Betriebseinheit geht über die Summe der ohnehin gewährleisteten Einzelrechte hinaus.[1086] In der Summe reicht er allerdings nicht weiter als der Schutz seiner wirtschaftlichen Grundlagen.[1087]

Eine Subsumtion der digitalen Identität eines Unternehmens bzw. einer juristischen Person gelingt allerdings auch hier nur partiell. Dazu bedarf es allerdings zweier Manifestationen des Eigentumsschutzes, die als Beispiel dienen sollen.

Bezugnehmend auf den Ansatz, das Unternehmen als Funktions- und Organisationseinheit dem Eigentumsbegriff des Art. 14 Abs. 1 GG unterzuordnen, findet sich eine durch die Gesetzgebung konkretisierte Form in §§ 453, 433 BGB – dem Unternehmenskauf.[1088] Hiernach ist der (Ver-)Kauf eines Unternehmens als bestehende Sach- und Rechtsgesamtheit möglich. Dies meint jedoch nicht die bloße Einigung über ein Bündel an Einzelrechten, sondern die vollumfängliche Übertragung von Verfügungs- und Entscheidungsbefugnissen. Ebenso ist „der Verkäufer neben der Übertragung der übertragbaren Gegenstände verpflichtet [...], den Käufer in diesen Komplex von Sachen, Rechten, Pflichten und Immaterialgütern einzuweisen“.[1089] Ein Unternehmenskauf gem. §§ 453, 433 BGB umfasst also auch „Goodwill, Know-how, Geschäftsgeheimnisse, Kundenstamm, Lieferantenbeziehungen, etc.“[1090] und damit jene Güter, denen isoliert nicht zwingend ein

1083 So *Hagen*, GewArch 2005, 402 (407).
1084 BVerfGE 13, 225 (229 f); 45, 142 (173). BGHZ 23, 157 (163); 45, 150 (155).
1085 Vgl. *Axer* in: Epping/Hillgruber, BeckOK GG, Art. 14, Rn. 52 aE sowie *Axer*, FS Isensee (2002), S. 121 (134 f); *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 200 aE.
1086 So *Depenheuer/Froese* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 14, Rn. 133.
1087 BVerfGE 58, 300 (353); 143, 246 (331, Rn. 240).
1088 Eine ähnlich ganzheitliche Betrachtung erfolgt gem. §§ 1 ff und §§ 22 ff HGB – so *Axer*, FS Isensee (2002), S. 121 (135) und *Hagen*, GewArch 2005, 402 (402 f).
1089 *Westermann* in: Säcker et al., MüKo BGB, Bd. IV, § 453 BGB, Rn. 20.
1090 *Faust* in: Hau/Poseck, BeckOK BGB, § 453, Rn. 27; *Axer*, FS Isensee (2002), S. 121 (134 f); *Hagen*, GewArch 2005, 402 (407 f). Vgl. *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 204.

Vermögenswert zukommt.[1091] Gleichermaßen kommt der unternehmensbezogenen digitalen Identität als Unternehmensbestandteil kein eigener Vermögenswert zu. Wie dargestellt, kann dieser aber in Relation mit dem Unternehmen entstehen und wäre im Falle eines Unternehmenskaufes ebenso preisbestimmend[1092]. Der digitalen Identität eines Unternehmens kommt daher nur als Teil der vermögensrechtlichen Gesamtbetrachtung entsprechender Schutz zu, der die einzelnen, unternehmenspersönlichkeitsrechtlichen Aspekte nicht hinreichend würdigt und aufgrund seiner Ausrichtung nicht würdigen kann.[1093]

Im Speziellen könnte dennoch für den Schutz der digitalen Identität als Teil des Unternehmenseigentums die Nutzung als Werbeinstrument sprechen, würde die Rechtsprechung des „Kontakts nach Außen" bloß abstrakt berücksichtigt: Gemäß zivil-[1094] wie verwaltungsgerichtlicher[1095] Rechtsprechung ist auch die Lage eines Unternehmens an der öffentlichen Straße vom Schutzkreis des Art. 14 Abs. 1 GG umfasst. „Dieses Recht schützt vor einem völligen Abschneiden vom öffentlichen Verkehrsraum sowie in gewissem Grade vor anderen ‚Kontakt-Störungen'", beispielsweise das Versagen unternehmensbezogener[1096] Kommunikation mit Passanten wie Werbung durch Lichttransparente oder Hinweis- und Werbeschilder.[1097] Obschon das Internet nicht vom Anlieger- und Gemeingebrauch geprägt ist, könnte sich in der Parallelwertung ebenso das unternehmerische Werberecht

1091 Vgl. *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 206.

1092 Vgl. *Westermann* in: Säcker et al., MüKo BGB, Bd. IV, § 453 BGB, Rn. 20; *Leisner* in: Isensee/Kirchhof, HStR VIII, § 173, Rn. 26.

1093 Ähnlich auch *Ziegelmayer*, GRUR 2012, 761 (763).

1094 BGHZ 45, 150 (157); 57, 359 (361 f).

1095 BVerwG NJW 1975, 357; E 54, 1 (3).

1096 Hierzu sei erwähnt, dass in der zivilgerichtlichen Rechtsprechung stets eines betriebsbezogenen Eingriffes bedarf. Betroffen ist der Gewerbebetrieb als solcher abseits ablösbarer Rechte, als Organismus – BGHZ 29, 65 (74); 193, 227 (Rn. 21); *Prinz* in: Fezer/Büscher/Obergfell, UWG, S 7, Rn. 111; *Hagen*, GewArch 2005, 402 (402). Der Zweck, „diffuse Schadensbilder auszuklammern" – so *Wagner* in: Säcker et al., MüKo BGB, Bd. VI, § 823 BGB, Rn. 369 –, trifft insofern auch auf die Spezifizierung des Grundrechtseingriffs bzw. betroffenen Grundrechtsguts zu. Analog zur Berufsbezogenheit des Eingriffs in Art. 12 Abs. 1 GG ist für Eingriffe in die Unternehmensfreiheit der entsprechende Unternehmensbezug erforderlich. Ähnlich auch BVerfGE 13, 225 (229 f): „[...] so daß grundsätzlich nur ein Eingriff in die Substanz dieser Sach- und Rechtsgesamtheit Art. 14 GG verletzen könnte."

1097 *Papier/Shirvani* in: Maunz/Dürig, GG-Kommentar, Art. 14, Rn. 201 f.

an öffentlich zugänglichen Werbeflächen im digitalen Raum unter das Recht am eingerichteten und ausgeübten Gewerbebetrieb subsumieren lassen. Dafür spricht zumindest, dass in beiden Fällen ein unternehmerisches Interesse vorliegt und ein Verbot dieser Handlungspraxis neben Einschnitten in die unternehmerische Handlungsfreiheit des Art. 12 Abs. 1 GG auch das vermögensbezogene Recht am eingerichteten und ausgeübten Gewerbebetrieb zur Folge hätte. Diesem Aspekt kommt aber vor besagtem Art. 12 Abs. 1 GG sowie dem Hintergrund der möglichen Inhalts- und Schrankenbestimmung nur geringe Aufmerksamkeit zu. Mithin ist die digitale Identität als Mittel der Werbung „am digitalen Wegesrand" nicht eigenständig geschützt, sondern unter Würdigung erwähnter Rechtsprechung höchstens mittelbar. Eingangs aufgezeigte, unternehmenspersönlichkeitsrechtliche Facetten würdigt auch dieser Ansatz unzureichend.

Folglich schützt das Recht am eingerichteten und ausgeübten Gewerbebetrieb des Art. 14 Abs. 1 GG die digitale Identität juristischer Personen trotz seiner weiten Definition nur unzureichend, was nicht auf die Ausgestaltung der entsprechenden Inhalts- und Schrankenbestimmungen zurückzuführen ist. Vielmehr eignet sich das Grundrecht per se nicht zum Schutz von Gütern mit Persönlichkeitsbezug.

d) Grundrechte des Art. 2 Abs. 1 iVm 1 Abs. 1 GG

Hoffnungsvoll sind daher die aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG bzw. im Unternehmenskontext lediglich aus Art. 2 Abs. 1 iVm 19 Abs. 3 GG zu folgernden Einzelrechte in den Blick zu nehmen. Dafür kommen ebensolche Rechte in Betracht, die nicht auf dem Menschenwürdekern des ursprünglichen Persönlichkeitsrechts aufbauen oder sich zumindest partiell ohne selbige Aspekte anwenden lassen.[1098]

1098 BVerfGE 118, 168 (203); vgl. auch 95, 220 (242). Ebenso *Stern*, StaatsR IV/1, S. 247; *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 64; *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2 I, Rn. 47; *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 383; *Enders* in: Epping/Hillgruber, BeckOK GG, Art. 19, Rn. 40; *Enders*, Die Menschenwürde in der Verfassungsordnung, S. 450 f.

Insofern sind das Grundrecht auf informationelle Selbstbestimmung[1099], das Recht am gesprochenen Wort[1100] und am eigenen Namen[1101] sowie eigenen Bild[1102], Aspekte des Ehrschutzes[1103], das GGVIS[1104] sowie das Recht auf Geheim- und Privatsphäre[1105] grundsätzlich relevant. Vorliegend ist in Bezug auf die digitale Identität aber dem Grundrecht auf informationelle Selbstbestimmung sowie dem Reputationsschutz zu nähern, wohingegen die übrigen Schutzrichtungen aufgrund ihrer einzelfallabhängigen Relevanz nicht weiter vertieft werden.

Wie bereits im Rahmen der Berufsfreiheit erläutert, erstreckt sich der Reputationsschutz des Art. 12 Abs. 1 GG überwiegend auf den status activus bzw. positivus: Die Entstehung, Ausgestaltung und Auflösung der unternehmensbezogenen digitalen Identität als Instrument und Teil des Unternehmensrufes.[1106] Dementsprechend bedarf es eines negatorischen grundrechtlichen Schutzes, der sowohl Eingriffe des Staates[1107] als auch in mittelbarer Drittwirkung zwischen

1099 BVerfGE 118, 168 (204); *Tettinger* in: Merten/Papier, HGr II, § 51, Rn. 64; *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 103; *Jarass*, NJW 1989, 857 (860); .

1100 BVerfGE 106, 28 (43 f).

1101 *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 103; *Brauer*, Das Persönlichkeitsrecht der juristischen Person, S. 42 ff auf § 12 BGB analog stützend.

1102 Offen lassend BVerfG NJW 2005, 883.

1103 *Brauer*, Das Persönlichkeitsrecht der juristischen Person, S. 45 ff; *Klippel*, JZ 1988, 625 (631 f); vgl. auch *Prinz* in: Fezer/Büscher/Obergfell, UWG, S 7, Rn. 122. Auch aus den wirtschaftlichen Aspekten der Art. 12 und 14 GG ableitend *Lorenz* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 2 I, Rn. 385; wohl auch *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 103.

1104 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2 GG, Rn. 33; *Drallé*, GGVIS, S. 68 ff.

1105 BVerfGE 118, 168 (205); *Westermann*, Steht der Genossenschaft das „Allgemeine Persönlichkeitsrecht“ zu?, S. 345 (351); *Brauer*, Das Persönlichkeitsrecht der juristischen Person, S. 59 f; *Klippel*, JZ 1988, 625 (632); *Meissner*, Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht, S. 83.

1106 Sub D.I.2.b).

1107 Vgl. BVerfGE 105, 252 (265 f); 105, 279 (303 f); 148, 40 (51 f, Rn. 28 ff).

Wettbewerbsteilnehmern[1108] gilt. Zwar findet sich dies partiell bei ausreichender Gefährdung des Unternehmens in Art. 14 Abs. 1 GG[1109] sowie bei Einschränkung der Berufsausübung in Art. 12 Abs. 1 GG[1110], jedoch fangen diese nur Extreme auf und bieten daher kaum effektiven Schutz. Schon deshalb bietet es sich an, diesen Schutz im subsidiären[1111] Unternehmensrecht des Art. 2 Abs. 1 GG zu verankern. Dennoch müssten sich auch sachliche Erwägungen finden lassen, um einen Reputationsschutz aus der persönlichkeitsrechtlichen – nicht wirtschaftsrechtlichen – Lesart des Art. 2 Abs. 1 GG abzuleiten. Prima facie scheint hierfür der Ehrschutz des Art. 2 Abs. 1 iVm 1 Abs. 1 GG als Vorbild geeignet. Seine persönlichkeitsrechtliche Prägung weist allerdings einen starken Bezug zur Menschenwürde auf[1112], sodass er um entsprechende Aspekte gekürzt bzw. angepasst werden muss. Als Geschäftsehre umfasst er unter Würdigung der Eigenart juristischer Personen iSd Art. 19 Abs. 3 GG den sozialen Achtungs- und Geltungsanspruch des Unternehmens im Wettbewerb und zu geschäftlichen Zwecken.[1113] Per Definition kommt es also nicht auf die Menschenwürde an, da auch ein Unternehmen der Schmähung, Diskriminierung und Diffamierung erliegen kann.[1114] Derartige Beeinträchtigungen fokussieren sich auf die Reputation und den Unternehmenskern als Äquivalent zur Menschenwürde, der beispielsweise – neben

1108 Adressiert wird dabei die horizontale Ausrichtung der Drittwirkung, deren Wirkung unabhängig des Rechtssubjekts eintritt. Wenngleich sich die Lüth-Entscheidung des BVerfG (E 7, 198 [205 ff]) auf Basis zivilrechtlicher und bürgerlicher Pflichten nur auf die Drittwirkung zugunsten natürlicher Personen bezieht, so muss diese im Rahmen der wesensmäßigen Anwendbarkeit des Art. 19 Abs. 3 GG ebenso für juristische Personen gelten. Demgemäß erstreckt sich die unternehmensbezogene Drittwirkung in wettbewerbsrechtlichen Vorschriften, vgl. *Klippel*, JZ 1988, 625 (631); *Ziegelmayer*, GRUR 2012, 761 (762). – Die Drittwirkung im Bereich des Art. 19 Abs. 3 GG einzig bejahend *Enders* in: Merten/Papier, HGr IV, § 89, Rn. 71.

1109 Sub D.I.2.c).

1110 Sub D.I.2.b).

1111 Zur Subsidiarität siehe Fn. 1007.

1112 Den Ehrschutz daher ablehnend BVerfGE 93, 266 (291); vgl. BVerfGK 8, 89 (99 f) sowie *Krug*, Ehre und Beleidigungsfähigkeit von Verbänden, S. 209 ff. Anders OLG Stuttgart NJW 1976, 628. Ausführlich *Hubmann*, Persönlichkeitsrecht, S. 289.

1113 *Klippel*, JZ 1988, 625 (631); *Wronka*, Das Persönlichkeitsrecht juristischer Personen, S. 98, 104 f; *Meissner*, Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht, S. 83; *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2, Rn. 224.

1114 Vgl. *Enders* in: Merten/Papier, HGr IV, § 89, Rn. 79.

Einrichtung und Nutzung digitaler Identitäten – in Produktqualität, Marken, Werbung oder sozialem Engagement verkörpert ist[1115]. Schäden am Unternehmensvermögen iSd Art. 14 Abs. 1 GG oder praktische Einschränkungen iSd Art. 12 Abs. 1 GG sind lediglich Kollateralschäden; der unternehmerische Ehrschutz ist vorrangig[1116]. Diese sachliche Plausibilität sieht sich zudem in der Ähnlichkeit der (mittelbaren) grundrechtlichen Gefährdungslage bestätigt: Sowohl natürliche als auch juristische Personen unterliegen bei Nutzung digitaler Identitäten gleichermaßen den Gefahren des Online-Diskurses, sei es die aufgrund der Vernetzung intensivierte Prangerwirkung oder die fast unmögliche Wiederherstellung eines beschädigten Rufes[1117]. Beiden ist jedoch ein „Interesse an äußerlich ungehinderter, möglichst freier Entfaltung und Verfolgung eigener Zwecke eigen“[1118], das sich nunmehr im partizipatorisch geprägten Internet unter Einsatz digitaler Identitäten verwirklicht. Die digitale Ebene steht jedermann offen und ermöglich dadurch ebenso jedermann eine Beeinträchtigung der digitalen Identität: Was für natürliche Personen oder zwischen Wettbewerbsteilnehmern eine Meldung auf der eigenen Facebook-Seite ist[1119], ist für staatliche Akteure die im Internet veröffentliche Pressemitteilung zum Boykottaufruf[1120]. Unabhängig der Eingriffsrichtung zeigt sich damit die bestehende Notwendigkeit einer Anerkennung und Vereinheitlichung des grundrechtlichen Schutzes unternehmerischer Reputation. Dies führt jedoch nicht zu einem grenzenlosen Schutz: Wie bei natürlichen Personen gewährleistet er nicht „nur so dargestellt zu werden, wie es genehm ist“.[1121] Hinzunehmen sind stets die „Offenlegung wahrer Tatsachen [...], solange sie sich im Rahmen der üblichen Grenzen individueller Entfaltungschancen halten“[1122],

1115 *Ziegelmayer*, GRUR 2012, 761 (762).
1116 Vgl. *Prinz* in: Fezer/Büscher/Obergfell, UWG, S 7, Rn. 122.
1117 Ausführlich *Ziegelmayer*, GRUR 2012, 761 (673 ff). Vgl. auch BVerfG, Beschluss vom 6.11.2019 – Az. 1 BvR 16/13 –, Rn. 103.
1118 *Enders* in: Epping/Hillgruber, BeckOK GG, Art. 19, Rn. 41.
1119 *Ziegelmayer*, GRUR 2012, 761 (764). Vgl. BVerfG NJW 2016, 3362.
1120 Vgl. BVerfGE 148, 11 (12, Rn. 3; 35 ff, Rn. 68 ff).
1121 StRspr BVerfGE 97, 391 (403); 97, 125 (149); 99, 185 (194); 101, 361 (380); 105, 252 (266); 114, 339 (346). BVerfG NJW 2016, 3362; NJW 2012, 765 (757, Rn. 19); NJW 2011, 511 (511, Rn. 21); Beschluss vom 6.11.2019 – Az. 1 BvR 16/13 –, Rn. 82, 107.
1122 BVerfG NJW 2016, 3362.

sachliche „Kritik der Qualität [der] Produkte oder [des] Verhaltens“[1123] sowie das staatliche Interesse zum Schutz und zur Aufklärung der Allgemeinheit[1124]. Dies hindert jedoch nicht daran, von einem prinzipiell weiten Schutz des Unternehmensrufes bzw. der Geschäftsehre auszugehen, welcher die digitale Identität als Repräsentationsmöglichkeit vollumfänglich einschließt.

Im Kern ist sich bei Betrachtung der digitalen Identität als Instrument und Ansammlung von Informationen aber dem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG zuzuwenden. Obschon das BVerfG in seiner initialen Rechtsprechung nur von „neuen Gefährdungen der *menschlichen* Persönlichkeit“[1125] ausgegangen ist, gewährt es juristischen Personen später ebenso grundrechtlichen Schutz gegenüber „Gefährdung[en] hinsichtlich ihrer spezifischen Freiheitsausübung“[1126]. Seitdem folgt auch die Literatur dieser Anwendbarkeit[1127], jedoch nur selten im Zusammenhang mit der Unternehmenspersönlichkeit[1128]. Grundlegend ist die unternehmerische informationelle Selbstbestimmung auf den Schutz der wirtschaftlichen Tätigkeit gerichtet[1129], worin sich bereits (und erneut) das Kriterium des Unternehmensbezugs abzeichnet. Es dient zur Abgrenzung des üblicherweise nur natürlichen Personen zugänglichen Schutzes personenbezogener Daten. Schließlich setzt sich letztgenanntes Dogma bis zuletzt in der harmonisierenden DSGVO fort, wie der Wortlaut des Art. 4 Nr. 1

1123 BVerfGE 105, 252 (266) – Einfügung durch den Bearbeiter. Vgl. auch BGH NJW 2008, 2110 (2115, Rn. 29) mwN vor dem Hintergrund der Schmähkritik.
1124 Hierzu BVerfGE 99, 185 (197 f).
1125 So BVerfGE 65, 1 (41) – Hervorhebung durch den Bearbeiter.
1126 So BVerfGE 118, 168 (204) – Einfügung durch den Bearbeiter.
1127 Zustimmend *Di Fabio* in: Maunz/Dürig, GG-Kommentar, Art. 2, Rn. 224; *Remmert* in: Maunz/Dürig, GG-Kommentar, Art. 19 III, Rn. 103; *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 33; *Wilms*/*Roth*, JuS 2004, 577 (578); unter Hinzuziehen von Art. 12 Abs. 1 GG auch *Kunig*, Jura 1993, 595 (599) sowie *Ziegelmayer*, GRUR 2012, 761 (763). Hinsichtlich des Grundrechts auf Datenschutz aus Art. 8 GrC, Art. 8 EMRK bejahend *Heißl*, EuR 2017, 561 (570). Ablehnend wegen Nähe zur Menschenwürde dagegen *Bernsdorff* in: Meyer/Hölscheidt, GrC-Kommentar, Art. 8, Rn. 18.
1128 *Schnabel*, CR 2016, 342 (347).
1129 BVerfGE 118, 168 (204).

sowie Erwägungsgrund 14 S. 2 DSGVO statuieren.[1130] Bei Lichte besehen benennt Erwägungsgrund 14 S. 2 DSGVO aber expressis verbis „personenbezogene Daten juristischer Personen" wie „Name, Rechtsform oder Kontaktdaten", die ausschließlich in der wirtschaftlichen Tätigkeit des Unternehmens verwendet werden;[1131] es darf „nicht um die dahinter stehenden Personen gehen"[1132]. Diese ist in einer funktionalen Betrachtung des Datums zu ermitteln und regelmäßig beispielsweise bei unternehmensbezogenen Kontaktdaten als „Anlaufstelle" regelmäßig gegeben.[1133] Sie unterliegen damit nicht dem Anwendungsbereich der DSGVO, sondern – sofern geregelt – den Regelungen des Mitgliedsstaates.[1134] Angesichts dessen ist zumindest davon auszugehen, dass juristische Personen über unternehmensbezogene – also nicht-personenbezogene – Daten verfügen können (sollen). Der Schutz kann zwar nicht weiter reichen als jener natürlicher Personen[1135], muss aber im Umkehrschluss das entsprechende Äquivalent ohne Menschenwürdebezug abdecken. Umfasst sind neben der informationellen Geheim- und Privatsphäre in Form von Betriebs- und Geschäftsgeheimnissen bzw. Interna[1136] wie Kundendaten des Unternehmens[1137] auch Schutz und Verwendung von gewerblicher Kennzeichen sowie Abkürzungen, Unternehmensbezeichnungen und Warenzeichen. Eine Diffamierung letzterer ist allerdings oftmals in den vermögensrechtlichen Bereich des Art. 14 Abs. 1 GG einzuordnen[1138], sodass es im Schwerpunkt der Beeinträchtigung der Reputation bzw. Geschäftsehre oder einer bloß die Selbstbestimmung verdrängenden Handlung für eine Aktivierung

1130 *Schnabel*, WM 2019, 1384 (1385 f).
1131 *Rabe*, K&R 2019, 464 (465 f).
1132 *Schnabel*, WM 2019, 1384 (1387); vgl. auch *Bleckmann*/*Helm*, DVBl 1992, 9 (15).
1133 *Rabe*, K&R 2019, 464 (466).
1134 *Rabe*, K&R 2019, 464 (467). Anders dagegen die Rechtsprechung des EuGH, hierzu detailliert S. 466 f des Beitrages mwN.
1135 BVerfGE 128, 1 (43).
1136 Vgl. *Klippel*, JZ 1988, 625 (632); *Ziegelmayer*, GRUR 2012, 761 (763); *Heißl*, EuR 2017, 561 (568). Dies schließt beispielsweise auch personenbezogene Daten der Mitarbeiter ein, wie sich aus dem Parallellaufen von DSGVO und GeschGehG ergibt – so *Gola*, DuD 2019, 569 (570). Interna ohne Personenbezug dagegen nicht unter Art. 2 Abs. 1 GG subsumierend *Wolf*, Der Schutz des Betriebs- und Geschäftsgeheimnisses, S. 115 f.
1137 *Heißl*, EuR 2017, 561 (568); *Wolf*, Der Schutz des Betriebs- und Geschäftsgeheimnisses, S. 115. Ablehnend *Jarass*, NJW 1989, 857 (860).
1138 *Klippel*, JZ 1988, 625 (633).

des Art. 2 Abs. 1 GG bedarf. Die alleinige Verdrängung findet sich allerdings überaus selten, was (erneut) für die subsidiäre Funktion des Art. 2 Abs. 1 GG spricht. Vor diesem Hintergrund ist die digitale Identität einer juristischen Person nur in Bezug auf die wirtschaftliche Tätigkeit im informationellen Kontext geschützt. Soweit der spezifische Fall nicht bereits durch Art. 12 Abs. 1 oder 14 Abs. 1 GG abgefangen wurde, bewahrt das Grundrecht das Geheimhaltungsinteresse an Einzelheiten der (unternehmensbezogenen) digitalen Identität sowie die Hoheit iSd informationellen Selbstbestimmung „wann und innerhalb welcher Grenzen“[1139] der Unternehmensidentität zuzuordnende Daten, Kennzeichen und Marken verwendet oder gar der Öffentlichkeit offenbart werden.

Überdies besteht auch ein Schutz der Vertraulichkeit und Integrität technischer Systeme für juristische Personen gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Dieser systemische Grundrechtsschutz bezieht sich jedoch eher auf Abwehr technischer Gefahren[1140], wenngleich die im System hinterlegten digitalen Identitäten und sonstige Informationen iSd informationellen Selbstbestimmung mittelbar ebenso hiervon umfasst sind. Dementsprechend erfolgt der detaillierte Blick im nachfolgenden Abschnitt.

Das Auffanggrundrecht des Art. 2 Abs. 1 GG stellt sich damit als Bindeglied zwischen dem vermögensrechtlichen und dem funktionsbeschränkenden Schutz juristischer Personen dar. Sowohl der Schutz der Geschäftsehre als auch die formalistische Selbstbestimmtheit über den Verbleib von Informationen finden sich hierin. Der dadurch bestehende, weite Schutzbereich schließt jeweils die digitale Identität juristischer Personen spezifisch ein – sei es in der Außenwirkung als Reputationsschutz oder in Summe und in seinen informationellen Einzelteilen qua Art. 2 Abs. 1 GG.

1139 BVerfGE 65, 1 (42).
1140 *Krügel*, MMR 2017, 795 ff.

e) Conclusio für juristische Personen gem. Art. 19 Abs. 3 GG

Der schon zu Beginn dieser Untersuchung neutral formulierte Begriff der digitalen Identität findet somit nicht nur auf juristische Personen Anwendung, sondern ist im Rahmen des hier vertretenen Unternehmenspersönlichkeitsrechts auch ausreichend geschützt[1141]. Dies gestaltet sich durch den Trias aus dem Recht am eingerichteten und ausgeübten Gewerbebetrieb des Art. 14 Abs. 1 GG, der Berufsfreiheit des Art. 12 Abs. 1 GG und der persönlichkeitsrechtlichen Komponente des Art. 2 Abs. 1 GG. Im Einzelnen schützt der vermögensrechtliche Aspekt des Art. 12 Abs. 1 GG die juristische Person iSe wirtschaftlichen Betätigungsfreiheit, also auch die Ausgestaltung und Nutzung digitaler Identitäten. Der vermögensrechtliche Aspekt des Art. 14 Abs. 1 GG wiederum betrifft den Bestand des Unternehmens als Ganzes. Die bestehende digitale Identität wäre sodann vom Betriebseigentum iSe Nutzungsrechts umfasst, jedoch weniger in seinen informationellen Einzelteilen. Diese sind vielmehr unter den Schutz des Art. 2 Abs. 1 GG zu stellen, wobei sich dieser sowohl auf die Geschäftsehre als auch auf die informationelle Selbstbestimmung hinsichtlich der digitalen Identität bezieht. Der eingangs erwähnte Trias fängt damit nicht nur bestehende, sondern auch zukünftige Darstellungsformen von Unternehmen auf. Ihr Schutz steht damit in nichts dem natürlicher Personen nach.[1142]

II. Technische Betrachtungsweise

Abschließend bleibt in diesem Kapitel zu untersuchen, ob und wie der technikbezogene Grundrechtsschutz die digitale Identität einschließt. Im Zentrum dieses

1141 Ebenso ein Unternehmenspersönlichkeitsrecht befürwortend *Meissner*, Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht, S. 159 ff; *Korneeva*, Das Persönlichkeitsrecht des Unternehmens, S. 119 f; *von Lilienfeld-Toal*, Das allgemeine Persönlichkeitsrecht juristischer Personen des Zivilrechts, S. 125 ff; *Ziegelmayer*, GRUR 2012, 761 (762 ff); *Klippel*, JZ 1988, 625 (633 ff).

1142 Vgl. *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 34.

Abschnitts steht daher der IT-systembezogene Schutz unabhängig des Informationsgehaltes oder einer vertieften, wertenden Einordnung der jeweiligen Endgeräte in die (Persönlichkeits-)Sphären. Namentlich umfasst die Betrachtung die Grundrechte der Art. 13 Abs. 1, 10 Abs. 1 sowie das Grundrecht auf informationelle Selbstbestimmung und das GGVIS aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Letzteren kommt dabei eine umfängliche Betrachtung zu. In die jeweils verfassungsrechtlich geschützte Technik bzw. den jeweilig geschützten Anwendungsfall ist die digitale Identität sodann einzuordnen.

Hinsichtlich der weiteren Prüfung ist jedoch eine Änderung in der Prüfungsstruktur vorzunehmen: Wohingegen zuvor zwischen natürlicher und juristischer Person unterschieden wurde, kann nun für diesen Abschnitt von einer derartigen Trennung abgesehen werden. Allumfassend richtet sich der grundrechtliche Schutz dieser Lesart auf einen Sphärenschutz in Form technischer Einrichtungen. Die in der Sphäre geschützten Interessen können auf unterschiedlichem verfassungsrechtlichem Ursprung beruhen – beispielsweise dem Schutz der Privatsphäre aufseiten natürlicher Personen oder der Schutz der „betrieblichen Privatsphäre“ eines Unternehmens in Form von Betriebs- und Geschäftsgeheimnissen. Der verfassungsrechtliche Schutz der technischen Einrichtung versteht sich aber regelmäßig als Vertrauens- und Bestandsschutz. Dieser ist abseits der Menschenwürde des Art. 1 Abs. 1 GG zu verorten und daher unabhängig der personellen Schutzfähigkeit zu betrachten.[1143]

1143 Zu Art. 13 GG siehe stRspr BVerfGE 32, 54 (72); 42, 212 (219); 44, 353 (371); 76, 83 (88); 96, 44 (51); 106, 28 (43); 120, 274 (309); *Herdegen* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 13, Rn. 34, 37; *Papier* in: Merten/Papier, HGr IV, § 91, Rn. 8; *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 88; *Bethge*, Grundrechtsberechtigung juristischer Personen, S. 37/38. Zum Fernmeldegeheimnis des Art. 10 Abs. 1 GG siehe stRspr BVerfGE 67, 157 (172); 100, 313 (358); 106, 28 (36, 43); *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 24; *Stern*, StaatsR IV/1, S. 261; *Stettner* in: Merten/Papier, HGr V, § 92, Rn. 42. Zum Grundrecht auf informationelle Selbstbestimmung siehe BVerfGE 118, 168 (204); *Stern*, StaatsR IV/1, S. 246 f; vgl. auch LG Berlin ZUM 2004, 578 (579 f). Hinsichtlich des GGVIS siehe *Drallé*, GGVIS, S. 68 ff; *Freimuth*, Gewährleistung der IT-Sicherheit, S. 160 ff; *Rudolf* in: Merten/Papier, HGr IV, § 90, Rn. 80.

1. Unverletzlichkeit von Wohnraum und Privatheit, Art. 13 Abs. 1 GG

Zuvorderst ist sich der Unverletzlichkeit des Wohnraumes gem. Art. 13 Abs. 1 GG zu widmen. Darunter ist der Schutz der räumlich umgrenzten, der Öffentlichkeit entzogenen Privatsphäre zu verstehen.[1144] Dementsprechend weist das Grundrecht eine Nähe zur Menschenwürde des Art. 1 Abs. 1 GG auf.[1145] In Abhängigkeit der Nutzung der Räumlichkeit entfernt sich der Schutz des Art. 13 Abs. 1 GG von der Menschenwürde, sofern es sich um weniger private Räumlichkeiten wie Betriebs- und Geschäftsräume handelt.[1146] Die damit weit zu verstehende Sphäre ist dann beeinträchtigt, wenn ein Umgehen der räumlichen Abgrenzung vorliegt. Auch das Überwinden von Umfriedungen, (verschlossenen) Türen und anderen Hindernissen ohne Einwilligung des Nutzungsberechtigten der Räumlichkeit stellt einen Eingriff dar.[1147]

In Bezug auf digitale Sachverhalte hat das Bundesverfassungsgericht den Eingriffsbegriff um Mittel und Maßnahmen erweitert, die „einen Einblick in Vorgänge der Wohnung verschaffen, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind."[1148] Schutzgut ist also nicht nur die räumliche Sphäre an sich, sondern auch die darin entäußerte Information.[1149] Um diese

1144 StRspr BVerfGE 18, 121 (131 f); 32, 54 (75); 89, 1 (12); 120, 274 (309). Auch *Gornig* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 13, Rn. 1 ff; *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 85 ff; *Albers*, DVBl 2010, 1061 (1064).

1145 BVerfGE 42, 212 (219); 106, 28 (43); 113, 348 (391); *Gornig* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 13, Rn. 4.

1146 Vgl. BVerfGE 32, 54 (69 ff); 42, 212 (219); 44, 353 (371); 76, 83 (88); 96, 44 (51); 106, 28 (43); 109, 279 (314); *Herdegen* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 13, Rn. 34; *Papier* in: Merten/Papier, HGr IV, § 91, Rn. 9; *Gornig* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 13, Rn. 22, 36. Ebenso ist Art. 8 Abs. 1 EMRK auf juristische Personen anwendbar, siehe nur EGMR NJW 1993, 718 sowie Urt. v. 16.4.2002, Az. 37971/97. Ablehnend dagegen *Kühne* in: Sachs, GG, Art. 13, Rn. 4.

1147 Vgl. *Herdegen* in: Kahl/Waldhoff/Walter, BonnK GG, Art. 13, Rn. 27 f; *Gornig* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 13, Rn. 16 f, 43 f.

1148 BVerfGE 120, 274 (310).

1149 BVerfGE 109, 279 (374 f); *Hermes* in: Dreier, GG, Art. 13, Rn. 12.

mittels technischer Hilfsmittel zu erlangen, kann im Rahmen einer sog. Online-Durchsuchung je nach Ausgestaltung der heimlich installierten Software auf die in Endgeräten integrierte aktive Sensorik oder verbundene Peripheriegeräte – hauptsächlich Kameras und Mikrofone, jüngst insbesondere von Sprachassistenten[1150] – zugegriffen werden.[1151] Der Eingriff beginnt jedoch erst mit Einschalten bzw. Nutzen dieser Instrumente, nicht schon mit der Installation der Software.[1152] Wenngleich dabei wiederum „Software-Umfriedungen" wie Firewalls oder Virenscanner[1153] überwunden werden, erklärt dies nicht das jeweilige Endgerät als Wohnraum iSd Art. 13 Abs. 1 GG. Die räumliche Integrität, die Art. 13 Abs. 1 GG schützt, hat folglich kein technisches Äquivalent.[1154] Gelingt der Zugriff lediglich auf Datensätze des Endgerätes, so erfolgt der Eingriff in die informationellen Grundrechte des Art. 2 Abs. 1 iVm 1 Abs. 1 GG.[1155] Demgemäß kann Art. 13 Abs. 1 GG schon nicht die digitale Identität schützen. Sie bildet sich und existiert ausschließlich auf digitalen Speichermedien. Einzig Gespräche über den Umgang und die Verwendung dieses Alter Ego können für einen Schutz durch Art. 13 Abs. 1 GG relevant sein. Der Schutz der räumlichen Privatsphäre des Art. 13 Abs. 1 GG kommt der digitalen Identität damit nicht zugute.

1150 Siehe hierzu *Rüscher*, NStZ 2018, 687 (688).

1151 Pressemitteilung des Chaos Computer Clubs vom 8.10.2011, abrufbar unter https://www.ccc.de/de/updates/2011/staatstrojaner; BVerfGE 120, 274 (310); *Gercke*, CR 2007, 245 (248).

1152 BVerfGE 120, 274 (311).

1153 Vgl. *Gercke*, CR 2007, 245 (249); *Kutscha*, NJW 2007, 1169 (1170); *Hofmann*, NStZ 2005, 121 (124).

1154 Vgl. auch *Gercke*, CR 2007, 245 (250); *Hofmann*, NStZ 2005, 121 (124); *Hornung*, JZ 2007, 828 (829 f) als Erwiderung auf *Rux*, JZ 2007, 285 (insbes. 292 ff).

1155 Siehe nur BVerfGE 120, 274 (311 ff).

2. Fernmeldegeheimnis, Art. 10 Abs. 1 Var. 3 GG

Plausibler erscheint da ein Schutz durch das Fernmeldegeheimnis des Art. 10 Abs. 1 Var. 3 GG. Seinem Schutz unterliegt die der unkörperlichen[1156] Individualkommunikation immanente Vertraulichkeit bzw. „Privatheit auf Distanz“[1157].[1158] Die Auflösung der räumlichen Privatheit von Gesprächen vis-à-vis durch ortsunabhängige und digitale, nunmehr alltägliche Kommunikationsformen (Bilder, Sprachnachrichten als Fortentwicklung des Short Message Service, etc.) macht besagte Privatheit brüchig und verletzbar. Durch ein (notwendiges) Einbeziehen eines Dritten zur Überwindung der räumlichen Distanz werden die Grenzen des Vertrauens gedehnt und Dritte (unfreiwillig) einbezogen.[1159] Um die Vertraulichkeit weiterhin zu erhalten, muss der Dritte bestimmte Grundsätze zum Schutz des Inhalts und der Umstände laufender Kommunikationsprozesse wahren. Im Vergleich zu den weiteren Freiheiten des Art. 10 Abs. 1 GG bedarf es beispielsweise der Ausrichtung des angebotenen Kommunikationsmodells auf „einen privaten, vor den Augen der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen (Informationen)“[1160]. Hierzu kann sich auch technischer Mittel wie etwa Zugangsschlüsseln[1161] (Passwörter, Login-Daten) bedient werden, insbesondere nach dem dynamischen Verständnis des Grundrechts[1162]. Eine unmittelbare Bindung Privater an Art. 10 Abs. 1 GG besteht jedoch nicht, sodass dem Gesetzgeber die Prärogative zur Vorgabe technischer Standards und dem Umgang

1156 *Pagenkopf* in: Sachs, GG, Art. 10, Rn. 14a f.
1157 So *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 19.
1158 BVerfGE 67, 157 (172); 85, 386 (395 f); 100, 313 (358); 106, 28 (37); 115, 166 (182); 120, 274 (340 f); *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 62, 64; *Stettner* in: Merten/Papier, HGr V, § 92, Rn. 20; *Deusch/Eggendorfer*, K&R 2017, 93 (93 f).
1159 BVerfGE 85, 386 (396); 106, 28 (36 f); 115, 166 (182); *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 65; *Schwabenbauer*, AöR 137 (2012), 1 (16); *Bizer*, DuD 1996, 5 (5).
1160 So BVerfGE 67, 157 (171).
1161 Vgl. BVerfGE 120, 274 (341).
1162 BVerfGE 46, 120 (144); 106, 28 (36); 113, 348 (383); 115, 166 (182 f); *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 60, 23; vgl. auch *Pagenkopf* in: Sachs, GG, Art. 10, Rn. 14 c.

mit Inhalts-, Verkehrs- und Bestandsdaten[1163] obliegt.[1164] Der Schutz des Grundrechts bezieht sich allerdings nur auf laufende Vorgänge[1165] und die Speicherung von Kommunikationsdaten außerhalb des Herrschaftsbereich der Teilnehmenden[1166]. Mithin bezieht er „den Informations- und Datenverarbeitungsprozeß [sic], der sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließt [sic], und den Gebrauch, der von den erlangten Kenntnissen gemacht wird", ein.[1167] Nach Abschluss der Kommunikation im Herrschaftsbereich der Teilnehmenden verbleibende Daten unterliegen dagegen dem Schutz des Grundrechts auf informationelle Selbstbestimmung, Art. 2 Abs. 1 iVm 1 Abs. 1 GG.[1168] Insofern ergänzt Art. 10 Abs. 1 GG den Schutz der Art. 13 und 2 Abs. 1 iVm 1 Abs. 1 GG.[1169]

Seine technische Prägung erhält das Grundrecht durch sein Schutzgut: Die geschützte Vertraulichkeit beruht nicht auf zwischenmenschlichem Vertrauen[1170], sondern dem Fernmeldevorgang als Informationsmedium. Die Gefährdung des Fernmeldegeheimnisses besteht nicht wie bei übrigen Varianten des Art. 10 Abs. 1 GG durch den Dritten als Person, sondern die mögliche technische Angreifbarkeit der Verbindung durch einen über den Dienstleister des Mediums hinausgehenden Personenkreis.[1171] Diesbezügliche Schutzmaßnahmen liegen allerdings außerhalb des Herrschaftsbereiches des Kommunikationsteilnehmers. Aus der Ohnmacht

1163 Diesbezüglich bleibt die Nähe zum laufenden Telekommunikationsvorgangs zu berücksichtigen, sodass nicht jedes Bestandsdatum dem Schutz des Art. 10 Abs. 1 GG unterliegt – so *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 65.

1164 Zur Rolle des Gesetzgebers auch *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 40.

1165 BVerfGE 115, 166 (183 f).

1166 Umkehrschluss aus BVerfGE 115, 166 (184), unmittelbar E 120, 274 (307/308). Ebenso *Buermeyer*, StV 2013, 470 (474).

1167 So BVerfGE 100, 313 (359) unter Verweis auf 65, 1 (46). Ähnlich BVerfGE 106, 28 (38) unter Verweis auf die grundrechtliche Gefährdungslage; 110, 33 (69 f) ; *Schwabenbauer*, AöR 137 (2012), 1 (15/16). Scheinbar damit brechend E 115, 166 (183 ff); 120, 274 (307 ff).

1168 BVerfGE 115, 166 (184); 120, 274 (307 f).

1169 BVerfGE 115, 166 (187, 199 f); *Buermeyer*, StV 2013, 470 (473).

1170 Vgl. hierzu *Nettesheim*, VVDStRL 70 (2010), 7 (22): „Verfassungsrechtlichen Schutz des Vertrauens in die Integrität des Kommunikationspartners gibt es [...] nicht."

1171 *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 61, 44; vgl. *Pagenkopf* in: Sachs, GG, Art. 10, Rn. 14a.

generiert sich ein Vertrauensschutz gegenüber dem Handeln des Dritten zum Schutz der technischen Integrität.[1172] Zwangsnotwendig gehört zu den „bereichsspezifischen Schutzvorkehrungen" des Art. 10 Abs. 1 GG[1173] also ein gefestigter, übertragungssicherer Weg zum Erhalt der Verborgenheit der Kommunikation[1174].

Prima facie liegt der technische Schutz der grundrechtlich geschützten Kommunikationsvorgänge damit in der Verantwortung des Diensteanbieters. Näher besehen ist dies jedoch ein synallagmatisches Verhältnis, bei dem der Nutzer bzw. Teilnehmer entsprechende Vorgaben des Diensteanbieters berücksichtigen muss, um einem effektiven Schutz durch den Diensteanbieter beizuwirken. Dabei kann es sich z.B. um ein ausreichend langes und variantenreiches Passwort handeln, das regelmäßig gewechselt wird. Darüber hinaus dienen Login-Daten oftmals zur Generierung eines Schlüssels (bspw. Hash-Wertes), der ausschließlich einseitig beim Nutzer bzw. Teilnehmer bekannt ist.[1175] Das damit scheinbare Verlagern der Ohnmacht hin zur machtvollen (ggf. informationellen) Selbstbestimmung löst den Schutz des Art. 10 Abs. 1 GG nicht auf, sondern ist im Speziellen eine besondere Maßnahme des Diensteanbieters zum Schutz vor Angriffen auf die eigene Infrastruktur sowie die Daten der Nutzer. Lediglich der Schutz des einseitig vorhandenen Schlüssels liegt allein in der Sphäre des Kommunikationsteilnehmers, sodass entsprechende Grundrechte des Art. 2 Abs. 1 iVm 1 Abs. 1 GG in Betracht kommen. Das Beiwirken der Nutzer ist allerdings nicht als Selbstschutz zu begreifen, da derartige Maßnahmen sich nur auf Datensätze im Herrschaftsbereich beziehen können und einseitig vom Nutzer ausgehen.[1176] Sub specie der Schutzrichtung des Art. 10 Abs. 1 GG ist der Selbstschutz

1172 Vgl. *Nettesheim*, VVDStRL 70 (2010), 7 (26).

1173 *Nettesheim*, VVDStRL 70 (2010), 7 (17).

1174 So *Pagenkopf* in: Sachs, GG, Art. 10, Rn. 14c unter Rekurs auf BVerfGE 67, 157 (171).

1175 Zum Verfahren siehe vgl. *Eckert*, IT-Sicherheit, S. 420 ff; *Hellmann*, IT-Sicherheit, S. 57 ff. Als Beispiel lässt sich hier der sog. Secret Key beim Passwort-Manager 1Password nennen, bei dem die Sicherheit durch ein Zwei-Schlüssel-Verfahren erhöht wird – hierzu https://1password.com/files/1Password-White-Paper.pdf.

1176 Vgl. *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 2 f, 42 sowie die dargestellten Selbstschutzmaßnahmen bei *Hossenfelder*, Pflichten von Internetnutzern zur Abwehr von Malware und Phishing in Sonderverbindungen, S. 125 ff, die allesamt aufseiten des Nutzers vorgenommen werden.

iSd informationellen Selbstbestimmung durch einen präventiven Charakter geprägt, wo „die spezifischen Gefahren der räumlich distanzierten Kommunikation [...] im Herrschaftsbereich des Empfängers, der eigene Schutzvorkehrungen gegen den ungewollten Datenzugriff treffen kann, nicht [bestehen].“[1177] Nur sofern der Selbstschutz dazu dient, das Fernmeldegeheimnis aufrechtzuerhalten oder die objektive Geheimheit der Kommunikation zu verstärken, kommt ein Schutz des Art. 10 Abs. 1 GG in Betracht.[1178] Vor diesem Hintergrund eine *Transport*verschlüsselung[1179] nicht als Teil der grundrechtlich geschützten vertraulichen Signal*übertragung*anzuerkennen ließe die Entwicklungsoffenheit sowie den status activus des Grundrechts aussen vor.[1180] Demgemäß umfasst das Fernmeldegeheimnis des Art. 10 Abs. 1 GG in technischer Hinsicht sämtliche Maßnahmen zum Schutz vor der Kenntnisnahme Dritter, sofern sie die Vertraulichkeit der Individualkommunikation stärken; auf den Initiator der Maßnahme kommt es nicht an. Für den grundrechtlichen Schutz ist er keinesfalls obligatorischer Natur.[1181]

Für die digitale Identität ist das Fernmeldegeheimnis des Art. 10 Abs. 1 GG zunächst nur in Belangen der Individualkommunikation relevant. Sofern ein

1177 BVerfGE 115, 166 (184) – Einfügungen durch den Bearbeiter.

1178 *Eichenhofer*, Der Staat 55 (2016), 41 (46). Im Zweifel über die Geheimheit ist von einem Schutz durch das Fernmeldegeheimnis auszugehen – so BVerfGE 125, 260 (311).

1179 Zum Begriff differenzierend siehe *Buermeyer*, StV 2013, 470 (471); vor dem Hintergrund des Art. 32 DSGVO auch *Ritter* in: Schwartmann et al., DSGVO/BDSG, Art. 32, Rn. 39. Als Beispiele hierfür kann neben den für E-Mails typischen Varianten mit Transport Layer Security (TLS) in Form von IMAPS und POP3S auch das für Instant Messaging relevante Signal-Protokoll genannt werden. Letzteres wird bis zuletzt beim gleichnamigen Messenger sowie bei WhatsApp eingesetzt. Die Verschlüsselung via S/MIME und OpenPGP/GPG ist dagegen eine *Inhalts*verschlüsselung, weshalb sie auch offline zu anderen Zwecken eingesetzt werden kann – hierzu *Eckert*, IT-Sicherheit, S. 801 ff, 806 ff. Bei einem Einsatz zum Schutz der Individualkommunikation muss unter Würdigung der Schutzbereichsdefinition des Art. 10 Abs. 1 GG aber ebenso von einem Schutz durch das Fernmeldegeheimnis ausgegangen werden – iE ebenso *Durner* in: Maunz/Dürig, GG-Kommentar, Art. 10, Rn. 91, 52 f; *Bizer*, DuD 1996, 5 (6 f); *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 66. Ablehnend *Buermeyer*, StV 2013, 470 (474 f).

1180 *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 15: „Verschlüsselungsfreiheit“. Überdies dient die Verschlüsselung dem Selbstdatenschutz und ist sowohl durch das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG als auch Art. 2 Abs. 1 GG geschützt – umfassend hierzu *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 9 ff, 17 ff.

1181 So auch *Schwabenbauer*, AöR 137 (2012), 1 (18 f).

Messenger-Dienst mit einem Zugangsdaten-Paar (z.B. Benutzername und Passwort) verwendet wird, besteht ein fließender Übergang zum Schutz des Fernmeldegeheimnisses. Die Einzeldaten unterliegen dem Schutz personenbezogener Daten nach Art. 2 Abs. 1 iVm 1 Abs. 1 GG, wohingegen die Funktionen der digitalen Identität als Mittel der vertraulichen Kommunikation vom Schutz des Art. 10 Abs. 1 GG umfasst sind. Je nach Handhabe über die technischen Gegebenheiten erweitert sich der Schutzumfang um Mittel der Verschlüsselung zum Schutz und Erhalt der Vertraulichkeit.

Darüber hinaus bleibt ein Blick auf die einzelnen geschützten Positionen des Grundrechts zu werfen: Der Schutz von Inhalten und Umständen jeglicher Individualkommunikation begründet sich nicht nur aus dem geschützten Kommunikationsvorgang. Vielmehr begründet die Möglichkeit der Anreicherung von Orten der Kommunikationsteilnehmer, Verbindungszeit und -dauer, Häufigkeit der Kontaktaufnahme, Art und Weise der verwendeten Kommunikationsmittel, Verbindungsdaten der Teilnehmer, Anschlüsse und Nummern mit entsprechender Identifikationswirkung für übrige Verbindungsdaten[1182] das Entstehen von (Sozial-)Profilen[1183] – also dem Kommunikationsteilnehmer nur bedingt zugängliche digitale Identitäten. Der Unvermeidbarkeit dieser Datenerhebung ist aber die teilweise Flüchtigkeit der Daten sowie die Zweckgebundenheit und Erforderlichkeit der Verwertung einzelner Daten entgegenzusetzen.[1184] Die schon im Datenschutzrecht bewährten Grundsätze finden also auch hier kontextualisiert Anwendung[1185] und reduzieren zumindest die nicht-zielgerichtete Aggregation von Daten.

In Summe ergibt sich damit ein bloß partieller, funktions- bzw. bereichsspezifischer Grundrechtsschutz durch das Fernmeldegeheimnis des Art. 10 Abs. 1

1182 BVerfGE 100, 313 (358); 113, 348 (383); 115, 166 (183 f); 120, 274 (309); *Horn* in: Isensee/Kirchhof, HStR VII, § 149, Rn. 101; *Durner* in: Maunz/Dürig, GG-Kommentar, Art. 10, Rn. 86; *Gusy* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 10, Rn. 65; *Eichenhofer*, Der Staat 55 (2016), 41 (46 f).

1183 *Schwabenbauer*, AöR 137 (2012), 1 (10); *Eichenhofer*, Der Staat 55 (2016), 41 (47).

1184 Vgl. BVerfGE 100, 313 (359 ff); 110, 33 (53 ff); 120, 274 (316).

1185 BVerfGE 100, 313 (358 f); 110, 33 (53); 115, 166 (189); 125, 260 (310).

Var. 3 GG. Er umfasst nur die Verwendungsweise digitaler Identitäten zur unkörperlichen Individualkommunikation. Soweit die Vertraulichkeit dieser Kommunikation durch Selbstschutzmaßnahmen geschützt werden soll, sind ebendiese Maßnahmen ebenso vom Fernmeldegeheimnis gedeckt. Dass durch die Grundsätze der Erforderlichkeit und Zweckmäßigkeit die Aggregation und Kumulation von Daten nach Möglichkeit vermieden wird, stellt lediglich einen Nebeneffekt des Art. 10 Abs. 1 Var. 3 GG und entsprechender einfachgesetzlicher Vorschriften dar. Der daraus resultierende positive Effekt wirkt sich eher auf den informationellen Schutz und das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG aus.

3. Informationelle Selbstbestimmung

Wie bereits in informationeller Hinsicht[1186], scheint sich auch in technischer Hinsicht der umfänglichste Schutz aus dem Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG zu ergeben. Die beschriebene Selbstbestimmtheit bei Datenverarbeitungsvorgängen setzt schließlich eine technische Infrastruktur voraus. Diese Selbstverständlichkeit findet sich in der Magna Charta des Grundrechts – dem Volkszählungsurteil[1187] – höchstens im Ansatz: Den „moderne[n] Entwicklungen und [...] neuen Gefährdungen“, denen mit dem Grundrecht begegnet werden soll[1188], muss sich auf Basis der Entwicklungsoffenheit des Grundrechts entsprechend modern gestellt werden. Es kann nicht ausreichen, auf technische Gefahren bloß rechtliche Mittel wie Unterlassungs- und Löschungsansprüche zu gewähren. Eher muss das im Grundrecht verankerte Bewusstsein über die eigene Datennutzung auch technische Schutzmaßnahmen einbeziehen. Hinsichtlich Zweck und Verknüpfungsmöglichkeiten „müssen der Informationserhebung und Informationverarbeitung *innerhalb des Informationssystems* zum Ausgleich entsprechende Schranken gegenüberstehen.“[1189] Damit

1186 Siehe hierzu D.I.1.b).
1187 BVerfGE 65, 1.
1188 BVerfGE 65, 1 (42).
1189 BVerfGE 65, 1 (48) – Hervorhebung durch den Bearbeiter.

benennt das Gericht Schranken innerhalb bzw. durch das System, was ein Indiz für den nunmehr normierten Ansatz des Privacy by Design/Default darstellen könnte.

Erst bei späteren Urteilen zu technikbezogenen Eingriffen – namentlich zur Vorratsdatenspeicherung und zu Online-Durchsuchungen – dringt dieses Verständnis stärker durch. Hinsichtlich der Online-Durchsuchung informationstechnischer Systeme für die Persönlichkeitsentfaltung setzt das Gericht voraus, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet.[1190] Im Wortlaut ähnelt die Passage stark dem später im Urteil definierten GGVIS[1191], weshalb die Aussage die spätere Definition lediglich vorbereitet. Vor dem Hintergrund technischer Selbstschutzmaßnahmen lässt sich die Passage allerdings auch derart verstehen, dass das verfassungsrechtliche Datenschutzgrundrecht durchaus technische Komponenten umfasst – sie sind aufgrund des entstandenen Schutzbedürfnisses lediglich „nicht hinreichend"[1192]. Im Hinblick auf die Vorratsdatenspeicherung erkennt das Bundesverfassungsgericht mit Blick auf Telekommunikationsverkehrsdaten den Grundsatz der Datensicherheit en détail an, wenn es konkrete Vorgaben für eine „Implementierung eines wirksamen Datenschutzes" gibt.[1193] In weiteren Urteilen mit ähnlicher Zielrichtung verklingen aber jegliche Ausführungen hinsichtlich der Datensicherheit als technischer Aspekt des Schutzes personenbezogener Daten. Diese Lücke wird auch nicht durch Entscheidungen des EuGH oder EGMR bezüglich Art. 8 GrC und Art. 8 EMRK gefüllt.[1194]

Konsultiert man die rechtswissenschaftliche Literatur in der Hoffnung auf eine verfassungsrechtliche Verankerung der Datensicherheit, so bleibt diese unerfüllt.

1190 BVerfGE 120, 274 (306).
1191 Siehe BVerfGE 120, 274 (313 ff).
1192 BVerfGE 120, 274 (306).
1193 BVerfGE 125, 260 (325/326).
1194 Lediglich einfachgesetzliche Vorgaben fordernd EuGH, Urteil v. 08.04.2014, Az. C-293/12, Rn. 66. Ähnlich oberflächlich EGMR, U. v. 30.07.1998, Az. 58/1997/842/1048, Rn. 46: „the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection".

Die verfassungsrechtliche Literatur hält sich bei einer Positionierung dieser zurück oder geht von einem Bestehen innerhalb des Grundrechts auf informationelle Selbstbestimmung aus. Beispielsweise sieht *Starck* die „Integrität von Daten" als Fallgruppe der informationellen Selbstbestimmung an[1195], *Stern* sieht „materiellrechtliche, prozedurale und organisatorische Vorkehrungen zur Datensicherheit" objektiv-rechtlich verankert[1196]. In den Einzelheiten bleiben die Stimmen jedoch stumm. Konkreter werden nur Vertreter des (einfachgesetzlichen) Datenschutzrechts, insbesondere in Bezug auf die Verpflichtung von Verantwortlichen zu Maßnahmen der Datensicherheit gem. Art. 24 Abs. 1, 25 und 32 DSGVO. Expressis verbis sollen hiernach geeignete technische und organisatorische Maßnahmen vonseiten der Verantwortlichen eingesetzt werden, um die Sicherheit der Verarbeitung und ein angemessenes Schutzniveau zu gewährleisten. Hierzu sind besonders frühzeitige Maßnahmen nach Art. 25 Abs. 1 DSGVO in Form der technischen Implementierung des Datenschutzes by Design (Hardware) und by Default (Software) zu berücksichtigen.[1197] Im Übrigen sind Maßnahmen der verarbeitenden Stellen an den „Stand der Technik" gebunden. Auffällig ist aber die in Art. 32 Abs. 1 lit. b DSGVO definierte Anforderung an eine solche Maßnahme. Sie muss „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer" sicherstellen. Stellt man diesen Wortlaut den Schutzzielen der IT-Sicherheit, festgehalten in § 2 Abs. 2 BSI-G, gegenüber, gleichen sich diese in dem Schutz der „Verfügbarkeit, Unversehrtheit [bzw. Integrität] oder Vertraulichkeit von Informationen"[1198].

1195 *Starck* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I, Art. 2, Rn. 177.

1196 *Stern*, StaatsR IV/1, S. 237.

1197 *Hartung* in: Kühling/Buchner, DSGVO, Art. 25, Rn. 11, 14 ff und 24 ff; *Schläger* in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, Teil G, Rn. 35 ff; *Richter* in: Jandt/Steidle, Datenschutz im Internet, B.IV. Rn. 5.

1198 § 2 Abs. 2 BSI-G – Einfügung durch den Bearbeiter.

Darüber hinaus wird in der datenschutzrechtlichen Literatur der Begriff der Datensicherheit regelmäßig synonym mit der Systemsicherheit verwendet[1199] und die Definition der Schutzziele sowie Schutzmaßnahmen werden mittels Nomenklatur der IT-Sicherheit befüllt[1200]. Insofern schafft die Literatur keine klaren Verhältnisse, derer sich aufgrund der unklaren gesetzlichen Auskleidung kaum zu entziehen ist.

Hilfreicher ist dagegen der Blick auf die Historie des § 9 BDSG a.F., der sich durch die Umsetzung der Datenschutz-Richtlinie 95/46/EG zum Knotenpunkt der Datensicherheit bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten entwickelte.[1201] Zweck (auch dieser) Regelung ist die (technische) Abwehr von Beeinträchtigungen des Persönlichkeitsrechts durch die automatisierte Verarbeitung personenbezogener Daten.[1202] Die Einschränkung auf den Schutz personenbezogener Daten ergibt sich durch den Gesamtzweck des BDSG a.F. gem. § 1 I[1203], wohingegen Art. 32 Abs. 1 lit. b DSGVO einen starken Systembezug aufweist. Letzterer lässt sich zwar ebenso durch die persönlichkeitsrechtlich geprägten Ziele des Art. 1 DSGVO einschränken. In der Literatur wird diese Überlegung aber kaum angestellt, wie sich anhand der Definition der Begriffe des

1199 Beispielsweise *Jandt* in: Kühling/Buchner, DSGVO, Art. 32, Rn. 1; *Albrecht*/*Jotzo*, Das neue Datenschutzrecht der EU, § 2, Rn. 14; *Dix* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.5, Rn. 1 ff; *Roßnagel*, MMR 2005, 71 (74) und *Roßnagel*, ZD 2018, 339 (341); *Jandt*, DuD 2017, 562 (562); *Lotz*/*Wendler*, CR 2016, 31 (33); *Schmidt-Jortzig*, DÖV 2018, 10 (15); *Hansen*, DuD 2021, 234 (234 f.). Einzig differenzierend zwischen Systemdatenschutz und Systemschutz *Hoffmann-Riem*, AöR 134 (2009), 513 (532). Möglicherweise basiert dies auf der allgemeinen Formulierung der Definition der Datensicherheit in DIN 44300.

1200 *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 32, Rn. 38 ff sowie vgl. *Hansen*, DuD 2021, 234 (234 f.); *Jandt* in: Kühling/Buchner, DSGVO, Art. 32, Rn. 22 ff, 18; *Schläger* in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, Teil G, Rn. 29 ff; *Bizer*, DuD 2007, 725 (727). Vgl. auch *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 8 f, 44 ff.

1201 Zur Historie siehe nur *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 4 ff.

1202 So *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 37 aE unter Verweis auf *Wybitul*, ZD 2013, 539 (540); *Lotz*/*Wendler*, CR 2016, 31 (33).

1203 *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 11.

Art. 32 Abs. 1 lit. b DSGVO durch das BSI-G und die dadurch geförderte terminologische Vermengung erkennen lässt.[1204] Systemsicherheit entspricht nach dieser Sichtweise der Datensicherheit.

Dass diese Schlussfolgerung fehl geht, legt zunächst die erwähnte Einschränkung durch die Zweckstellung der Kodifikationen nahe. Offensichtlicher ist aber die terminologische Trennung zwischen System- und Datensicherheit. Wenngleich beide dieselben (Schutz-)Ziele verfolgen, ist der Bezugspunkt ein signifikant anderer:

Datensicherheit bezieht sich, wie dargelegt, als Teil des Datenschutzes auf die Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten. Der technische, vorwiegend integritätsbezogene Begriff[1205] ist also mit den datenschutzrechtlichen Schutzzwecken aufzuladen. Die Aspekte der Verfügbarkeit, Integrität und Vertraulichkeit stellen Parameter für die Ermittlung dieser Sicherheit dar. Die Erweiterung der Kriterien ist durch den (notwendigerweise) entwicklungsoffenen Begriff stets möglich, wie sich am Kriterium der Resilienz in Art. 32 Abs. 1 lit. b DSGVO erkennen lässt[1206]. In seiner sicherheitsgeprägten Lesart erscheint die Datensicherheit als status negativus der informationellen Selbstbestimmung, wenn „die technischen Systeme nur das können, was sie dürfen“[1207]. Zugleich gewährt die Datensicherheit den status activus der informationellen Selbstbestimmung. Beispielsweise bedingen sich Verfügbarkeit und Integrität dahingehend, dass die stetige Verfügungsmöglichkeit über ein Datum einschließlich der Beständigkeit des Aussagegehalts die Selbstbestimmung stärkt.[1208] Zur Gewährleistung der Datensicherheit kann auf technische Mittel wie die Härtung von Hardware, aber auch organisatorische Aspekte im Umgang mit Datenschutzvorfällen, zurückgegriffen

1204 Siehe Fn. 1200.

1205 Siehe nur *Eckert*, IT-Sicherheit, S. 6: „Die Datensicherheit [...] ist die Eigenschaft eines funktionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen.“ Vgl. auch *Jandt* in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 17, Rn. 40; *Brodowski* in: Kipker, Cybersecurity, § 13, Rn. 80; ausführlicher *Kipker*, <kes> 2021, 61 ff.

1206 Zum Kriterium siehe nur *Gonscherowski*/*Hansen*/*Rost*, DuD 2018, 442 ff.

1207 *Roßnagel*, MMR 2005, 71 (74); vgl. *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 44 ff sowie *Bizer*, DuD 2007, 725 (726).

1208 Vgl. *Roßnagel*, MMR 2005, 71 (74).

werden.[1209] „Insoweit stehen Datensicherheit und Datenschutz nicht beziehungslos nebeneinander, sondern bedingen sich gegenseitig"; sie bilden ein „gemeinsames Konzept".[1210] Die Datensicherheit gewährleistet lediglich den technischen und organisatorischen Rahmen der Verarbeitung persönlichkeitsrelevanter Daten bzw. des Datenschutzes.[1211]

Systemsicherheit bezieht sich dagegen unter Berücksichtigung der Definition in § 2 Abs. 2 BSI-G lediglich auf Informationen als terminus technicus, was einen breiten Anwendungsspielraum eröffnet. Technisch ausgedrückt: „Die Informationssicherheit [...] ist die Eigenschaft eines funkionssicheren Systems, nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen."[1212] Demnach würde das BSI-G auch den Schutz personenbezogener Daten umfassen. Dem steht jedoch die übrige Formulierung des § 2 BSI-G entgegen, da sich die Maßnahmen der IT-Sicherheit ausschließlich auf informationstechnische Systeme, Komponenten oder Prozesse sowie das jeweilige Äquivalent auf Anwendungsebene erstrecken. Folglich kommt es nicht auf die Gewährleistung der Schutzziele während der informationell relevanten Verarbeitung personenbezogener Daten, sondern auf den Schutz des Systems und einzelner Prozesse als solche an. Dieser besteht beispielsweise in der „Vorgabe von allgemeinen technischen Richtlinien für die Sicherheit, von konkreten Vorgaben für die Konfiguration der Informationssicherheit im Einzelfall und Maßnahmen zur Abwehr konkreter Gefahren."[1213] Die weitere Konzeption der Aufgaben des Bundesamts für Sicherheit in der Informationstechnik gem. § 3 Abs. 1 BSI-G bestätigt dies. Unter anderem widmet sich das Gesetz der Abwehr von Schadprogrammen (§ 2 Abs. 5 BSI-G) und Sicherheitslücken (§ 2 Abs. 6 BSI-G) –

1209 Vgl. *Schuster*, CR 2020, 726 (729).

1210 *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 11 aE und 14 aE; vgl. auch *Roßnagel* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.4, Rn. 48 und *Lotz*/*Wendler*, CR 2016, 31 (34).

1211 *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 12; *Bizer*, DuD 2007, 725 (727).

1212 *Eckert*, IT-Sicherheit, S. 6.

1213 So die Begründung der Novelle des BSI-G, siehe BT-Drs. 16/11967, S. 10. Hiervon ist der Begriff des Systemdatenschutzes abzugrenzen – ausführlich dazu *Dix* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.5, Rn. 1 ff.

wenn auch nur der Informationstechnik des Bundes. Dementsprechend weist die Schutzrichtung eine Nähe zum GGVIS auf.[1214]

Festzuhalten ist somit, dass Datensicherheit und Systemsicherheit nicht synonym sind, sondern eigenständige Aspekte darstellen.[1215] Die synonyme Bezeichnung erklärt sich aus der Historie des § 9 BDSG a.F., der vornehmlich den Schutz der heimischen informationstechnischen Geräte und Verarbeitungsvorgänge beabsichtigte. Dieser Gedanke lässt sich mit der heute vernetzten Gesellschaft und Dynamik der technischen Entwicklung nicht vereinbaren.[1216] Daher ist die im Bereich des Individuums liegende Datensicherheit von der überwiegend der Kontrolle entzogenen Systemsicherheit zu trennen. Dennoch bedingen sich beide Aspekte in Abhängigkeit des Einzelfalls. Die Systemsicherheit kann sich denklogisch schon begünstigend auf die Datensicherheit auswirken, wenn sich die jeweilige Sicherheitsmaßnahme auch auf Verarbeitungsprozesse personenbezogener Daten erstreckt.[1217] So wirkt sich ein Penetrationstest zur Überprüfung der Netzwerksicherheit eines Unternehmens sowohl auf den Schutz der gesamten Infrastruktur als auch die darin befindlichen Daten aus; entsprechend handelt es sich um eine technische Maßnahme iSd Art. 32 DSGVO.[1218] Umgekehrt können Maßnahmen der Datensicherheit allerdings nur bedingt auf die Systemsicherheit auswirken, da sie per Definition nur einzelne Prozesse umfasst. Die Datensicherheit ist daher nur ein „flankierendes Element der informationellen Selbstbestimmung".[1219]

1214 Hierzu sogleich sub D.II.4.

1215 Mit gleichem Ergebnis auch *Freimuth*, Gewährleistung der IT-Sicherheit, S. 79 ff, 81 sowie *Jandt* in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 17, Rn. 2 ff sowie vertiefend zu Unterschieden Rn. 12 ff.

1216 *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 2; *Gerling*, DuD 1997, 197 (197).

1217 Vgl. *Karg* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition), BDSG 2003, § 9, Rn. 28a, 18.

1218 Hierzu ausführlich *Deusch/Eggendorfer*, K&R 2018, 223 (226 ff). Dagegen zwischen Verarbeitungen zum Zweck der Netz- und Informationssicherheit iSd ErwGr 49 und technischen und organisatorischen Maßnahmen der Art. 25, 32 DSGVO differenzierend *Jandt* in: Hornung/Schallbruch, IT-Sicherheitsrecht, § 17, Rn. 58.

1219 *Bizer*, DuD 2007, 725 (725, 727).

Folglich kann bezüglich der technischen Ausrichtung des Grundrechts auf informationelle Selbstbestimmung in Form der Datensicherheit aus verfassungsrechtlicher Rechtsprechung und Literatur keine Definition übernommen werden. Einfache Gesetze können hierzu ebensowenig beitragen. Dennoch lässt sich aus der wiederholten Regelung einzelner Anforderungen der Datensicherheit in § 9 BDSG a.F. und Art. 24, 25 sowie 32 DSGVO ableiten, dass der nationale wie europäische Gesetzgeber stets von einer gesetzgeberischen Prärogative in diesem Bereich der informationellen Selbstbestimmung ausgeht. Dementsprechend begreift dieser seine Grundrechtsbindung aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG qua objektiver Funktion des Grundrechts.[1220] Die Sicherheit der Datenverarbeitung weist als Teil des Datenschutzes einen Gemeinwohlbezug auf,[1221] der sich in einer Schutzpflicht des Staates erschöpft. Der Staat hat insofern entsprechende Instrumente und Maßnahmen zum Schutz vor ungesicherter Datenverarbeitung personenbezogener Daten zu nutzen, um die zunehmende Digitalisierung und Entkopplung vom Einzelgerät durch kontextualisierte, verknüpfte mobile Geräte (z.B. SmartWatch und Fitness-Tracker für Fitness-Anwendungen, Mobiltelefon als ortsungebundenes Multimedia-Gerät) nicht zur Gefahr für die digitalen Identitäten der Grundrechtsträger werden zu lassen. Leider zeichnet sich diesbezüglich eine sog. Plug-and-Play-Falle ab, die in einer „spielerisch-einfache[n] Gestaltung von IT-Umgebungen“ resultiert.[1222] Beispielsweise geht die Anmeldung mit einem Facebook-, Google- oder Apple-Nutzerkonto bei anderen Diensten bedeutend leichter von der Hand, wohingegen das dabei entstehende potentielle Sicherheitsrisiko – z.B. bei einem schwachen Passwort des Hauptkontos bei besagten Diensteanbietern – verschwiegen wird. Schließlich gefährdet dies z.T. sensible Daten des Nutzers im Falle eines Identitäts(daten)diebstahls in einem bedeutend größeren Ausmaß. Um diesem Herr zu werden, kann der Gesetzgeber entsprechende Vorgaben beim Angebot von identitätsbezogenen Dienstleistungen treffen. Hier steht dem Gesetzgeber unter Berücksichtigung unternehmerischer Grundrechte (Art. 12 Abs. 1, 14 Abs. 1 GG) ein weiter Handlungsspielraum zu. Zum Beispiel könnte er

1220 Hierzu grundlegend C.III.
1221 Vgl. *Wybitul*, ZD 2013, 539 (539).
1222 Hierzu ausführlich *Heckmann*, NJW 2012, 2631 (2633).

auf eine Zertifizierung von Diensten mit besonderer persönlichkeitsschützender Ausrichtung zurückgreifen[1223], unmittelbare und verpflichtende Anforderungen an Hersteller[1224] kodifizieren oder ein Recht auf datenerhebungsfreie Produkte[1225] bzw. Angebote manifestieren. Demgemäß besteht sowohl eine subjektive als auch objektive Schutzrichtung der Datensicherheit, die in den jeweiligen Funktionen des Grundrechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG aufgeht.

Die digitale Identität genießt vor diesem Hintergrund in technischer Hinsicht wie schon informationell vollumfänglichen Schutz durch das Grundrecht auf informationelle Selbstbestimmung. Soweit ein Personenbezug aufgrund der Referenzierung der einzelnen Identitätsdaten möglich ist, findet das Grundrecht in seinem dargelegten subjektiven und objektiven Schutzgehalt Anwendung. Subjektiv ist der Inhaber der digitalen Identität gegenüber technikbezogenen Eingriffen Grundrechtsgebundener (status negativus) und im Einzelfall durch die Nutzungsmöglichkeit präventiv wirkender, technischer Mittel (status activus) ermächtigt. Objektiv kommt dagegen der Gewährleistungsgehalt des Grundrechts zur Geltung, indem der Staat effektive Mittel zur Förderung subjektiver Grundrechtselemente

1223 Den Grundstein hierfür legen bereits Art. 42, 43 DSGVO.

1224 Vermeintlich sind diese in Art. 25, 32 DSGVO geregelt, welche die Implementierung technischer Maßnahmen expressis verbis regeln. Beide Schlüsselnormen sind jedoch nur an Verantwortliche und Auftragsverarbeitende gerichtet, sodass Hersteller ohne eine der beiden Eigenschaften nicht daran gebunden sind, Informationstechnik von Beginn an datenerhebungsarm zu entwickeln. Dies wurde auch in der datenschutzrechtlichen Literatur bemängelt, siehe nur *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 32, Rn. 15; *Schläger* in: Schläger/Thode, Handbuch Datenschutz und IT-Sicherheit, Teil G, Rn. 7; *Richter* in: Jandt/Steidle, Datenschutz im Internet, B.IV., Rn. 13, 33. Sieht man diese Norm als Mittel zur Regulierung namhafter Hersteller und Anbieter von IT-Diensten, erklärt sich die Formulierung der Normen. Dann tragen sie allerdings nicht zu einer grundsätzlichen Erhöhung der Datensicherheit bei; das Kriterium der Datenschutzfreundlichkeit und Datensicherheit muss sich als Kaufargument bzw. Feature etablieren. Der Sinn und Zweck der Regelung wäre verfehlt. Kritisch muss einer derartigen datenschutzrechtlichen Verpflichtung jedoch entgegengehalten werden, dass eine Verpflichtung des Herstellers ohne Verarbeitungskontext aus der Systematik und dem Zweck des Datenschutzrechts herausfällt – so *Schulz*, CR 2012, 204 (207). Ob sich dies durch das Produkthaftungsgesetz regeln lässt, indem die Datenerhebung bei bestimmten Produkten als Produktfehler anerkannt wird – so *Becker*, JZ 2017, 170 (180) – bleibt an anderer Stelle zu erörtern.

1225 Hierzu *Becker*, JZ 2017, 170 (175 ff).

oder zum Schutz des Grundrechtsträgers schon vor der Datenverarbeitung erwägt. In jedem Fall ergänzt die Datensicherheit als technikgeprägte Lesart den verfassungsrechtlichen Datenschutz der digitalen Identität.

4. Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Abschließend ist sich dem verfassungsrechtlichen Systemsschutz[1226] zu widmen, der durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme verkörpert wird. Wie auch das Grundrecht auf informationelle Selbstbestimmung, ist dieses Grundrecht durch die Rechtsprechung des Bundesverfassungsgerichts aus der Taufe gehoben worden, da das Allgemeine Persönlichkeitsrecht und weitere Schutzgehalte der Konjunktion von Art. 2 Abs. 1 und 1 Abs. 1 GG keinen ausreichenden Schutz boten.[1227] Ob die digitale Identität ihrerseits hierin Schutz findet, ist anhand der Definition des Grundrechts in Abgrenzung zur dargestellten Datensicherheit des Art. 2 Abs. 1 iVm 1 Abs. 1 GG zu untersuchen.

Titelgebend umfasst das Grundrecht den Schutz jeglicher informationstechnischer Systeme. Dabei handelt es sich um eigengenutzte Systeme[1228], über die „allein oder zusammen mit anderen zur Nutzung berechtigten Personen [...] verfügt“ wird.[1229] Als informationstechnische Systeme qualifiziert sie gemäß Rechtsprechung die Eigenschaft, „personenbezogene Daten erzeugen, verarbeiten oder speichern“ zu

1226 Ganz h.M. – BVerfGE 120, 274 (313) sowie Beschluss vom 8.6.2021 – Az. 1 BvR 2771/18 –, Rn. 29 = ZD 2021, 685; *Hoffmann* et al., Die digitale Dimension der Grundrechte, S. 70 f; *Freimuth*, Gewährleistung der IT-Sicherheit, S. 155 f; *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 50 f; *Hoffmann-Riem*, JZ 2008, 1009 (1013); *Luch*, MMR 2011, 75 (75). Vgl. auch *Rudolf* in: Merten/Papier, HGr IV, § 90, Rn. 79; *Hoffmann-Riem*, AöR 134 (2009), 513 (532). Dagegen auf den Schutz personenbezogener Daten reduzierend *Drallé*, GGVIS, S. 31.

1227 BVerfGE 120, 274 (313).

1228 *Hoffmann-Riem*, JZ 2008, 1009 (1019); *Hoffmann-Riem*, AöR 134 (2009), 513 (530).

1229 BVerfGE 120, 274 (315).

können[1230] – unabhängig technischer Begriffe[1231] oder kritischer Diskurse[1232]. Von Bedeutung ist zudem die Vernetztheit des Systems. Wenngleich dies keine eigenständige Voraussetzung für das IT-System darstellt[1233], legt das Gericht diesen Schwerpunkt bei der Skizzierung der grundrechtlichen Gefährdungslage. Expressis verbis erstreckt es den Schutz aber auf Systeme, die „allein *oder* in ihren technischen Vernetzungen personenbezogene Daten" offenlegen könnten. Es schließt damit Gefährdungen nicht-vernetzter Systeme[1234] ein, sofern das System „personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten [kann], dass ein Zugriff [...] es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung der Persönlichkeit zu erhalten."[1235] Dieser „Zusammenhang von Entfaltungsfreiheit und Informationstechnik hat sich seitdem noch verstärkt. Die Umstellung ehemals analoger Vorgänge auf digitale Prozesse [...] erhöh[t] die Abhängigkeit von Informationstechnologie ständig weiter."[1236] Der ideenhistorische Ursprung des Allgemeinen Persönlichkeitsrechts begrenzt folglich den Gehalt des Grundrechts auf Systeme, denen potentiell ein Personenbezug innewohnt; auf die tatsächliche Datenqualität und -menge kommt es nicht an.[1237]

1230 BVerfGE 120, 274 (313).

1231 Siehe nur *Eckert*, IT-Sicherheit, S. 3: „Ein IT-System ist ein geschlossenes oder offenes, dynamisches technisches System mit der Fähigkeit zur Speicherung und Verarbeitung von Informationen."

1232 Ausführlich *Drallé*, GGVIS, S. 29 ff; *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, S. 37 ff; *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 22 ff; *Freimuth*, Gewährleistung der IT-Sicherheit, S. 155 f in Abgrenzung zum einfachgesetzlichen Begriff des IT-Systems; *Eifert*, NVwZ 2008, 521 (522 f); *Hornung*, CR 2008, 299 (302 f); ; *Sachs*/*Krings*, JuS 2008, 481 (484); *Hoeren*, MMR 2008, 365 (365 f). Unabhängig vom Personenbezug auf sämtliche aktive und inaktive IT-Systeme und -Komponenten erstreckend *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 22. Zutreffend differenzierend im Einzelfall auf die aktive Recheneinheit oder den potentiellen Quantität und Qualität der Daten abstellend *Hornung*, CR 2008, 299 (303) sowie *Drallé*, GGVIS, S. 30; vgl. auch *Böckenförde*, JZ 2008, 925 (929).

1233 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 27 mwN. Vgl. auch *Drallé*, GGVIS, S. 32; *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 30; *Hornung*, CR 2008, 302. Scheinbar anders *Luch*, MMR 2011, 75 (76).

1234 Derartige Gefährdungen beschreibend *Herrmann*, GGVIS, S. 27.

1235 BVerfGE 120, 274 (314) – Einfügungen nicht im Original enthalten.

1236 BVerfG, Beschluss vom 8.6.2021 – Az. 1 BvR 2771/18 –, Rn. 33 = ZD 2021, 685 – Einfügungen nicht im Original enthalten.

1237 *Hornung*, CR 2008, 299 (302); *Böckenförde*, JZ 2008, 925 (928).

Das Potential ist stets einzelfallbezogen zu ermitteln[1238], weshalb auch dieses Grundrecht aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG als technisch und kontextuell entwicklungsoffen bezeichnet werden kann. Es fängt also auch einst vom Bundesverfassungsgericht als Negativ-Beispiel erwähnte, nunmehr moderne Modelle der Heimvernetzung zur Steuerung der Haustechnik – kurz: Smart Home – wie Smart-Metering-Geräte[1239] auf.

Der Schutz des jeweiligen informationstechnischen Systems ist in zweierlei Hinsicht zu gewährleisten[1240]: Vertraulichkeit und Integrität. Die Vertraulichkeit bezieht sich zunächst auf das Interesse des Nutzers, dass die in einem informationstechnischen System gespeicherten Daten vertraulich bleiben.[1241] Sie konkretisiert damit das im Allgemeinen Persönlichkeitsrecht wurzelnde Recht der Selbstbewahrung.[1242] Das Vertraulichkeitsinteresse generiert sich aus der Eigennnutzung des informationstechnischen Systems.[1243] Der Aspekt weist damit einen deutlichen (Grundrechts-)Subjektbezug[1244] auf, indem der auf Nutzerseite bei bzw. nach Nutzung des Systems entstehende „Zustand zwischen Wissen und Nichtwissen“[1245] über technische Einzelheiten zu einem verfassungsrechtlich geschützten Interesse erwächst. Auf diese Weise wird nicht nur die subjektive wie individuelle Persönlichkeitsentfaltung berücksichtigt.[1246] Gleichermaßen begegnet das Gericht der Ohnmacht aufgrund zunehmender technischer Komplexität. Der Grundrechtsträger kann einzelne Verarbeitungsvorgänge und technische Gegebenheiten

1238 Vgl. *Albers*, DVBl 2010, 1061 (1068); *Herrmann*, GGVIS, S. 129: „Probleme bei der Anwendung ergeben sich somit nicht aus dogmatischen Gesichtspunkten, sondern aus der Klassifizierung der vielfältigen technischen Gerätschaften.“

1239 Zu dieser Problematik in informationeller Hinsicht bereits D.I.1.d)aa)(3).

1240 Dem im Titel enthaltenen Gewährleistungsaspekt kommt keine eigenständige Bedeutung zu; sie ist Grundrechten genuin – *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 29; vertiefend und als bloße Zielstellung des Grundrechts darlegend *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 44 ff. Nunmehr bestätigt durch BVerfG, Beschluss vom 8.6.2021 – Az. 1 BvR 2771/18 –, Rn. 33 f = ZD 2021, 685.

1241 BVerfGE 120, 274 (314).

1242 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 28.

1243 BVerfGE 120, 274 (314, 315).

1244 So auch *Luch*, MMR 2011, 75 (75).

1245 Derart den Begriff der Vertrautheit definierend *Simmel*, Soziologie – Untersuchungen über die Formen der Vergesellschaftung, S. 274.

1246 *Böckenförde*, JZ 2008, 925 (928).

nicht mehr im Einzelnen überblicken und muss auf den subjektiven Eindruck des Systems vertrauen.[1247] Dies bietet die Grundlage für ein erwartetes[1248], systembezogenes Vertrauen[1249]: „Das unspezifische Vertrauen bezieht sich dann generell darauf, daß [sic] jedes dieser Systeme in seiner Spezifikation seinen funktionalen Erwartungen gerecht wird.“[1250] Dies wird je nach Einzelfall durch den Kontrollverlust an Daten verstärkt.[1251] Der These „Vertrauen ‚in die Technik‘ gibt es nicht“[1252] kann daher schon aus den psychologischen Gesichtspunkten nicht zugestimmt werden[1253], die das Urteil des Bundesverfassungsgericht mit der aufgezeigten Attribuierung von Vertrauen aufgreift. Demgemäß ist die Komplexität des Systems qua Vernetzung oder Persönlichkeitsrelevanz der Daten Voraussetzung des Grundrechts und der Vertraulichkeit.[1254]

Dieser subjektive Aspekt des Grundrechts wird durch den objektiven Aspekt der Integrität begrenzt. So ist die Integrität durch den Zugriff auf das informationstechnische System bedroht; „die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems [ist] genommen.“[1255] Sie knüpft ausschließlich an der objektiven Unberührtheit des Systems an[1256], ohne auf subjektiv wahrnehmbare Mängel des Systems (z.B. merkliche Änderung der Reaktionsgeschwindigkeit des Systems, auffälliges Verhalten) einzugehen. Für eine Beeinträchtigung des Grundrechts in dieser Hinsicht reicht das Überwinden

1247 Vgl. *Hoffmann-Riem*, JZ 2008, 1009 (1012 f); *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, S. 148/149. Dementgegen setzt *Luch*, MMR 2011, 75 (76) für die Vertraulichkeitserwartung die Kenntnis des kompletten Datenbestandes voraus.

1248 Im Einzelnen zur Abgrenzung von Vertraulichkeitsinteresse und -erwartungen im Urteil des BVerfG *Sachs*/*Krings*, JuS 2008, 481 (484).

1249 *Hoffmann-Riem*, JZ 2008, 1009 (1012).

1250 Ausführlich zum psychologischen Hintergrund *Wagner*, Zeitschrift für Soziologie 1994, 145 (150 f).

1251 Vgl. *Eichenhofer*, Der Staat 55 (2016), 41 (51).

1252 So *Eichenhofer*, Der Staat 55 (2016), 41 (53) mwN; auch *Hoeren*, MMR 2008, 365 (365).

1253 Im Ergebnis ebenso *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 40 f.

1254 *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 24 f; *Luch*, MMR 2011, 75 (76). Letztlich argumentum e contrario bzgl. BVerfGE 120, 274 (313).

1255 BVerfGE 120, 274 (314).

1256 *Böckenförde*, JZ 2008, 925 (928); vgl. *Luch*, MMR 2011, 75 (75).

der beschriebenen technischen Hürde und der potentielle Zugriff auf die Systeminhalte bereits aus. Der Integritätsschutz setzt damit vor der Erlangung und Verarbeitung der Daten an und verlagert den grundrechtlichen Schutz zeitlich vor.[1257] Insoweit ist es von der informationellen Integrität zu differenzieren, die sich lediglich auf den Erhalt des Informationsgehaltes von Daten bezieht.[1258]

Die einander konträren, nebeneinanderstehenden Schutzkomponenten[1259] sind jedoch nicht voneinander isoliert anzuwenden, sondern beziehen sich aufeinander. Die Integrität des Systems wird durch den Aspekt der Vertraulichkeit subjektiviert und die Verdinglichung des Grundrechts[1260] aufgelöst, indem deren funktionaler Bezug berücksichtigt wird.[1261] Sie beziehen sich letztlich auf dasselbe Schutzgut: Den Schutz des digitalen bzw. technikgerichteten Vertrauens und dahingehender Erwartungen.[1262]

Dennoch ist fraglich, ob der Schutz der Vertraulichkeit und Integrität nicht in den dargestellten gleichnamigen Aspekten der informationellen Selbstbestimmung aufgeht. Das GGVIS stützt sich auf das IT-System im Hinblick auf seine Verwundbarkeit, die durch Ausnutzung technischer Mängel einen Rückgriff auf informationelle bzw. persönlichkeitsrelevante Gehalte des Systems ermöglicht.[1263] Die zur Lösung notwendige Abgrenzung zur informationellen Selbstbestimmung iSd Art. 2 Abs. 1 iVm 1 Abs. 1 GG ist entsprechend diffizil und kreist seit dem Urteil des Bundesverfassungsgerichts um Systeme, die „personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein

1257 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 28; *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 43, ausführlich S. 46 ff; *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, S. 150; *Hoffmann-Riem*, JZ 2008, 1009 (1016); *Böckenförde*, JZ 2008, 925 (928); *Hornung*, CR 2008, 299 (303).

1258 Hierzu sub D.I.1.c).

1259 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 28.

1260 *Hornung*, CR 2008, 299 (302); *Britz*, DÖV 2008, 411 (412); vgl. auch *Eifert*, NVwZ 2008, 521 (522).

1261 *Luch*, MMR 2011, 75 (75); *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 28.

1262 *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 50; *Hoffmann-Riem*, JZ 2008, 1009 (1012); vgl. auch *Berger*, DVBl 2017, 804 (805 f).

1263 Exemplarisch hierzu BVerfG, Beschluss vom 8.6.2021 – Az. 1 BvR 2771/18 –, Rn. 34 ff = ZD 2021, 685.

Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen [...].“[1264] Der damit herausgestellte quantitative Aspekt ist bislang in der Literatur maßgebend.[1265] Formelhaft: Liegt ein Eingriff in ein System zur Erlangung eines großen Datenbestandes vor, ist das GGVIS einschlägig – auch wenn es sich im Kern um eine Erlangung nur einzelner Daten handelt.[1266] Hierin künden sich bereits Abgrenzungsprobleme anhand der Datenmenge an.[1267] Diese sind jedoch derart zu verstehen, dass eine Abgrenzung nicht nur anhand der Quantität erhobener Daten gelingen kann. Bedenkt man den unterschiedlichen Aussagegehalt einzelner Daten nach aktuellem Stand der Technik, mag man das Abwenden von „Daten mit punktuellem Bezug“[1268] in Zweifel ziehen. Je nach Datum und Informationsgehalt kann der punktuelle Bezug durchaus persönlichkeitsrelevant sein, beispielsweise bei Informationen über den Gesundheitszustand auf Basis eines kontinuierlich verwendeten Pulsmessgerätes. Ein Eingriff zur Erhebung dieser Daten unterscheidet sich gemäß dem Urteil des Gerichts bei diesen eindimensionalen informationstechnischen Systemen nicht zu übrigen Eingriffen dieser Art.[1269] Sodann bliebe aber der Integritätsschutz dieser Systeme offen und der lückenschließende Schutz durch das GGVIS selbst lückenhaft. Diese Lücke kann auch das Grundrecht auf informationelle Selbstbestimmung bei Besehen seines persönlichkeitsbezogenen Schutzzwecks nicht ausfüllen. Es dient wie gezeigt[1270] vielmehr der Hoheit und Souveränität über eigene Daten, als dass der datenbezogene Integritätsschutz sich auch auf die Technik erstreckt. Anderenfalls würde das Grundrecht auf informationelle Selbstbestimmung als allumfassendes Digitalgrundrecht verkommen; der datenschutzrechtliche Kern der

1264 BVerfGE 120, 274 (314).
1265 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 23, 24 aE; *Eifert*, NVwZ 2008, 521 (521 f); *Hornung*, CR 2008, 299 (301 f); *Gurlit*, NJW 2010, 1035 (1037); *Hoeren*, MMR 2008, 365 (366).
1266 Vgl. die Faustformel von *Hoffmann-Riem*, JZ 2008, 1009 (1019); *Bantlin*, JuS 2019, 669 (670).
1267 So *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 23, 25; vgl. auch *Kutscha*, NJW 2008, 1042 (1043).
1268 So BVerfGE 120, 274 (313).
1269 Vgl. BVerfGE 120, 274 (313).
1270 Sub D.I.1.d)aa)(3).

Volkszählungsentscheidung und die Auffangfunktion des Allgemeinen Persönlichkeitsrechts des Art. 2 Abs. 1 iVm 1 Abs. 1 GG bliebe unberücksichtigt. Unter Würdigung des im Urteil zur Online-Durchsuchung dargelegten Schutzerfordernisses – „um neuartigen [persönlichkeitsrechtlichen] Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann“[1271] – ist also sowohl der quantitativ wie qualitativ potentielle Aussagegehalt der Daten eines Systems und der Nutzungskontext zu berücksichtigen. Mithin eignet sich das Kriterium der Quantität allein entgegen der h.M. nicht in jedem Fall zur Abgrenzung und bedarf der dargelegten Ergänzung.

Diesem Ansatz kann allerdings (weiterhin) entgegnet werden, dass die Einbeziehung der Qualität für eine erweiterte Verhältnismäßigkeitsprüfung des Grundrechts auf informationelle Selbstbestimmung und gegen die Notwendigkeit des GGVIS spricht.[1272] Würde eine einheitliche und umfängliche Prüfung unter dem Grundrecht auf informationelle Selbstbestimmung erfolgen, würde nicht nur die Prüfungsstruktur des Grundrechts überdehnt[1273], sondern auch dessen Schutzrichtung verkannt[1274]. Wie bereits in informationeller Hinsicht dargelegt[1275], steht das Grundrechtssubjekt und die aktive wie passive Ausübung der Datensouveränität im Mittelpunkt seines grundrechtlichen Schutzes. Sämtliche Fragmente dieses Grundrechts unterstützen oder ermöglichen erst dieses selbstbestimmte Dasein. Weiter gestaltet sich die Gefährdung durch das Verdrängen aus der Position des

1271 BVerfGE 120, 274 (303).

1272 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 23; *Eifert*, NVwZ 2008, 521 (521 f); *Hoeren*, MMR 2008, 365 f; *Sachs*/*Krings*, JuS 2008, 481 (483); krit. auch *Britz*, DÖV 2008, 411 (413 f). Dagegen für eine Notwendigkeit *Böckenförde*, JZ 2008, 925 (928); *Hoffmann-Riem*, JZ 2008, 1009 (1015 ff) sowie vgl. *Hoffmann-Riem*, AöR 134 (2009), 513 (530 f); *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 207 ff; *Herrmann*, GGVIS, S. 85; *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, S. 147 f.

1273 So *Böckenförde*, JZ 2008, 925 (928); *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 204.

1274 Mit ähnlichem Ergebnis auch *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 180 f.

1275 Siehe D.I.1.b).

Datensouveräns. Das GGVIS dagegen legt den Schwerpunkt nur „mittelbar und instrumentell“[1276] auf den Datensouverän. Geschützt ist das informationelle System als Gefäß von Informationen aus menschlichen Interaktionen, seien sie bewusst oder unbewusst (z.B. Telemetrie- und Funktionsdaten)[1277] zugeführt. Es inkorporiert so subjektive Interessen und wird zum Vehikel des Grundrechtsschutzes.[1278] Die charakteristische Gefährdungslage des Grundrechts gestaltet sich vehikelbezogen durch Masseneingriffe, Heimlichkeit bzw. Vertraulichkeitsverletzungen und mangelnde Kenntnisnahme- und Rechtsschutzmöglichkeiten des Grundrechtsträgers.[1279] Das initiierende Urteil des Bundesverfassungsgerichts adressiert schon im Namen die Integrität und Bestandskraft des Systems und übergibt den Schutz und Erhalt dieser komplexen Gefäße dem Staat. Dazu gehört iSe Schutzpflicht auch die Aufgabe, die Verwirklichung von Risiken bei entsprechender Kenntnis – z.B. in Form von bestehenden IT-Sicherheitslücken – zu vermeiden und nach Möglichkeit abzuwenden.[1280] Insofern wird der technisch bestehende Schutzwall[1281] normativ-verfassungsrechtlich gehärtet.[1282] Das Grundrecht auf informationelle Selbstbestimmung weist demgemäß eine deutlich subjektive, den Grundrechtsträger im Zentrum sehende Perspektive auf, während das GGVIS dieses Zentrum umgibt und als Grundlage der Datensouveränität dient.

Die vorangehende Gegenüberstellung zeigt deutlich, dass es keine Gründe für eine mangelnde Notwendigkeit des GGVIS gibt und es ebensowenig durch das Grundrecht auf informationelle Selbstbestimmung zu ersetzen ist. Auch wenn

1276 Vgl. *Eifert*, NVwZ 2008, 521 (522).
1277 BVerfGE 120, 274 (305); *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 32; *Hoffmann-Riem*, JZ 2008, 1009 (1016 f); *Böckenförde*, JZ 2008, 925 (928).
1278 *Böckenförde*, JZ 2008, 925 (928).
1279 BVerfGE 120, 274 (314) sowie Beschluss vom 8.6.2021 – Az. 1 BvR 2771/18 –, Rn. = ZD 2021, 685; *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 178; *Böckenförde*, JZ 2008, 925 (928).
1280 Grundlegend BVerfG, Beschluss vom 8.6.2021 – Az. 1 BvR 2771/18 –, Rn. 34 ff = ZD 2021, 685.
1281 *Hoffmann-Riem*, JZ 2008, 1009 (1017).
1282 *Hornung*, CR 2008, 299 (302).

es berechtigte Gründe eines bestehenden Schutzes der Vertraulichkeit personenbezogener Daten durch die informationelle Selbstbestimmung gibt[1283], begrenzt dies höchstens die Ausrichtung des GGVIS in diesem Punkt. Diese ist jedoch ohnehin, wie eben dargelegt, anderer Natur und deutlich von der Schutzrichtung der informationellen Selbstbestimmung zu differenzieren. Die Verschiedenheit beider Grundrechte und ihre eigenständigen Eingriffsszenarien münden in einem Nebeneinander anstatt einem Subsidiaritätsverhältnis[1284].[1285] In Bezug auf das Allgemeine Persönlichkeitsrecht ließe sich diskutieren, ob GGVIS und informationelle Selbstbestimmung in ihrer dogmatischen Rolle nicht jene der Presse- und Rundfunkfreiheit in Bezug auf die Meinungsfreiheit des Art. 5 Abs. 1 S. 1 Alt. 1 GG aufweisen.[1286] Dies bleibt allerdings abseits dieser Untersuchung zu vertiefen.

Rekurrierend auf die Systemsicherheit als Sicherheit informationstechnischer Systeme, Komponenten und Prozesse bleibt auf die im vorigen Abschnitt erwähnte „Nähe zum GGVIS“ einzugehen.[1287] Die bisherige bzw. aufgezeigte Definition und Abgrenzung zum Grundrecht auf informationelle Selbstbestimmung bestätigt grundsätzlich die Nähe, als dass der im GGVIS enthaltene Technikbezug durch den Integritätsschutz die Grundlagen für eine Berücksichtigung der Mensch-Maschine-Interaktion und -Beziehung in der verfassungsrechtlichen Abwägung bedeutet. Der Systemschutz in seiner informatischen wie einfachgesetzlichen Gestalt löst sich jedoch überwiegend von der Beziehung zum Menschen und legt unabhängig der Systemarchitektur und -verwendung Prinzipien und Vorgaben

1283 *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 23, 24; *Eifert*, NVwZ 2008, 521 (521 f); *Hoeren*, MMR 2008, 365 f; *Sachs*/*Krings*, JuS 2008, 481 (483).

1284 Hierzu *Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, Art. 2, Rn. 24 unter Verweis auf 120, 274 (302); *Eifert*, NVwZ 2008, 521 (522).

1285 *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 208 f, zur Subsidiarität siehe S. 252 ff; *Albers*, DVBl 2010, 1061 (1068); vgl. *Drallé*, GGVIS, S. 146 f. Scheinbar auch *Bantlin*, JuS 2019, 669 (670) und *Luch*, MMR 2011, 75 (76 f). Nur bzgl. Art. 10 Abs. 1 GG kritisch *Britz*, DÖV 2008, 411 (414).

1286 Eine ähnliche Parallele aufzeigend *Luch*, MMR 2011, 75 (76).

1287 Sub D.II.3.

sicherer Systeme fest. Die sowohl nach § 2 Abs. 2 BSI-G als auch in der Informatik[1288] vertretenen Prinzipien der Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen beziehen sich auf das System als solches und als Informations- bzw. Datenverarbeitungs- und -speicherort. Ob und wann, wie und wo personenbezogene Daten verarbeitet werden, ist für die Anwendung dieser Aspekte und Herstellung dieser Systemsicherheit irrelevant.[1289] Diese weite Formulierung führt lediglich dazu, dass IT-Systeme mit Persönlichkeitsrelevanz durch diesen Schutz ebenfalls betroffen sind. Die systemspezifischen Besonderheiten, wie z.B. der potentielle Verarbeitungszweck und -umfang in Relation zur persönlichkeitsbezogenen Aussagekraft der Daten, finden vielmehr ihm Rahmen einer Verhältnismäßigkeitsprüfung Anklang. Ähnliche Parallelen zeigen sich im Schutz kritischer Infrastrukturen, die im Gesundheitsbereich auch besondere personenbezogene Daten (vgl. Art. 9 Abs. 1 DSGVO) und dahingehende besondere Verarbeitungssituationen mittelbar-technisch berücksichtigen.[1290] Folglich schließt die Systemsicherheit die Schutzrichtung des GGVIS ein, entspricht dieser jedoch nicht aufgrund der durch das Bundesverfassungsgericht und Art. 2 Abs. 1 iVm 1 Abs. 1 GG verkörperten Nähe zum Persönlichkeitsrecht. Das GGVIS dient damit nicht dem Schutz jeglicher IT-Systeme[1291], auch wenn faktisch die überwiegende Anzahl genutzter Systeme Telemetrie- und Funktionsdaten erhebt und die Möglichkeit einer digitalen Identität – ergo auch der Persönlichkeitsrelevanz iSd GGVIS – gegeben ist.

In dieser Krux kündigt sich bereits der Schutz der digitalen Identität durch das GGVIS an: Die weite Definition der digitalen Identität, die nicht nur prima facie personenbezogene Daten einbezieht, erschöpft sich im Schutz potentiell persönlichkeitsrelevanter Systeme. Soweit die auf einem eigengenutzten System entstehende digitale Identität durch personenbeziehbare Daten geprägt ist, genießt die technische Umgebung des Datenkonstrukts den Schutz des GGVIS. Der Hinweis

1288 Siehe nur *Eckert*, IT-Sicherheit, S. 7 ff.
1289 Vgl. zur Definition der IT-Security *Eckert*, IT-Sicherheit, S. 6.
1290 Hierzu vgl. *Kraaibeek*, Sicherung kritischer Infrastrukturen im Gesundheitswesen, 79 (81 ff).
1291 So auch *Hoffmann-Riem*, AöR 134 (2009), 513 (531); *Herrmann*, GGVIS, S. 126. Dementgegen die Verformung zum „apersonalen technikorientierten Grundrecht“ ankündigend *Eifert*, NVwZ 2008, 521 (522).

des Bundesverfassungsgerichts auf durch den Nutzer nicht bewusst erzeugte Daten in Bezug auf „sein Verhalten und seine Eigenschaften“[1292] deutet jedoch an, dass auch die erst aufgrund der Vernetzung oder bei näherer Analyse entstehenden digitalen Identitäten vom Schutzbereich umfasst sind. Die daraus resultierende Grundvoraussetzung einer datenerzeugenden Mensch-Maschine-Interaktion ist folglich in Bezug auf die digitale Identität stets gegeben. Der grundrechtliche Schutz erstreckt sich jedoch nur auf die dargestellte vertrauens- und systembezogene Schutzrichtung; sie ergänzt damit den bestehenden Schutz durch das Grundrecht auf informationelle Selbstbestimmung. Umgekehrt schließt der durch das Gericht vorausgesetzte potentielle Personenbezug Systeme aus, die sich durch eine mangelnde Datenerfassung auszeichnen und keine digitale Identität inkorporieren. Erst, wenn die Datenerfassung durch die Manipulation des fraglichen Systems und die Erstellung einer Identität erreicht wird, können Vertraulichkeitserwartung und -interesse grundrechtlich aufgefangen werden. Darüber hinaus kommt der objektivrechtliche Schutz[1293] des Grundrechts dem Schutz der digitalen Identität zugute: Das von *Eifert* geforderte Szenario für die Begründung des GGVIS – ein „realistisches, persönlichkeitsrelevantes, eigenständiges Gefahrenpotenzial für die Integrität der technischen Systeme“[1294] – findet sich nunmehr in der Ausnutzung von Schwachstellen in IT-Systemen zur Durchführung geheimdienstlicher oder polizeilicher Maßnahmen, konkret der Quellen-Telekommunikationsüberwachung oder der Online-Durchsuchung[1295]. Insoweit erstreckt sich die Schutzpflicht des Staates, derartige Beeinträchtigungen von IT-Systemen fernzuhalten[1296], auch auf digitale Identitäten.

Der mittelbare, grundrechtliche Schutz digitaler Identitäten durch den Schutz des eigengenutzten informationstechnischen Systems ist folglich durch das GGVIS gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG gegeben, soweit das System potentiell

1292 BVerfGE 120, 274 (305).
1293 Vertiefend *Taraz*, GGVIS und Gewährleistung digitaler Privatheit, S. 156 ff; *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, S. 209 ff.
1294 *Eifert*, NVwZ 2008, 521 (522).
1295 Hierzu *Derin*/*Golla*, NJW 2019, 1111 (1114 f).
1296 So auch *Derin*/*Golla*, NJW 2019, 1111 (1114 f). In abstrakten Zielstellungen präventiver verbleibend *Heinemann*, Grundrechtlicher Schutz informationstechnischer Systeme, S. 211 ff.

quantitativ und/oder qualitativ Aussagen über den Inhaber der digitalen Identität enthält.

5. Conclusio der technischen Betrachtung

Die vorangehende Betrachtung zeigt, dass der Verfassung nicht nur ein subjektbezogener Schutz innewohnt. Die Grundrechte der Art. 13 Abs. 1, 10 Abs. 1 Var. 3 und 2 Abs. 1 iVm 1 Abs. 1 GG weisen auch einen Vertrauensschutz auf, der sich im technischen Kontext als Annex zum Grundrechtssubjekt auf Güter und Beziehungen zu Dritten darstellt. Im Falle der Unverletzlichkeit des Wohnraumes des Art. 13 Abs. 1 GG gelingt dies durch die Berücksichtigung subjektiver Vertraulichkeitsinteressen, die durch die Räumlichkeit objektiviert werden und so Schutz erlangen. Ähnlich verkörpert ist die Kommunikation des Fernmeldegeheimnisses des Art. 10 Abs. 1 Var. 3 GG, wenngleich fernmeldetechnische Vorgänge sich durch elektromagnetische, nicht physisch wahrnehmbare, Signale auszeichnen. Hierbei wird die Individualkommunikation für einen breiteren Kreis an Dritten auf technischer Ebene wahrnehmbar, setzt jedoch ein Vertrauen in die Garantie einer Geheimheit und Sicherheit der Kommunikation durch den Dritten voraus. Schutzgegenstand ist daher die Vertraulichkeit der Kommunikationsinhalte und -umstände, die durch einen vertrauenswürdigen Dritten und damit außerhalb des eigenen Herrschaftsbereiches zu sichern ist. Artikel 2 Abs. 1 iVm 1 Abs. 1 GG schützt das Vertrauen dagegen personenbezogen: Das Grundrecht auf informationelle Selbstbestimmung berücksichtigt die Vertraulichkeit der Daten nicht nur informationell, sondern auch iSe Datensicherheit. Dieser Aspekt ist Teil des Grundrechts und ergänzt die technische Lesart des Schutzes personenbezogener Daten, indem die Selbstbestimmtheit auch technisch verstanden wird. Sodann sind auch die Vertraulichkeit und Integrität personenbezogener Daten Teil der Selbstbestimmung, soweit die Überprüfbarkeit durch den Diensteanbieter – in den zu vertrauen ist – gewährleistet wird. Soweit sich diese Aspekte aber aufgrund technischer Komplexität des potentiell persönlichkeitsrelevanten Systems eigenen Schutzmaßnahmen und der Datensouveräntität entziehen, kommt das GGVIS als technikbezogener Schutz in Betracht. Die Vertraulichkeit setzt sich hier aber

nicht in Beziehungen zu Diensteanbietern als Datenverarbeitende, sondern als das System als Datenspeicher- und verarbeitungsort fort. Der verfassungsrechtliche Vertrauensschutz durchzieht damit alle technischen bzw. technikbezogenen Vorgänge, die vom Grundrechtssubjekt regelmäßig nicht überblickt und kontrolliert werden können.

Die digitale Identität findet in dieser Betrachtung nur bedingt Schutz. Während dieses immaterielle Datenkonstrukt sich nicht im Schutz der räumlichen Privatheit des Art. 13 Abs. 1 GG wiederfindet, ist sie mittelbar vom Fernmeldegeheimnis des Art. 10 Abs. 1 Var. 3 GG umfasst. Dieser Schutz gilt nicht nur für die je nach Dienstleistung notwendigen digitalen Identitäten, sondern auch die mit Kommunikationsvorgängen einhergehenden Umstände der Kommunikation. Konkreter schützen die eigenständigen Grundrechte des Art. 2 Abs. 1 iVm 1 Abs. 1 GG die digitale Identität, indem sie die den zu schützenden Gegenstand zweiseitig flankieren: Der Schutz der informationellen Selbstbestimmung in seiner technischen Lesart schließt auch die digitale Identität ein. Die enthaltene Datensicherheit stellt dabei besonders präventive Mittel und die Prinzipien des Privacy by Design und Default heraus. Das Grundrecht erhält so den Fokus der Selbstbestimmung, der auch in Richtung eines technischen (Selbst-)Schutzes zu verstehen ist. Das GGVIS fängt dagegen im Vorfeld der eigentlichen Datenaggregation zu einer digitalen Identität auch jene Systeme auf, die sich potentiell zur Erstellung einer Identität bei Einsichtnahme eignen. Zur Bestimmung dieser bedarf es jedoch der Berücksichtigung der Quantität und Qualität, um einen die informationelle Selbstbestimmung ergänzenden Schutz zu gewährleisten. Andernfalls bliebe der Schutz der personenbezogenen Systemsicherheit iSd Grundrechts für eindimensionale Systeme offen, obschon sie Daten mit einem hohen Risiko für die Persönlichkeit bergen.

III. Zusammenfassung

So faccettenreich die digitale Identität (B.) und das verfassungsrechtliche Schutzkonzept im Allgemeinen (C.) auch sind, so lässt sich der konkrete Schutz im

Ergebnis auf bekannte und bewährte Grundrechte reduzieren. Sowohl auf informationeller als auch technischer Ebene stellt Art. 2 Abs. 1 iVm 1 Abs. 1 GG durch seine konkretisierten, eigenständigen Grundrechte den Mittelpunkt der digitalen Identität dar. Dies ist vorhersehbar, wenn es (überwiegend) ein Konstrukt personenbezogener Daten zu untersuchen gilt.

Dennoch besticht dieses Kapitel durch die aufgezeigten Zwischentöne. So konnte für natürliche Personen gezeigt werden, dass die Anonymität bzw. anonyme und anonymisierte Daten eine besondere Variante der digitalen Identität darstellen. Diese findet prima facie keinen Schutz im Grundrecht auf informationelle Selbstbestimmung, erlangt ihn jedoch auf den zweiten Blick als dessen manifestierter status negativus. Weiter ist diese Variante als Teil der sphärenbezogenen Bewertung digitaler Identitäten von besonderer Bedeutung. Bei diesem Maßstab, der sowohl Quantität als auch Qualität des Aussagegehaltes von Daten und Datensammlungen berücksichtigt, ist diese Variante der Gegensatz zum öffentlich einsehbaren Klardatum. Die an der Sphärentheorie angelehnte Betrachtungsweise durchdringt letztlich das einfachgesetzliche Datenschutzrecht in vielerlei Hinsicht und dient im Besonderen als verfassungsrechtliche Leitlinie für die Verhältnismäßigkeit bzgl. aggregierter Datensätze. Juristische Personen können auf diesen Maßstab mangels einer Menschenwürde iSd Art. 1 Abs. 1 GG nicht zurückgreifen. Dieser Malus ist auf Art. 19 Abs. 3 GG zurückzuführen. Ungehindert dessen schützt Art. 2 Abs. 1 GG als Kulminationspunkt sowohl die Geschäftsehre juristischer Personen als auch ihre informationelle Selbstbestimmung. In letzterem Fall ist der Schutzgegenstand jedoch nicht die Gesamtheit personenbezogener Daten der Mitarbeiter, sondern jede betriebsbezogene Information, die nicht von spezielleren Schutzbereichen umfasst ist. Der jeweilige informationelle Schutz läuft in der systembezogenen Lesart des Art. 2 Abs. 1 iVm 1 Abs. 1 GG – dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – zusammen. Der darin bestehende Vertraulichkeitsschutz gegenüber dem eigens genutzten informationstechnischen System gilt für beide Grundrechtssubjekte, soweit sich aufgrund des Einsatzzwecks darin potentiell ein entsprechendes Substrat der Persönlichkeit befindet. Angesichts der Durchdringung des Alltags mit digitalen Begleitern und weiterer Informationstechnik hat

dieses Grundrecht an Bedeutung und Schutzweite gewonnen. Als systemschützendes Grundrecht dient es jedoch nur der Systemsicherheit als solches, während die Datensicherheit durch das Grundrecht auf informationelle Selbstbestimmung aufgefangen wird. Gemeinsam bilden sie sowohl ein inneres (datenmäßiges) wie äußeres (systemgerichtetes) Schutzkonzept.

Die Reichweite des Art. 2 Abs. 1 iVm 1 Abs. 1 GG ist allerdings erst zu adressieren, wenn sich entsprechende spezielle Schutzkonzepte nicht eignen oder nur unzureichenden Schutz bieten. Leider war dies für die übrigen dargestellten Grundrechte allumfassend gegeben. So kommt natürlichen Personen kein Eigentumsschutz an den „eigenen" Daten gem. Art. 14 Abs. 1 S. 1 Alt. 1 GG zu. Ein Konzept der Datenarbeit ist aufgrund der Beschränkung durch geltendes Datenschutzrecht und die informationelle Selbstbestimmung nur bedingt durch die Berufsfreiheit des Art. 12 Abs. 1 GG geschützt. Der digitalen Identität juristischer Personen kommt dagegen ein Schutz aus Art.12 Abs. 1 und 14 Abs. 1 GG zu. Im Lichte des Art.19 Abs. 3 GG schützt Art. 12 Abs. 1 GG schwerpunktmäßig die wirtschaftliche Betätigungsfreiheit und damit höchstens Teilaspekte in der Konstruktion der digitalen Identität. Das Recht am eingerichteten und ausgeübten Gewerbebetrieb des Art. 14 Abs. 1 GG betrifft dagegen nur den Bestand des Unternehmens als Ganzes, schützt höchstens mittelbar die digitale Identität. In technischer Hinsicht findet sie hingegen keinen Schutz in der Unverletztlichkeit des Wohnraumes des Art. 13 Abs. 1 GG. Das Fernmeldegeheimnis des Art. 10 Abs. 1 Var. 3 GG kann dagegen nur temporären Schutz für die Dauer des Kommunikationsvorgangs sowie damit einhergehende Metadaten gewähren.

In aller Kürze: Die digitale Identität findet auch konkreten verfassungsrechtlichen Schutz in den dargestellten Grundrechten.

E. Lückenhafter Schutz? – Zusammenfassung und Ausblick

Jeder hat das Recht auf den Schutz seiner Daten
und die Achtung seiner Privatsphäre.
– Art. 7 Abs. 1, Charta der digitalen Grundrechte (2018)

Unter Würdigung der vorangehenden Kapitel bleibt nun zu untersuchen, ob der in einem Rekurs aufgezeigte Schutz der digitalen Identität auch Verästelungen einfachgesetzlicher Art de lege lata ausgebildet hat oder sich de lege ferenda eine Erweiterung abzeichnet. Schlussendlich ist ein Blick von der Gegenwart in die Zukunft der digitalen Identität zu wagen.

I. Abschließende verfassungsrechtliche Betrachtung

Die Kapitel B. bis D. zeigen den umfassenden, materiellen Schutz der digitalen Identität. Das Datenkonstrukt, das sich aus einzelnen Attributen bildet und entweder selbst als Identifier fungiert (dann Quasi-Identifier) oder mit einem solchen verknüpft ist, erweist sich als vielgestaltig und grundrechtssubjekt-neutral. Ebenso breit bzw. multidimensional ist das verfassungsrechtliche Schutzkonzept, das aufgrund seiner allgemeinen Ausgestaltung für besagte Vielgestaltigkeit gewappnet ist. Dies bestätigt sich nicht nur in den verschiedenen Anwendungsfällen digitaler Identitäten und der Gegenüberstellung mit den grundrechtlichen Schutzrichtungen, sondern auch in concreto in grundrechtlich geschützten Handlungsweisen.

Als Basisnorm fungiert hier Art. 2 Abs. 1 iVm 1 Abs. 1 GG, sowohl in Bezug auf technische wie informationelle Aspekte digitaler Identitäten. Natürliche Personen können sich auf das Grundrecht der informationellen Selbstbestimmung berufen, das aus dargelegten Gründen um eine rechtliche Würdigung der Daten-Qualität und -Quantität im Rahmen der Verhältnismäßigkeit zu erweitern ist. Denn auch hier ist die Sphärentheorie für eine Einordnung des Informationsgehaltes in qualitativer und quantitativer Hinsicht nutzbar zu machen. Für juristische Personen ist die verfassungsrechtliche Grundlage um den menschlichen Aspekt des Art. 1 Abs. 1 GG zu kürzen und beschränkt auf den betriebsbezogenen Kontext wie die Geschäftsehre oder weitere Daten mit Unternehmensbezug gem. Art. 2 Abs. 1 GG. Letztere werden nur bedingt von den üblicherweise der Unternehmenspersönlichkeit dienenden Art. 12 Abs. 1, 14 Abs. 1 GG geschützt. Wenn auch diese Kürzung zu einem anderen Betrachtungswinkel führt, so steht der Schutz dieser artifiziellen digitalen Identität jener persönlichkeitsgeprägten Variante natürlicher Personen kaum nach. Der systembezogene Schutz beider Grundrechtssubjekte auf dem Boden des GGVIS , der sich aus dem in das informationstechnische System investierte Vertrauen speist und datenunabhängig den Bestand und die Zuverlässigkeit der technischen Infrastruktur umfasst.

Die für diese Arbeit grundlegende Frage, ob und in welcher Form die digitale Identität grundrechtlich geschützt ist, ist hiermit positiv zu beantworten und im Einzelnen dargelegt.

II. Einfachgesetzlicher Schutz de lege lata

Rekurs nehmend auf die ausführliche Darstellung bleibt nun zu reflektieren, inwieweit die aufgezeigten verfassungsrechtlichen Schutzrichtungen bereits einfachgesetzlich aufgefangen sind. Dadurch sollen mögliche Lücken aufgezeigt werden, die dann zwecks Erfüllung staatlicher Schutzpflichten in Korrekturansätzen münden könnten.

Der Schutz der digitalen Identität natürlicher Personen ist durch die bestehenden Gesetze weitestgehend abgedeckt. Das Datenschutzrecht bezieht sich als solches wie gezeigt nur auf personenbezogene (Einzel-)Daten, erstreckt sich aber mittelbar auch auf aggregierte Datensätze – beispielsweise durch das Gebot der Datensparsamkeit gem. Art. 5 Abs. 1 lit. c DSGVO oder mittels risikobasierter Betrachtungsweise (vgl. ErwGr 76 DSGVO). Inwieweit die jeweilige digitale Identität ihrem Aussagegehalt und ihrer Persönlichkeitssphäre nach vom Schutz umfasst ist, ist einzelfallabhängig zu bestimmen. Problematisch bleibt weiterhin die Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Daten. Aus Richtung des Datenschutzrechts ist angesichts Erwägungsgrund 26 DSGVO keine Lösung zu erwarten. Die mangelnde Definition oder sonstige legislative Regulierung (Standards, exemplarische Aufzählungen, Abstufungen je besonderer Verarbeitungssituation wie etwa für Wissenschaft und Forschung) des risikobasierten Ansatzes an der Schwelle zwischen pseudonymen und anonymisierten Daten trägt hierzu maßgeblich bei. In zeitlicher Hinsicht kann das Regelungskonstrukt aus DSGVO und BDSG ebenso nicht überzeugen, wo lt. Erwägungsgrund 27 DSGVO keine Anwendung auf Daten Verstorbener erfolgt. Der Lebenszyklus-Aspekt digitaler Identitäten ist damit in pränataler wie postmortaler Hinsicht nicht reflektiert. Postmortal kann sich lediglich auf persönlichkeitsrechtliche Aspekte gem. § 823 Abs. 1 BGB iVm Art. 2 Abs. 1 iVm 1 Abs. 1 GG berufen werden. Dass es darüber hinaus an einer einfachgesetzlichen Regelung eines Dateneigentums mangelt, ist dagegen aus dargelegten Gründen[1297] nicht zu beanstanden. Weiter kann das Netzwerkdurchsetzungsgesetz in seiner persönlichkeitsrechtlichen Schutzrichtung[1298] (vorerst) keine Relevanz für die digitale Identität entfalten.

Juristischen Personen kommt im Rahmen dieser Arbeit nicht schon aufgrund anderer Grundrechte eine Sonderstellung zu. Auch auf einfachgesetzlicher Ebene sind die Regelungen zum Schutz der digitalen Unternehmenspersönlichkeit eher begrenzt. Die einführende Definition sowie die Einordnung zwischen Art. 12 Abs. 1, 14 Abs. 1 und 2 Abs. 1 iVm 1 Abs. 1 GG wird lediglich in der Literatur

1297 Sub D.I.1.d).

1298 Vgl. *Spindler*, GRUR 2018, 365 ff; *Hoven/Gersdorf* in: Gersdorf/Paal, BeckOK InfoMedienR, § 1 NetzDG, Rn. 4.

diskutiert. Regelungen, die typischerweise dem Schutz des verfassungsrechtlichen Persönlichkeitsrechts zuzuordnen sind – beispielsweise das Kunsturhebergesetz – sind aufgrund besagter Prägung nur natürlichen Personen zugänglich; hier verdrängt die einfachgesetzlich verkörperte Menschenwürde des Art. 1 Abs. 1 GG die unternehmerischen Interessen juristischer Personen iSd Art. 19 Abs. 3 GG. Einen Hoffnungsschimmer mag man im bereits referenzierten Geschäftsgeheimnisgesetz erkennen, da dieses zumindest Aspekte des Unternehmens aus Art. 14 Abs. 1 GG berücksichtigt.[1299] Hierin sind jedoch keine Regelungen eines detaillierten Unternehmenspersönlichkeitsrechts zu erkennen.

In technischer Hinsicht sind die betroffenen Interessen nicht durch ein übergeordnetes, allgemeines Gesetz aufgefangen. Das BSI-Gesetz sowie damit verknüpfte Änderungsgesetze und -regelungen (IT-Sicherheitsgesetz 1.0 und 2.0; nationales Umsetzungsgesetz der NIS-Richtlinie) beziehen sich schon qua Anwendungsbereich überwiegend auf die „Sicherheit der Informationstechnik des Bundes“. Nur vereinzelt greift das Gesetz seine fördernde Rolle gem. § 3 Abs. 1 S. 1 BSI-G auf, indem sich generell der „Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik“[1300] und der „Forschung im Rahmen gesetzlicher Aufgaben“[1301], weiter aber „Beratung und Warnung [...] der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen“[1302]. Im Übrigen regelt das Gesetz grundlegend das Pflichtenkorsett für kritische Infrastrukturen iSd § 2 Abs. 10 und digitale Dienste gem. § 2 Abs. 11 BSI-G. Der Schutz der IT-Sicherheit kann daher nur bereichsspezifisch gefunden werden, wobei das IT-Sicherheitsgesetz in seiner Form als Artikelgesetz als Wegweiser dienen kann – verweisend auf Art. 4 (Telemediengesetz) und 5 (Telekommunikationsgesetz) IT-SiG. So fanden sich in § 13 Abs. 7 TMG a.F. grundlegende technische Anforderung an Telemedienanbieter zum Schutz der technischen Infrastruktur (S. 1 Nr. 1 und Nr. 2 lit. b) und der personenbezogenen Daten der

1299 Hierzu sub D.I.2.c).
1300 § 3 Abs. 1 S. 2 Nr. 3 BSI-G.
1301 § 3 Abs. 1 S. 2 Nr. 1 BSI-G.
1302 § 3 Abs. 1 S. 2 Nr. 14 BSI-G.

Nutzer (S. 1 Nr. 2 lit. a) durch technische und organisatorische Vorkehrungen. Erstere sind nun in § 19 Abs. 4 TTDSG integriert. Die Variante des § 13 Abs. 7 S. 1 Nr. 2 lit. a TMG a.F. wird durch die spezielleren Vorschriften der Art. 25, 32 DSGVO verdrängt. Das Telekommunikationsgesetz in alter Fassung enthielt dagegen Regelungen zu Maßnahmen der Informationssicherheit bzgl. der Übertragungsleistung und/oder dem Schutz der Telekommunikationsinfrastruktur als Teil des bereichsspezifischen Dateschutzrechts in Teil 7. Dieses wurde nunmehr in seinem rein datenschutzrechtlichen Kern in dasTTDSG überführt; die rein infrastrukturbezogenen, technischen Schutzmaßnahmen verblieben dagegen im TKG und wurden in §§ 165, 169 TKG übernommen. Die Absätze des § 165 TKG bilden die Grundlage für eine Schutzkonzept von Telekommunikationsanlagen, bestehend aus einer allgemeinen Pflicht zu technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses (Art. 10 Abs. 1 GG) und von personenbezogenen Daten (Art. 2 Abs. 1 iVm 1 Abs. 1 GG) über besondere Pflichten für öffentliche Telekommunikationsnetze ergänzt durch eine Pflicht zur Vorlage eines Sicherheitskonzepts gem. §§ 166 Abs. 1, 167 TKG. Letzteres kann sich an dem gem. § 167 TKG von BNetzA, BSI und BfDI erarbeiteten Katalog von Sicherheitsanforderungen orientieren; der Katalog ist nicht verpflichtend[1303]. Netzbezogene Beeinträchtigungen sind gem. § 168 TKG unverzüglich zu melden. Persönlichkeitsbezogene bzw. die Beeinträchtigung des Schutzes personenbezogener Daten betreffende Meldungen richten sich dagegen gänzlich nach § 169 TKG. Die „bloße“ Verletzung verpflichtet zu einer Meldung ggü. der BNetzA sowie dem BfDI. Bei Verletzungen, durch die Personen „schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt“[1304] werden, ist dagegen die betroffene Person selbst mit den Angaben gem. Abs. 2 in Kenntnis zu setzen. Vollumfänglich bildet § 169 TKG damit das Informationsschema der Art. 33, 34 DSGVO ab, einschließlich einer risikoabhängigen Informationspflicht. Schließlich entfällt auch nach § 169 Abs. 1 S. 3 TKG die Informationspflicht, sofern

1303 Vgl. gibt die Begründung des Gesetzesentwurfes hierüber keinen Aufschluss – BT-Drs. 18/4096, S. 36.

1304 § 169 Abs. 1 S. 2 TKG.

hinreichende Schutzmaßnahmen nachweislich unternommen wurden oder gem. § 169 Abs. 1 S. 2 TKG ein nicht-schwerwiegender Fall vorliegt.

Die allerorts vorgegebenen Informations- bzw. Warnpflichten münden jedoch nicht zwangsläufig in einem besseren Schutzstandard, welcher der angedeuteten Erfüllung der Schutzpflicht aus dem GGVIS[1305] dient. Alle erwähnten Gesetzeswerke – BSI-G, TMG, TKG, TTDSG und DSGVO – verweisen auf einen Stand der Technik hinsichtlich der technischen und organisatorischen Maßnahmen. Die bloße Orientierungswirkung des Kataloges nach § 167 TKG sowie dem IT-Grundschutz-Katalog kann hierüber nicht hinweghelfen. Gemein ist den Begriffen ein Einbeziehen (branchen-)etablierter Schutzstandards[1306], die zumeist nachträglich in diese Kataloge aufgenommen werden. Auch zeigt sich ein (soweit berechtigtes) differenziertes Schutzniveau zwischen kritischen Infrastrukturen und privaten Endgeräten. Es bleibt jedoch zu fragen, ob letztere nicht als Angriffsvektor für derartige oder andere relevante Infrastrukturen dienen können. Die datenschutz- und IT-sicherheitsfreundliche Konstruktion von Hard- und Software ist insoweit nicht beaufsichtigt.[1307] So hat das BSI gem. §§ 7, 7a, 3 Abs. 1 S. 2 Nr. 14 und 14a BSI-G nur die Fähigkeit, also keine Pflicht, sich mit den implementierten technischen Standards in Endgeräten auseinanderzusetzen. In Relation zu den übrigen Aufgaben des § 3 BSI-G gerät diese Aufgabe ins Hintertreffen, steht die Sicherheit der Informationstechnik des Bundes doch im Mittelpunkt.

Insofern bleibt ein, wenn auch punktueller, Korrekturbedarf sowohl in datenschutzrechtlicher wie IT-sicherheitsrechtlicher Hinsicht erhalten. Datenschutzrechtlich bedarf es einer Begriffsklärung hinsichtlich der Anonymität und ein klareres Rechtskonstrukt zum Erhalt dieses Zustands in Relation zum (personenbezogenen) Datenschutzrecht. IT-sicherheitsrechtlich besteht ebenso der Bedarf nach einheitlichen Standards, die zumindest ein unteres Niveau an IT-Sicherheit

1305 Sub D.II.4.

1306 *Hladjk* in: Ehmann/Selmayr, DSGVO, Art. 32, Rn. 5; *Jandt* in: Kühling/Buchner, DSGVO, Art. 32 DSGVO, Rn. 10; *Hansen* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 32 DSGVO, Rn. 22 f; *Ekrot/Fischer/Müller* in: Kipker, Cybersecurity, § 3, Rn. 5, 8 ff.

1307 Vgl. *Vettermann*, BSI-Sicherheitstest revisited: Besserer Schutz durch DSGVO und Co. möglich?, S. 253 (259 f).

aus Verbrauchersicht garantieren. Dies betrifft insbesondere Endgeräte, die nicht vordergründig personenbezogene Daten bearbeiten (z.B. Router).[1308] Besagte Standards sollten auch entsprechend transparent aufbereitet und kommuniziert werden, um das Technikbewusstsein der Nutzenden zu fördern. Beide Forderungen münden in selbiger Zielstellung: Ein einheitliches Schutzniveau.

III. Korrekturansätze de lege ferenda

Insofern bleibt die Sachlage de lege ferenda zu betrachten und die geplanten Änderungen von Gesetzen oder ähnliche Korrekturbestrebungen zugunsten eines erweiterten einfachgesetzlichen Schutzes hin zu prüfen.

1. Datenstrategische Vorhaben von Bund und EU

Zuvorderst ist sich der nunmehr umgesetzten Änderung in Form des Zweiten Datenschutzanpassungs- und Umsetzungsgesetz (2. DSAnpUG) zu widmen. Dieses Artikelgesetz hat zur Aufgabe, allgemeine wie spezialgesetzliche datenschutzrechtliche Vorschriften anzupassen und ein harmonisches Verhältnis zwischen nationalem und europäischem Datenschutzrecht herbeizuführen. Vornehmlich werden hierzu Begriffsbestimmungen, Verweisungen und Rechtsgrundlagen angepasst.[1309] Hinsichtlich des Bundesdatenschutzgesetzes ist lediglich die Erweiterung der Rechtsfertigungsgründe zur Verarbeitung besonderer personenbezogener Daten um die zwingend erforderliche Verarbeitung „aus Gründen eines erheblichen öffentlichen Interesses“, § 22 Abs. 1 Nr. 1 lit. d BDSG. Mit Blick auf das gleichermaßen geänderte BSI-Gesetz und der dortigen Einfügung in § 3 S. 1 BSI-G – „im öffentlichen Interesse liegende Aufgaben“ – lässt sich die unter anderem dort genutzte Öffnungsklausel des Art. 6 Abs. 3 S. 1 lit. b, Abs. 1 lit. e DSGVO

1308 *Vettermann*, BSI-Sicherheitstest revisited: Besserer Schutz durch DSGVO und Co. möglich?, 253 (260).

1309 BT-Drs. 19/4674, S. 2.

erkennen. Diese Annahme stützen auch die weiteren eingefügten Vorschriften des BSI-G, welche die Verantwortlichkeit des BSI für die Verarbeitung personenbezogener Daten regeln (§§ 3a, 6a-6f BDSG). Dennoch sind die Änderungen durch das 2. DSAnpUG marginal und bereiten keine zukünftigen Änderungen in begrifflicher oder systematischer Hinsicht vor. Dass die durch die DSGVO überflüssig gewordene Regelung des § 13 Abs. 7 S. 1 Nr. 2 lit. a TMG a.F. nicht gestrichen worden ist, mag die mangelnde Weitsicht belegen. Zumindest ist nicht davon auszugehen, dass zum Erlass am 20.11.2019 bereits Einzelheiten des TTDSG und damit die Überarbeitung der Regelung bekannt war.

Perspektivisch sind daher die Datenstrategien der Akteure – also Bund und EU – in den Blick zu nehmen. Schließlich zeigen diese die Planung gesetzgeberischer Vorhaben sowie anderer staatlicher Programme an und enthalten dementsprechend legislative Korrekturansätze. Zu beachten ist jedoch, dass sich beide zum Stand der Untersuchung im Konsultationsverfahren befinden und daher nur eine Indizwirkung von ihnen ausgeht.

Das Eckpunkte-Papier zur Datenstrategie der (ehemaligen) Bundesregierung vom 18.11.2019[1310] sieht das „enorme Innovationspotenzial“ im Fokus. „Damit eng verbunden sind immer auch Fragen des verantwortungsvollen Umgangs mit den Möglichkeiten und Risiken sich stetig weiterentwickelnder Technologien der Datengenerierung, -sammlung und -auswertung. Es gilt also, die Chancen zu nutzen und zugleich die Wahrung grundlegender Werte, Rechte und Freiheiten unserer Gesellschaft zu gewährleisten.“[1311] Für den Schutz digitaler Identitäten bedarf es dementsprechend dem Erhalt bestehenden und der Erweiterung des dargestellten Schutzkreises, insbesondere um die Zielstellung des „selbstbestimmt[en], kompetent[en], unabhängig[en] und sicher[en]“ Individuums aufrechtzuerhalten. Positiv fällt auf, dass sich die Strategie sowohl mit nicht-personenbezogenen als auch personenbezogenen Daten befasst.

1310 Nachfolgend bezeichnet als Eckpunkte-Papier Datenstrategie. Das Dokument ist abrufbar unter https://www.bundesregierung.de/resource/blob/997532/1693626/e617eb58f3464ed13b8ded65c7d3d5a1/2019-11-18-pdf-datenstrategie-data.pdf.

1311 Eckpunkte-Papier Datenstrategie (Fn. 1310), S. 1.

Dass die Bundesregierung hierbei gleichermaßen den Schutz der informationellen Selbstbestimmung, von Geschäfts- und Betriebsgeheimnissen sowie Datenschutzrecht und Datensicherheit gewährleisten will[1312] reflektiert letztlich die dargelegte Bandbreite digitaler Identitäten natürlicher und juristischer Personen. In den einzelnen, angedeuteten Maßnahmen lässt sich dieser Ansatz nur mittelbar erkennen und dient als Prämisse für die Pläne zur Datenbereitstellung/-zugang und Datennutzung. Das Ziel der datengetriebenen Gesellschaft steht hier im Vordergrund, sei es bei der Evaluation von Anreizsystemen für eine gemeinwohlorientierte Datennutzung oder dem Auf- und Ausbau wettbewerbsfähiger und nachhaltiger Dateninfrastrukturen. Erwähnenswert ist aber der Aspekt, die Forschung durch „sichere und neue Methoden zur Anonymisierung und Pseudonymisierung" zu unterstützen.[1313] Hierin könnte die Bestrebung zu erkennen sein, die geforderten Mindeststandards zu etablieren oder rechtlich zu implementieren und neue Ansätze z.B. im Rahmen von Forschungsprojekten zu unterstützen. Ersteres ist angesichts der Förderung der Datennutzung durch „untergesetzliche Maßnahmen wie z.B. Förderungen, Normungen (Sicherheits-)Standards, Muster und Verhaltenskodizes (codes of conduct)"[1314] plausibel. Dennoch erscheint fraglich, ob und inwiefern die Abgrenzung zwischen anonymen und anonymisierten Datensätzen in der Tiefe erfolgt oder ob sich einem risikobasierten Ansatz bei der Betrachtung von personenbezogenen und nicht-personenbezogenen Daten angeschlossen wird. Letzteres mag aber mit einer klaren Abgrenzung kaum möglich sein. Auch zu der Anerkennung postmortaler oder pränataler Rechte, etwaiger Klarstellungen und einem Umdenken in Sachen „Dateneigentum" sind nicht ersichtlich. Das Eckpunkte-Papier deutet also grundsätzlich in eine richtige Richtung, könnte aber aufgrund der eher (daten-)wirtschaftlichen Schwerpunkte die verfassungsrechtlichen Interessen der Betroffenen vernachlässigen.

Die im Eckpunkte-Papier aufgezeigte Idee der datengetriebenen Gesellschaft setzt sich in der finalen Datenstrategie der (ehemaligen) Bundesregierung vom 27.

1312 Eckpunke-Papier Datenstrategie (Fn. 1310), S. 2.
1313 Eckpunke-Papier Datenstrategie (Fn. 1310), S. 3.
1314 Eckpunke-Papier Datenstrategie (Fn. 1310), S. 4.

Januar 2021[1315] fort. Als Grundpfeiler zur Zielerreichung wurde der Fokus jedoch merklich verschoben. Zwar sind Anonymisierung und Pseudonymisierung weiterhin zugunsten der Forschung zu fördern[1316] und eine Differenzierung von nicht-personenbezogenen und personenbezogenen Daten in der Nachnutzung ersichtlich. Der allein fördernde Ansatz zur Erforschung guter Anonymisierungspraktiken blieb jedoch bestehen; eine Definition oder anderweitige Klarstellung fehlt weiterhin. Weshalb die Bundesregierung beabsichtigt, „verschiedene Grade der Anonymität“[1317] ohne eine Definition eines einzelnen Grades abzubilden, ist nicht nachvollziehbar. Ausdrücklich bewegt sich die Datenstrategie dagegen weg von einem Dateneigentum[1318] und hin zu einer Regulierung der Datennutzung unter den Prämissen der Rechtssicherheit, Benutzerfreundlichkeit und Transparenz. Ob und inwieweit eine Evaluation des BDSG[1319] und eine Klärung der Rechtslage zwischen BDSG und DSGVO zur einfachgesetzlichen Schärfung der Anonymität beitragen können, ist fraglich. Zumindest wird die Auflösung der zersplitterten Regelung des bereichtsspezifischen Datenschutzrechts in TKG und TMG durch das TTDSG[1320] angestrebt, perspektivisch auf (quelloffenen) Open-Source-Protokollen bei der Nachnutzung von Daten gebaut[1321] und auch die wettbewerbsrechtlich kritische (Quasi-)Monopolstellung großer digitaler Akteure mittels Novelle des GWB[1322] aufgearbeitet. Einen besonderen Punkt hebt die Datenstrategie allerdings mit dem Ansatz des Datentreuhänders heraus, welcher als Informationsintermediär zwischen Betroffenem und verantwortlicher Stelle

1315 Nachfolgend bezeichnet als Datenstrategie BReg. Das Dokument ist abrufbar unter https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1.

1316 Datenstrategie BReg (Fn. 1315), S. 20 f.

1317 So Datenstrategie BReg (Fn. 1315), S. 34/35.

1318 So Datenstrategie BReg (Fn. 1315), S. 23: „Wir sprechen uns gegen die Schaffung eines ‚Dateneigentums‘ aus.“

1319 Datenstrategie BReg (Fn. 1315), S. 19.

1320 Datenstrategie BReg (Fn. 1315), S. 19.

1321 Datenstrategie BReg (Fn. 1315), S. 22, 25.

1322 Datenstrategie BReg (Fn. 1315), S. 22.

fungieren soll.[1323] Anvisiert werden dabei sowohl öffentlich-rechtliche Nutzungsmodelle sowie der B2B- und B2C-Bereich.[1324] Als Grundlage dafür soll neben den erwähnten Pseudonymisierungs- und Anonymisierungstechniken ein Hauptaugenmerk auf der sicheren Infrastruktur und der hohen Vertraulichkeit im Umgang mit den Datensätzen liegen. Die Verwaltung der eigenen Daten bei diesen Datentreuhändern soll durch ein sog. Personal Information Management System (PIMS) erfolgen[1325]. Offenbar adressiert die Bundesregierung hier die Verwaltung digitaler Identitäten durch die Schaffung eines Rechtsrahmens für Plattformen zur Identitätsdaten-Verwaltung, wie sie vereinzelt schon für den deutschen Markt mit Verimi[1326] und NetID[1327] konzipiert wurden. Insofern gewinnen digitale Identitäten und die Nutzung durch sowie Speicherung bei einem zentralen Intermediär an Bedeutung. Ein Rechtsrahmen für diese Diensteanbieter sowie zur Gewährleistung eines bereichsspezifischen wie dynamischen Schutzes der digitalen Identität in den gezeigten Facetten ist daher zwingend erforderlich. Hinsichtlich des Rechtsrahmens bietet der Data Governance Act[1328] mit seinem Kapitel III schon eine erste Grundlage. National zeigen sich bereits deutliche strukturelle Parallelen Konzeption des des Datencockpits im Rahmen des Registermodernisierungsgesetzes, welches sogleich näher zu betrachten ist[1329]. Das Ziel des Vertrauens in derartige Dienste wird perspektivisch allerdings durch Herausgabepflichten von Passwörtern und Zugangsdaten (§ 23) sowie Bestandsdaten (§ 22 TTDSG)[1330] untergraben, weshalb die im Ansatz zu befürwortende Strategie schon zu Beginn

1323 Datenstrategie BReg (Fn. 1315), S. 34.
1324 Datenstrategie BReg (Fn. 1315), S. 35.
1325 Datenstrategie BReg (Fn. 1315), S. 35.
1326 Siehe https://verimi.de.
1327 Siehe https://netid.de.
1328 Der Entwurf der Kommission ist abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767. Die im Juni 2022 in Kraft getretene, finale Fassung des DGA ist abrufbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.
1329 Sub E.III.3.
1330 Abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-zur-regelung-des-datenschutzes-und-des-schutzes-der-privatssphaere-in-der-telekommunikation-und-bei-telemedien.pdf?__blob=publicationFile&v=6.

ihrer Umsetzung an der Berücksichtigung verfassungsrechtlicher Interessen aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG zweifeln lässt.

Anders geartet ist dagegen das im Februar 2020 begonnene Konsultationsverfahren des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI), welches sich thematisch auf die Anonymisierung von Daten beschränkt.[1331] Wenngleich nicht Teil der Datenstrategie, ist dieses Verfahren dennoch interessant: Es bildet den Zwiespalt zwischen anonymisierten und pseudonymisierten personenbezogenen Daten ab und geht auf einzelne Rechtsgrundlagen der Verarbeitung ein. Die dahingehende rechtliche Diskussion bestätigt die Relevanz dieser Abgrenzung und einer Definition von Anonymität im Datenschutzrecht entgegen Erwägungsgrund 26 DSGVO. Die Lösung, die mit diesem Diskussionsvorschlag und der Befragung der Öffentlichkeit herbeigeführt werden soll, ist grundlegend zu begrüßen. Der Definitionsansatz des BfDI im Papier lässt jedoch bestehende gerichtliche oder vergangene Definitionen wie jene des § 3 Abs. 6 BDSG a.F. außen vor.[1332] Damit gelingt es schon nicht, eine gleiche Basis für die Diskussion herzustellen. Darüber hinaus wird auf das dynamische Verständnis aufgrund des risikobasierten Ansatzes der DSGVO nicht eingegangen; eine definitorische Abgrenzung zur naheliegenden Pseudonymisierung fehlt. Der positiv zu bewertende Ansatz des BfDI ist daher wenig geeignet als Schutzverstärkung de lege ferenda, vermag aber (vermeintlich) zu einer einheitlichen Definition des Datenschutzrechts zu führen: Die finale Positionierung des BfDI im Papier vom 29.06.2020[1333] greift die Punkte der Stellungnahmen durchaus auf, beschränkt sich aber auf die bekannten Definitionen nach dem relativen Verständnis einer Abgrenzung von Pseudonymisierung und Anonymisierung unter Rüückgriff auf

1331 Abrufbar unter https://www.bfdi.bund.de/SharedDocs/Konsultationsverfahren/2020/01_Anonymisierung-TK.pdf?__blob=publicationFile&v=6.

1332 Siehe S. 4 ff der Stellungnahme von FIZ Karlsruhe, abrufbar unter https://www.fiz-karlsruhe.de/sites/default/files/FIZ/Dokumente/Meldungen/BFDI-Stellungnahme-Konsulation-FIZ-Uni-Bonn-KIT-20200309.pdf.

1333 Abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung.pdf?__blob=publicationFile&v=2.

die Breyer-Entscheidung des EuGH.[1334] Wie auch im Beitrag von *Stürmer*[1335] wird im Papier davon ausgegangen, dass die Überprüfung der Anonymisierung auf ihre Validität „eine fortwährende Aufgabe des Verantwortlichen" ist – ohne eine Herleitung aus dem Pflichtenkorsett der DSGVO. Eine Klarstellung ist damit nur begrenzt gelungen.

Breiter gefasst als die nationalen Bestrebungen scheint mit einer zehnjährigen Laufzeit von 2020 bis 2030 die Datenstrategie der Europäischen Kommission.[1336] Allgemein wird darin beschrieben, dass Daten im 21. Jahrhundert die Hauptrolle in Wirtschaft und Gesellschaft einnehmen bzw. einnehmen werden: „Data is at the centre of this transformation and more is to come." Unter dieser Prämisse soll die europäische Wirtschaft und Gesellschaft in die Lage einer Vorreiterrolle – wie auch Deutschland selbst im Rahmen des o.g. Eckpunkte-Papiers[1337] – in Bezug auf Digitalisierung, Datenwirtschaft und Cloud-Dienste versetzt werden. Dies betrifft vor allem kleine und mittelständische Unternehmen (KMU) sowie Start-ups. Durch diverse Rechtsakte soll die Möglichkeit für diese Unternehmen wie auch Individuen bzw. natürliche Personen vereinfacht werden, Teil der Digitalisierung zu sein; der in Art. 1 Abs. 1 DSGVO aE erwähnte freie Verkehr von Daten soll inter- und intradisziplinär verstärkt werden. Dieser ist maßgebend für die beabsichtigte Errichtung eines Europäischen Datenmarktes – „a genuine single market for data, open to data from across the world"[1338]. Hierbei soll auch auf Daten- und IT-Sicherheit sowie die Rechte und Freiheiten der Beteiligten und ihre Datenkompetenz Rücksicht genommen werden.[1339] Die Probleme, die die Europäische Kommission damit adressiert, sind fast ausschließlich wirtschaftlicher Natur: Die fehlende Verfügbarkeit geeigneter (personenbezogener wie nicht-personenbezogener) Daten, ein verschobenes Kräfteverhältnis im

1334 Positionspapier des BfDI vom 29.06.2020 (Fn. 1333), S. 4.
1335 Siehe *Stürmer*, ZD 2020, 626 (629).
1336 Nachfolgend bezeichnet als Datenstrategie EU. Das Papier ist einsehbar unter https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.
1337 Datenstrategie EU (Fn. 1336), Rn. 2, 5.
1338 Datenstrategie EU (Fn. 1336), S. 4.
1339 Datenstrategie EU (Fn. 1336), S. 6.

internationalen Datenmarkt, mangelhafte Interoperabilität von Schnittstellen/Datensätzen und die fehlende Regulierung. Ebenso müssen Dateninfrastrukturen und die (datengenerierenden) Individuen gefördert werden. Deshalb widmet sich die Strategie der Umsetzung vierer Pfeiler, auf denen der Europäische Datenmarkt errichtet werden soll. Im Anschluss an eine interdisziplinäre Regulierung zu Zugang und Nutzung hochwertiger Datensätze[1340] werden sog. Enabler (dt. Auslöser, Befähiger) in Form von Forschungsprojekten und ähnlichen Unterstützungsleistungen genutzt[1341]. Letztere nehmen mit dem Zeitraum von 2021-2027 den größten Anteil der Strategie ein. Zugleich beginnt die Einrichtung von sog. Data Spaces, die im einzelnen recht technisch beschrieben, im Kern aber als Teil des großen Europäischen Datenmarktes zu sehen sind. Dies bestätigt zumindest der vierte Pfeiler der Strategie, welcher den Aufbau einer Vielzahl von Data Spaces in den Blick nimmt.[1342] Für die digitale Identität ist die bis hierhin überaus wirtschaftliche Sichtweise insoweit relevant, als dass Datensätze und ggf. auch digitale Identitäten nach dem vorgestellten Begriff einer breiten Masse zugänglich gemacht werden. Dies ist nicht per se negativ zu bewerten, sondern erfordert ein entsprechendes Schutzniveau durch staatliche Maßnahmen. Hierauf deutet zwar der regulatorische Rahmen des ersten Pfeilers hin. Dieser versteht sich vor dem Hintergrund des dritten Pfeilers jedoch eher als marktbezogenes Unterfangen: Der bislang nicht erwähnte Pfeiler bezieht die Interessen der Individuen unmittelbar ein und fördert Kompetenzen der Bürgerinnen und Bürger sowie KMU. Dies soll vor allem dadurch gelingen, das Recht auf Interoperabilität gem. Art. 20 DSGVO verstärkter durchzusetzen und damit die informationelle Selbstbestimmung der Betroffenen zu gewährleisten.[1343] Weitere, ausdrückliche Maßnahmen räumt die Datenstrategie jedoch nicht ein. Insgesamt kann damit auch diese Strategie nicht auf der Ebene der Grundrechtsgewährleistung überzeugen; Absichten zur Förderung von Standards zum Schutz digitaler Identitäten geschweige eine legislative

1340 Datenstrategie EU (Fn. 1336), S. 12 ff.
1341 Datenstrategie EU (Fn. 1336), S. 15 ff.
1342 Datenstrategie EU (Fn. 1336), S. 21 ff.
1343 Datenstrategie EU (Fn. 1336), S. 20/21.

Klarstellung von Anonymisierung und Pseudonymisierung – welche für den Austausch von Daten jeglicher Art zwingend notwendig ist – enthält der Plan nicht.

Im Verlauf des Jahres 2021 bestätigt sich die vermutete Streubreite der europäischen Datenstrategie, die sich in den Entwürfen des (bereits erwähnten) Data Governance Acts (DGA-E bzw. DGA für die finale Fassung)[1344], Digital Services Acts (DSA-E)[1345], Digital Markets Acts (DMA-E)[1346], Data Acts[1347] und AI Acts[1348] verwirklicht. Dabei decken DSA-E und DMA-E die zweiseitige Regulierung von datenverarbeitenden Unternehmen ab: Der DMA-E widmet sich wettbewerbs- und kartellrechtlichen Aspekten und fungiert als Regulierung des level playing field. Ergänzend reguliert der DSA-E Informationsintermediäre inhaltsbezogen; im Fokus stehen Netzwerk- und Informationsdienste („Mere Conduit", Art. 3), die vorübergehende Datenspeicherung („Caching", Art. 4) und die auf Dauer angelegte Speicherung auf Anfrage von Nutzenden („Hosting", Art. 5) sowie – nach dem aktualisierten Entwurf des EU-Rates[1349] – auch Suchmaschinen und Online-Marktplätze (siehe Art. 2 lit. f). Dadurch wird die Umsetzung datenschutzrechtlicher Transparenzpflichten durch plattformbezogene Transparenzvorgaben flankiert.

Von deutlicher Relevanz für die Materie der digitalen Identität ist aber der Digital Governance Act. Prinzipiell zielt dieser auf die Nutzbarmachung von Daten allgemein ab. Die Relevanz ergibt sich aber aus Abschnitt III und IV: Abschnitt III regelt ein Meldeverfahren für Daten-Intermediäre, die per definitionem als

1344 Siehe Fn. 1328.

1345 Einsehbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_de.

1346 Einsehbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de.

1347 Zum Bearbeitungszeitpunkt befindet sich der Entwurf noch in der Konsultations- und Entwicklungsphase. Weitere Informationen unter https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act.

1348 Einsehbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

1349 Einsehbar unter https://www.statewatch.org/media/2719/eu-council-dsa-compromise-chapters-1-2-11459-21.pdf.

Datentreuhänder verstanden werden können.[1350] „‚Dateninhaber' [ist] eine juristische Person, einschließlich öffentlicher Stellen und internationaler Organisationen oder natürliche Person, die in Bezug auf die betreffenden Daten keine betroffene Person ist, welche nach geltendem Unionsrecht oder geltendem nationalen Recht berechtigt ist, Zugang zu bestimmten personenbezogenen Daten oder nicht personenbezogenen Daten zu gewähren oder diese Daten weiterzugeben" – so Art. 2 Nr. 8 DGA. Die Intermediärsleistung einer Datentreuhand bezeichnet Art. 9 lit. a DGA als „Vermittlungsdienste zwischen Dateninhabern und potentiellen Datennutzern [...]; zu diesen Diensten können auch der zwei- oder mehrseitige Austausch von Daten oder die Einrichtung von Plattformen oder Datenbanken, die den Austausch oder die gemeinsame Nutzung von Daten ermöglichen, sowie die Einrichtung anderer spezieller Infrastrukturen für die Vernetzung von Dateninhabern mit Datennutzern gehören". Unter Berücksichtigung des Datenschutzrechts wird so der Ansatz der Personal Information Management Systems auf europäischer Ebene realisiert. Darüber hinaus erwähnenswert ist die in Abschnitt IV des DGA ausgestaltete Form des sog. Datenaltruismus. Nach diesem Konzept soll auf Basis einer Einwilligung eine „freiwillige Datenbereitstellung durch Einzelpersonen oder Unternehmen zum Wohl der Allgemeinheit"[1351] erfolgen. Neben Eintragungs- (Art. 17) und Transparenzerfordernissen (Art. 20) regelt der Abschnitt gem. Art. 21 auch „[b]esondere Anforderungen zum Schutz der Rechte und Interessen betroffener Personen und juristischer Personen im Hinblick auf ihre Daten". Besonders zu berücksichtigen sind dabei die enge Zweckbindung (Art. 21 Abs. 1 und 2) sowie die Einholung eines jeweiligen willensbestätigenden Aktes – eine Einwilligung bei natürlichen Personen, eine Erlaubnis zur Verarbeitung bei juristischen Personen (Art. 19 Abs. 3). Unwissentlich reflektiert der Entwurf damit das im Rahmen dieser Arbeit dargestellte Interesse beider betroffener Parteien und legt unionsrechtlichen Grundstein für eine Wahrnehmung von Interessen für unternehmensbezogene digitale Identitäten. Ganz ähnliche Regelungen finden sich im Hinblick auf das Fernmeldegeheimnis in § 1 Abs. 2 TTDSG

1350 So auch *Beise*, RDi 2021, 597 (601 f). Anders *Richter*, ZEuP 2021, 634 (641 f): Datentreuhand als Untergruppe von Datenmittlern bzw. Daten-Intermediären.

1351 DGA-E (Fn. 1328), S. 9.

bzw. § 91 Abs. 1 S. 2 TKG a.F., die jeweils „Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder Personengesellschaft"; sie „stehen personenbezogenen Daten gleich."

Die datenschutzrechtlich geprägten Novellierungsvorhaben und Strategien können aus dargestellten Gründen zunächst wenig überzeugen. Allesamt weisen sie in die Richtung einer datengetrieben Gesellschaft und Wirtschaft, übersehen aber die dafür notwendige Berücksichtigung der Rechte und Freiheiten der Betroffenen in concreto. Unionsrechtlicher Lichtblick bleibt dabei Art. 21 DGA. Die notwendige begriffliche Klarstellung der Anonymisierung weiß soweit nur das Konsultationsverfahren des BfDI zu adressieren.

2. IT-Sicherheitsgesetz 2.0: Zur Evolution des BSI

Konträr ist sich der Novellierung technisch geprägter Korrekturvorhaben des Gesetzgebers zu widmen, um die dargestellte technische Schutzrichtung der Grundrechte zu reflektieren. Dazu wird die an das IT-Sicherheitsgesetz anknüpfende Gesetzgebung in Form des IT-Sicherheitsgesetzes 2.0 näher betrachtet, die im Frühjahr 2019[1352] sowie 2020[1353] in Entwurfsfassungen und als Kabinettsentwurf[1354] öffentlich zugänglich gemacht wurde und nunmehr seit 28.5.2021 in Kraft ist. Hauptaugenmerk dieser Untersuchung sind die aufgezeigten Forderungen zum Schutz des GGVIS, namentlich der Gewährleistung der IT- bzw. Systemsicherheit durch anwendungsbezogene Mindeststandards sowie ein entsprechendes Schutzkonzept gegen Sicherheitslücken in Hard- und Software.

1352 Einsehbar unter https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/.

1353 Einsehbar unter https://netzpolitik.org/2020/seehofer-will-bsi-zur-hackerbehoerde-ausbauen/.

1354 Einsehbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf?__blob=publicationFile&v=2.

Der aus dem Jahr 2019 einsehbare Entwurf (nachfolgend i.E. BSI-G-neu 2019 und TMG-neu 2019) zielt auf die grundlegende Aufgabe des BSI ab, die Sicherheit in der Informationstechnik zu fördern und zu sichern. Dabei fokussiert es sich sowohl auf eine verbraucherschützende wie proaktive Rolle bei der Untersuchung von Sicherheitsvorfällen, die in Abwehrstrategien münden soll. „Dieses Gesetz dient daher dem Schutz der Gesellschaft, der Wirtschaft und des Staates." Diese Aufgabe wird durch Gesetzesänderungen in TKG, TMG, StGB und StPO flankiert; es handelt sich wie schon beim „IT-Sicherheitsgesetz 1.0" um ein Artikelgesetz. Konkret dienen die Änderungen des BSI-G der Erhöhung bzw. Ausdehnung des Aufsichtskreises des BSI, indem die etablierten Begriffe der Kritischen Infrastrukturen (§ 2 Abs. 10 BSI-G) und Digitale Dienste (§ 2 Abs. 11 BSI-G) um sog. Infrastrukturen im besonderen öffentlichen Interesse gem. § 2 XIV BSI-G-neu 2019 erweitert werden. Hierzu sollen nun Infrastrukturen aus dem Bereich Kultur und Medien[1355] sowie Dienste aus dem Bereich finanzieller Transaktionen mit entsprechender volkswirtschaftlicher Gefährdungslage im Falle eines IT-Sicherheitsvorfalls zählen. Entsprechend ihrer Relevanz für die Gesellschaft gelten für diese teilweise die gleichen Pflichten wie für Kritische Infrastukturen, so § 8f BSI-G-neu 2019 mit entsprechenden Verweisen. Im Einzelfall kann das BSI auch bestimmte Diensteanbieter bzw. Betreiber von Anlagen seinem Aufsichtskreis hinzufügen, wenn für diesen das Kriterium der Cyberkritikalität gem. § 8g BSI-G-neu 2019 erfüllt ist. Darüber hinaus erweitert der Entwurf das Aufgabenportfolio um verbraucherschützende Aufgaben, beispielsweise die unmittelbare Information von betroffenen Verbrauchern (vgl. § 3 Abs. 1 S. 1 Nr. 14, 14a und §§ 7, 7a BSI-G-neu 2019) und das Dasein als allgemeine Meldestelle für die Sicherheit in der Informationstechnik (§ 4b BSI-G-neu 2019). Darüber hinaus ermöglicht § 9a BSI-G-neu 2019 die Einführung eines freiwilligen IT-Sicherheitszertifikats, das trotz einer Kontrollkompetenz des BSI nur geringen Druck auf die Gewährleistung der in der Herstellererklärung benannten technischen Eigenschaften ausübt. Hierzu trägt insbesondere der Hinweis

1355 Hierunter versteht der Entwurf Akteure der „Pressefreiheit, der Berichterstattung und [der] Pluralität der Medien" – so die Begründung des Entwurfes von 2019, sub Fn. 1352. Befürwortend im Vorfeld der Veröffentlichung *Etteldorf*, AfP 2018, 114 ff.

der Gesetzesbegründung bei, dass es sich nur um „die Möglichkeit (nicht die Pflicht)“ des BSI handelt. Darüber hinaus ist nicht nachvollziehbar, warum nicht auf bestehende europäische Zertifizierungen zurückgegriffen[1356] und auf eine im Europäischen Binnenmarkt mit dem CE-Kennzeichen vergleichbare Harmonisierung hingewirkt wird. Auffallend ist, dass sich letztere auch auf den Schutz von Betriebs- und Geschäftsgeheimnissen erstreckt, was ein Gleichlaufen aus Gründen der Rechtseinheit mit dem geltenden GeschGehG andeutet. Der Eindruck, dass hierin aber auch der Schutz der digitalen Identitäten juristischer Personen zu erkennen ist, wird durch Einfügung der §§ 99 Abs. 2 Nr. 1, 3 und 202f Abs. 5 Nr. 1, 3 StGB im Rahmen des IT-Sicherheitsgesetzes 2.0 verstärkt.

Eigentlicher Kern des Entwurfes sind aber weitreichende Berechtigungen zur Untersuchung fremder Systeme auf maliziöse Inhalte oder Handlungsweisen. So benennt der Entwurf konkret in § 7b BSI-G-neu 2019: „Das Bundesamt kann zur Erfüllung seiner Aufgaben Maßnahmen zur Detektion und Auswertung von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken in öffentlich erreichbaren informationstechnischen Systemen durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt sind und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. [...] Ein informationstechnisches System ist ungeschützt [...], wenn öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund offensichtlich unzureichender Sicherheitsvorkehrungen von unbefugten Dritten auf das System zugegriffen werden kann.“ Hierzu erläutert die Begründung: „Dies wäre zum Beispiel dann der Fall, wenn für ein System werkseitig stets ein identisches Passwort (‚0000‘ oder ‚admin‘) vergeben würde oder wenn die werksseitige Vergabe der Passwörter nach einer öffentlich bekannten und einfachen Systematik erfolgte.“ In diesem Fall darf das BSI gem. § 7b Abs. 4 BSI-G-neu 2019 „Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen“ und auf Portscans oder Honeypot-Mechanismen zurückgreifen, also zT aktiv Anwendungen auf dem fremden System ausführen. Hier erscheint fraglich, ob auch ungeschützte Systeme iSd Norm dem grundrechtlichen Schutz des GGVIS unterliegen. Schließlich ist

1356 *Kipker*/*Scholz*, DuD 2021, 40 (43).

in dieser Art des Handelns ein staatlicher Eingriff zu sehen. Der Entwurf deutet mit der Eigenschaft der Schutzlosigkeit darauf hin, dass es sich um bewusst ungeschützte Systeme handelt. Dieser Gedanke wird jedoch ins Gegenteil verkehrt, wenn im Rahmen der Legaldefinition auf bekannte Sicherheitslücken oder offensichtlich unzureichende Sicherheitsvorkehrungen verwiesen wird. Zwar erscheint dies konsequent, lassen mangelnde Schutzvorkehrungen auf ein fehlendes Vertrauen in die Integrität des Systems schließen und berücksichtigen die Rechtsprechung des Bundesverfassungsgerichts.[1357] Der Grad der Offensichtlichkeit kann jedoch behördlich-subjektiv gefärbt sein, weil er die technische Kompetenz des Nutzers außer Acht lässt. Letzteres wird insbesondere durch eine fehlende (Legal-)Definition begünstigt.[1358] Gerade in Bezug auf bekannte Sicherheitslücken erscheint fraglich, ob und wie diese durch den Nutzer zu beheben sind. Ist dies nicht möglich bzw. zumutbar, verschiebt sich der grundrechtliche Schutz mangels ausreichender Kompetenz zulasten des Nutzers; ein Zugriff auf das System ist lt. Norm zulässig. Dass selbige mangelnde Kompetenz allerdings dazu führen kann, dass unbewusst Opfer von Botnetzen gewordene Systeme einen staatlichen System-Zugriff ermöglichen, scheint nicht im Sinne des GGVIS. Diesbezüglich hätte mit der im Rahmen dieser Arbeit dargestellten, der Rechtsprechung des Bundesverfassungsgerichts immanenten Terminologie[1359] gearbeitet werden müssen, um die Abgrenzung zwischen Vertrauen und System abbilden zu können. In Anlehnung an die Rechtsprechung zur Online-Durchsuchung hätte es auch eines Richtervorbehalts[1360] oder eines ähnlichen Mechanismus bedurft, welcher die Unabhängigkeit bei der Einschätzung des Systems wahrt; auch eine Unabhängigkeit des BSI selbst wäre hier erwägenswert[1361]. Ebenso fehlt es an einer Benennung des Grundrechts in § 11 BSI-G-neu 2019 zur Erfüllung des Zitiergebots gem. Art. 19 Abs. 1 S. 2 GG. Der systembezogene Schutz wird folglich durch diesen Entwurf unterlaufen. Auf Datenebene scheint dagegen die Einfügung des § 163g StPO

1357 Hierzu ausführlich sub D.II.4.
1358 Hierauf hinweisend *Kipker*/*Scholz*, DuD 2021, 40 (42).
1359 Sub D.II.4. unter Verweis auf BVerfGE 120, 274 (313 ff).
1360 BVerfGE 120, 274 (335).
1361 Ebenso fordernd ; *Kipker*/*Scholz*, DuD 2021, 40 (44). Partiell ablehnend dagegen *Schallbruch*, DuD 2021, 229 (231).

relevant, welcher den Zugriff auf und die Nutzung von Login-Daten bei Verdacht einer Straftat iSd § 100g StPO gegen den Willen des Inhabers ermöglicht. Diese Verwendung der digitalen Identität erscheint jedoch aus Gründen öffentlichen Interesses gerechtfertigt.

Der überarbeitete Entwurf vom 7.5.2020 (nachfolgend i.E. BSI-G-neu 2020 und TMG-neu 2020) enthält keine Änderungen und Einfügungen für StPO und StGB mehr und ist hinsichtlich des BSI-G und des TMG angepasst worden. Unter anderem wird der Bereich Medien und Kultur nicht mehr als Unternehmen in besonderem öffentlichem Interesse iSd § 2 Abs. 14 BSI-G-neu 2019 geführt. Stattdessen umfasst dieser Unternehmen, „die aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichen Interesse sind". Wie diese Formulierung genau zu verstehen ist, erklärt auch die Gesetzesbegründung nicht; es wird lediglich auf die zu verabschiedende, Unternehmen benennende Rechtsverordnung verwiesen. Auch fehlt die Möglichkeit einer Erweiterung der kritischen Infrastrukturen um Fälle mit hoher Cyberkritikalität; § 8g BSI-G-neu 2019 wurde ersatzlos gestrichen. Erhalten geblieben sind die Informations- und Warnaufgabe, das freiwillige IT-Sicherheitskennzeichen sowie die Prüffähigkeit von IT-Soft- und Hardware zu Zwecken des Verbraucherschutzes. Das Telemediengesetz hat hingegen eine bedeutende Erweiterung hinsichtlich der Pflichten des Diensteanbieters gem. § 13 TMG a.F. erfahren. Hier werden neben einer besonderen Pflicht für kritische Infrastrukturen in § 13 Abs. 7a TMG-neu-2019 und 2020 noch die Absätze 9 und 10 eingefügt. Absatz 9 zielt auf die Sperrung von Nutzern bzw. Nutzerkonten ab, die unrechtmäßig erlangte personenbezogene Daten oder Datensätze aus Geschäftsgeheimnissen auf der Plattform des Diensteanbieters (widerrechtlich) veröffentlichen. Damit adressiert der Entwurf aus 2020 – so auch die Begründung – die zahlreichen öffentlich zugänglichen Daten-Leaks. In Bezug auf Geschäftsgeheimnisse findet sich in Abs. X noch eine Erweiterung, indem für den Schutz der öffentlichen Sicherheit und Ordnung zuständige Stellen eine Sperrung der Daten anordnen können; personenbezogene Datensätze sind hiervon nicht umfasst, sondern umfänglich in § 15b TMG-neu 2019 bzw. 2020 geregelt. Dies mag in der Verpflichtungskette aus

Art. 33, 34 DSGVO begründet sein, die den Diensteanbieter bereits zur Information des Nutzers sowie Datenschutzbehörden und indirekt iVm den Grundsätzen des Art. 5 Abs. 1 DSGVO auch zu Schutzmaßnahmen zugunsten betroffener Personen verpflichtet. Hier gibt es zwar lt. Begründung des Entwurfes zwar keine Überlagerung, dennoch ein Gleichlaufen von Datenschutzrecht und Telemediengesetz. Die grundsätzlich dienstebezogene Ausrichtung des TMG wird durch die Einschränkung des § 15b TMG-neu 2019 bzw. 2020 auf personenbezogene Datensätze gespiegelt, erweitert die Pflichten des Diensteanbieters allerdings lediglich um eine weitere Meldestelle. Nähere Dokumentations- und Nachsorgepflichten, wie sie Art. 33, 34 DSGVO vorsehen, enthält die Regelung nicht und umgeht so das Normwiederholungsverbot des Erwägungsgrundes 8 DSGVO bzw. Art. 288 Abs. 3 AEUV weitestgehend. Dass die Norm allerdings das Leaken von personenbezogenen Daten wie Betriebs- und Geschäftsgeheimnissen in der selben Norm regelt, deutet auf die ähnliche Gefährdungslage hin und bestätigt (erneut) das im Rahmen dieser Arbeit vorgebrachte Argument des Schutzes digitaler Identitäten juristischer Personen.

Die erneut überarbeitete und letztlich umgesetzte Fassung vom 19.11.2020 enthält nur marginale Neuerungen, die auf die dargestellten Punkte kaum Einfluss haben.[1362] Bemerkenswert ist, dass die Änderungen des TMG im finalen Entwurf nunmehr vollständig gestrichen wurden; die Melde-Kaskade vor dem Hintergrund des geplanten § 15b TMG-neu 2019 ist damit obsolet. Auch in der geltenden Fassung des TTDSG finden sich keine Hinweise auf derartige Meldevorgänge; die Regelung der technischen und organisatorischen Vorkehrungen des § 19 TTDSG fängt dies nicht auf, sondern beschränkt sich auf die technischen Schwerpunkte des § 13 Abs. 7 TMG a.F.

1362 Der dritte Entwurf des IT-Sicherheitsgesetzes 2.0 einschließlich einer Kurzzusammenfassung von *Kipker* findet sich unter https://intrapol.org/2020/11/21/it-sig-2-0-dritter-referentenentwurf-mit-stand-vom-19-11-2020-veroeffentlicht/ sowie unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf;jsessionid=31938A3DC4DB3C427D01B29CE8179374.2_cid295?__blob=publicationFile&v=2.

In conclusio sind ansatzweise Bestrebungen zu einer Erweiterung des Schutzes digitaler Identitäten in IT-sicherheitsrechtlicher Hinsicht zu erkennen. Verbraucherschützende Aspekte können hier jedoch nur provisorisch wirken, bedarf es noch konkreter Pflichten aufseiten der Hersteller und Diensteanbieter. Diametral zu den befürwortenden Ansätzen zur Erhöhung der IT-Sicherheit wirken jedoch die Befugnisse des BSI zum aktiven (vermeintlichen) Schutz der Systeme. Die Möglichkeit der Überprüfung offener Systeme sowie etwaiger Zugriffsmöglichkeiten gegen und/oder ohne Willen oder Bewusstsein des Systeminhabers berücksichtigt nicht die fehlende Kenntnis zum Schutz eigener Systeme und setzt letztlich die vollumfängliche Umsetzung der Prinzipien „Data Protection by Design" und „Data Protection by Default" sowie einen informierten und update- bzw. upgradewilligen Nutzer voraus. Dies entspricht jedoch nicht der Realität. Beispielsweise können Hardware-Sicherheitslücken nur durch einen Austausch der Hardware selbst gelöst werden, die jedoch nicht jedem Bürger bzw. jeder Bürgerin jederzeit finanziell oder anderweitig möglich ist. Folglich handelt es sich um eine potentielle Eingriffsgrundlage einer breiten Masse an Systemen, die entgegen der möglichen Eingriffstiefe in gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG geschützte Systeme nicht in § 11 der BSI-G-Neufassung aufgeführt ist. Damit bestehen verfassungsrechtliche Bedenken gegenüber den Entwürfen aus 2019 und 2020 sowie der finalen Umsetzung des §§ 7b, 11 BSI-G.

Für die weitere Umformung des nationalen IT-Sicherheitsrechts – und damit auch der Rolle des BSI – ist abschließend noch ein Blick auf die Cybersicherheitsstrategie 2021[1363] der (ehemaligen) Bundesregierung sowie den Entwurf der NIS2-Richtlinie[1364] zu werfen.

Strategisch konzentriert sich die (ehemalige) Bundesregierung auf die Förderung der IT-Sicherheit von staatlichen Institutionen, Wirtschaft und Gesellschaft. Neu ist allerdings die sowohl in der Zielrichtung als auch in einzelnen Zielen konkrete

1363 Einsehbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=AF7B435DBA70B115EBACE34C2047B87F.2_cid295?__blob=publicationFile&v=1.

1364 Einsehbar unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN.

Benennung der Forschung als zu berücksichtigender Bereich. Während bislang die Forschung nur als wichtige Quelle für neue Entwicklungen und Lösungen gesehen wurde, wird sie nun konkret in die Umsetzung der Ziele einbezogen. Im Kern bewegt sich die Strategie aber dennoch nicht vom bisherigen Modus weg: Förderung der IT-Sicherheit durch Aufklärung, Information und Angebote – vor allem zu Zwecken des Verbraucherschutzes; Fördern und Verteidigen der nationalen wie internationalen Position (z.B. durch BSI) als Weltspitze der IT-Sicherheit; Zusammenarbeit der Bundesbehörden vor allem im Ermittlungs- und Strafverfolgungsbereich unter der Linie des BMI; Schutz kritischer Infrastrukturen; Anpassung bestehender Gesetze und Entwurf neuer Gesetze zur Reflexion des IT-Sicherheitsniveaus; Berücksichtigung neuer Techniken wie KI, elektronischer/-digitaler Identitäten und Authentifizierungsmechanismen. Dabei unberücksichtigt bleibt auch der zum Zeitpunkt der Veröffentlichung der Cybersicherheitsstrategie (konkret: 8.9.2021) der am 16.12.2020 veröffentlichte Entwurf der NIS2-RL. Erwähnenswerte Eckpunkte des Entwurfes sind zunächst die Überarbeitung der Terminologie und die Verzahnung der Europäischen und mitgliedsstaatlichen IT-Sicherheitsstrategie in der Tiefe. Ersteres bezieht sich auf die Auflösung des Begriffes „Digitale Dienste“, wie er zuvor in § 2 Abs. 11 BSI-G übernommen wurde. Die Richtlinie sowie Umsetzung soll nun anhand des Merkmals der Kritikalität (so ErwGr 11 NIS2-RL-E) eine Unterscheidung zwischen „essential entities“ und „important entities“ vornehmen, wobei besagte Digitale Dienste nun in den „important entities“ aufgehen. Zu bemerken ist hier auch, dass im Hintergrund auch diese Dienste um Soziale Netzwerke erweitert worden sind, dem Entwurf nach also als „important entities“ ebenfalls IT-sicherheitsrechtlichen Pflichten unterliegen. Die Verzahnung soll weiter durch mehrere Maßnahmen gelingen. Zum einen soll jeder Mitgliedsstaat zum Zweck der Mindestharmonisierung (Art. 3 NIS2-RL-E) eine nationale Cybersicherheits-Strategie vorweisen können, die den Mindestgehalt des Art. 5 Abs. 1 des Entwurfes berücksichtigt.

Unter anderem wird die ENISA, unter Rückgriff auf die Ziele der EU-Cybersicherheitsstrategie, mit weiteren Aufgaben im Rahmen der sog. Coordinated Vulnerability Disclosure (nachfolgend CVD) betraut, parallel zu der nationalen Aufgabe einer entsprechenden Meldestelle. Hier sollen die Mitgliedsstaaten eine

(bestehende oder neue) Stelle vorsehen, die entsprechende IT-Sicherheitslücken sammelt, gemeinsam mit der ENISA in einem Verzeichnis und mit entsprechenden Mindestangaben (Umfang und Risiko des Exploits, mögliche Patches, etc.) vorhält. Diesem Aspekt wird das BSI-G in all seinen Entwürfen sowie der aktuellen Fassung allerdings nicht gerecht. Nicht nur ist die begriffliche Auflösung nicht vorbereitet oder erwähnt worden; auch lässt das Gesetz keine Ansätze einer CVD erkennen. Mit gutem Willen lässt sich dieser Aspekt in die Aufgabe der allgemeinen Meldestelle gem. § 4 Abs. 1 BSI-G hineinlesen; diese deckt schließlich „Informationen über Sicherheitsrisiken in der Informationstechnik" ab. Dennoch fehlt es dann an einer konkreten Handlungsgrundlage zum Vermitteln zwischen meldender Einrichtung und betroffenem Unternehmen iSd Art. 6 NIS2-RL-E; die europäische Mindestharmonisierung gem. Art. 3 NIS2-RL-E würde unterlaufen. Dabei lässt sich auch zweifeln, ob es sich beim BSI und der derzeitigen Ausgestaltung um eine hinreichend vertrauenswürdige vermittelnde Stelle handelt. Die bereits erwähnte mangelnde Unabhängigkeit des Bundesministeriums sowie die Weisungsbefugnis des BMI gegenüber dem BSI lassen vermuten, dass bei bestimmten IT-Sicherheitslücken keine interessenausgleichende Position eingenommen wird. Vielmehr könnte das Bundesministerium als Sammelstelle für IT-Sicherheitslücken diese zum Zwecke der eigenen oder fremden Ermittlungstätigkeit zweckentfremden; eine gesetzliche Maßgabe gibt es hiergegen nicht. Lediglich dem in dieser Arbeit dargelegten Verständnis der Schutzpflicht des GGVIS widerspricht eine solche Verwendung. Dieser Schluss findet auch in der Rechtsprechung des BVerfG Halt, das bei fehlender gesetzlicher Implementierung eines IT-Sicherheitslücken-Managements eine Schutzpflichtverletzung annimmt[1365]. Damit drängt sich sowohl aus der Schutzpflichtenerfüllung als auch aus dem Umsetzungsauftrag der kommenden NIS2-RL der gesetzgeberische Auftrag auf, die Meldung und Schließung von IT-Sicherheitslücken in einer unabhängigen Institution zu verankern. Besonders zu berücksichtigen sind dabei die Interessen der IT-Sicherheitsforschung, für das Auffinden und Melden nicht vonseiten der

1365 BVerfG ZD 2021, 685 (686, Rn. 30 ff) sowie bestätigt in Nichtannahmebeschluss vom 20.1.2022, Az. 1 BvR 1552/19, Rn. 19 f.

Hersteller belangt zu werden.[1366] Dem hat sich die (neue) Bundesregierung im Koalitionsvertrag[1367] scheinbar angenommen, denn „[d]as Identifizieren, Melden und Schließen von Sicherheitslücken in einem verantwortlichen Verfahren, z.B. in der IT-Sicherheitsforschung, soll legal durchführbar sein."[1368] Dementsprechend würde „[d]ie Cybersicherheitsstrategie und das IT-Sicherheitsrecht [...] weiterentwickelt."[1369] Sollte dies nicht im Rahmen der Umsetzung des NIS2-RL-E erreicht werden, ist sich der Forderung einer Gewährleistung des einheitlichen Sicherheitsniveaus qua „europäischer IT-Sicherheits-Grundverordnung" von *Hackenjos et al.* anzuschließen.[1370]

3. Das Registermodernisierungsgesetz und die einheitliche Identifikationsnummer

Im Jahr 2020 manifestierte sich darüber hinaus ein Paradebeispiel der im Rahmen dieser Arbeit dargestellten digitalen Identität: Aufbauend auf der Einführung der Steuer-Identifikationsnummer im Jahr 2007 soll nun ebendiese als Grundlage für eine einheitliche (Bürger-)Identifikationsnummer für öffentliche Stellen übernommen werden. Der am 23.09.2020 veröffentlichte und zum 15.7.2021 umgesetzte Entwurf des Registermodernisierungsgesetz[1371] baut damit die in § 139b AO geregelte Identifikationsnummer als Referenz auf einen Basisdatensatz für behördliche Angelegenheiten aus, um die Digitalisierung der Verwaltung durch das Onlinezugangsgesetz (OZG) zu vereinfachen und entsprechenden Mängeln durch unterschiedliche Datenstrukturen in den verschiedenen Behörden „(z.B.

1366 Hierzu ausführlich das Whitepaper der inter- und intradiszipinären Initiative zur Schaffung eines rechtssicheren Rahmens für die IT-Sicherheitsforschung (kurz: sec4research) unter Beteiligung des Autors – *Balaban* et al., Whitepaper zur Rechtslage der IT-Sicherheitsforschung – sowie der dazugehörige Forderungskatalog unter https://sec4research.de/assets/Forderungen.pdf.

1367 Einsehbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf.

1368 Koalitionsvertrag 2021-2025 (Fn. 1367), S. 16.

1369 Koalitionsvertrag 2021-2025 (Fn. 1367), S. 16.

1370 Siehe *Hackenjos*/*Mechler*/*Rill*, DuD 2018, 286 (288 ff).

1371 Abrufbar unter https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/registermodernisierungsgesetz.html – nachfolgend als RegModG-E bezeichnet.

Transkriptionsfehler, Namensverwechslungen, unterschiedliche Aktualisierungsfrequenzen, unterschiedliche fachliche Anforderungen)“ entgegenzuwirken[1372]. „Dies lässt sich nur durch ein registerübergreifendes Identitätsmanagement mit einem eindeutigen und veränderungsfesten Ordnungsmerkmal (Identifikationsnummer) vermeiden.“[1373]

Als gesetzliche Grundlage für die Identifikationsnummer dient das durch den RegModG-E in Art. 1 formulierte Identifikationsnummerngesetz (IDNrG). Danach soll besagte Identifikationsnummer des § 139b AO als zusätzliches Ordnungsmerkmal zum Zweck der Zuordnung (Nr. 1), zur Verbesserung der Datenqualität (Nr. 2) und Daten(satz)minimierung bei öffentlichen Stellen (Nr. 3) eingeführt werden, § 1 IDNrG. Dementsprechend verpflichtet § 2 IDNrG sämtliche öffentliche Stellen des Bundes und der Länder zur Umsetzung, definiert den zu speichernden Datensatz in § 4 Abs. 2 IDNrG sowie entsprechende Erhebungs- und Verarbeitungszwecke in § 5 und 6 IDNrG. Auffällig ist hier jedoch, dass die Datenübermittlung nicht schlicht durch einen zentralen Datenspeicher erfolgt. Im Fall einer Datenabfrage oder sonstigen Datenkommunikation zwischen zwei öffentlichen Stellen erfolgt der Zugriff erst durch Erteilung einer Berechtigung durch eine sog. Vermittlungsstelle. Bereichsspezifisch soll diese gem. § 7 Abs. 2 IDNrG gebildet werden und mittels verschlüsselter Kommunikation als Zwischenstelle für Abfragen fungieren. Die Verantwortung für die jeweilige Verarbeitungstätigkeit übernimmt dann wieder jede einzelne abrufende Stelle, § 8 Abs. 1 IDNrG. In Bezug auf das erwähnte Onlinezugangsgesetz erfolgt eng verzahnt mit dem IDNrG das Angebot eines „Datencockpits“, in dem sich „natürliche Personen Auskünfte über Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können“, § 9 OZG-E. Insgesamt greift der Entwurf damit das dänische Modell[1374] der einmaligen Informationsangabe zur Vereinfachung des Verwaltungsverfahrens („Once Only“) auf.[1375]

1372 Siehe RegModG-E (Fn. 1371), S. 1. Vertiefend auch *Nationaler Normenkontrollrat*, Stellungnahme zum Registermodernisierungsgesetz, S. 12.
1373 Siehe RegModG-E (Fn. 1371), S. 1.
1374 Hierzu *Nationaler Normenkontrollrat*, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren., S. 30 f.
1375 RegModG-E (Fn. 1371), S. 35, 38.

Konkret dient die in dieser Form ausgestaltete Identifikationsnummer dann als „Schlüssel zu gehaltvollen Informationen über eine Person. Und nicht nur irgendein Schlüssel, sondern der Generalschlüssel. Anhand von Personenkennziffern können umfassende Persönlichkeitsprofile erstellt werden."[1376] Der Grundgedanke des RegModG greift folglich das im Rahmen der Volkszählungsentscheidung des Bundesverfassungsgerichts[1377] und schon 1969 mit der Mikrozensus-Entscheidung[1378] gezeichnete Bild einer Identitätsdaten-Infrastruktur auf, das in der verfassungsgerichtlichen Rechtsprechung fortwährend abgelehnt wurde. So statuiert das Bundesverfassungsgericht ausdrücklich: „[E]ine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal [...] [ist nicht mit der Verfassung vereinbar]; denn eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig"[1379]. Rückblickend auf das 2017 veröffentlichte Gutachten des Nationalen Normenkontrollrates zur Verfassungsmäßigkeit einer einheitlichen Identifikationsnummer[1380] und die darin erwähnte Untersuchung der Deutschen Universität für Verwaltungswissenschaften in Speyer[1381] sowie jüngere kritische Stimmen[1382] in Bezug auf das RegModG bleiben dementsprechend Zweifel an der Vereinbarkeit mit dem Grundrecht auf informationelle Selbstbestimmung gem.

1376 So *von Lewinski* im Interview mit Beck-aktuell vom 10.11.2020, abrufbar unter https://rsw.beck.de/aktuell/daily/magazin/detail/einheitsnummer-fuer-jeden-buerger.

1377 BVerfGE 65, 1 (53).

1378 BVerfGE 27, 1 (6).

1379 BVerfGE 65, 1 (53).

1380 *Nationaler Normenkontrollrat*, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren., S. 40 ff

1381 *Martini*/*Wagner*/*Wenzel*, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern.

1382 *Sorge*/*Leicht*, ZRP 2020, 242 (243 f); *Deutscher Anwaltverein*, Stellungnahme zum Gesetzentwurf der Bundesregierung zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze, S. 5 ff; *Gesellschaft für Informatik*, Stellungnahme zum Registermodernisierungsgesetz, S. 2 ff; *Nationaler Normenkontrollrat*, Stellungnahme zum Registermodernisierungsgesetz, S. 8 ff.

Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Neben allgemeinen Bedenken ausgehend von der verfassungsgerichtlichen Rechtsprechung[1383] bestehen erhebliche Bedenken hinsichtlich der eingriffsabschwächenden technischen und organisatorischen Maßnahmen. Eine Umsetzung unter einen Rückgriff auf geeignete und effektive Mittel wird grundlegend bezweifelt[1384] und bestehende Ansätze des RegModG scheinen veraltet[1385], insbesondere mit Blick auf europäische Alternativmodelle. Wiederholt wird hier auf das dezentrale Modell der bereichsspezifischen Personenkennziffer in Österreich referenziert[1386], welches mit der Nutzung von Hashwerten in Verbindung mit bereichsspezifischen Kürzeln[1387] durchaus zu überzeugen weiß. Gelegentlich wird auch die bestehende Funktion der eID bzw. des elektronischen Personalausweises zum Widerruf bereichsspezifischer Kennzeichen bzw. Pseudonyme (sog. Restricted Identification – kurz rID) erwähnt[1388], jedoch nicht vertieft. Vonseiten des Normenkontrollrates, welcher die im Regierungsentwurf aufgezeigten Gründe gegen ein Übernehmen des Modells[1389] bestätigt[1390], wird hiergegen vorwiegend der hohe Zeit und Kostenaufwand angeführt; überdies sei das deutsche Modell in technischer Hinsicht überzeugender[1391].

Abseits dieser Kritikpunkte weisen sämtliche Stimmen – zutreffend – darauf hin, dass sich das Bundesverfassungsgericht sich dem Ansatz einer einheitlichen

1383 *Deutscher Anwaltverein*, Stellungnahme zum Gesetzentwurf der Bundesregierung zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze, S. 6; *Gesellschaft für Informatik*, Stellungnahme zum Registermodernisierungsgesetz, S. 2. Vgl. auch *Martini*/*Wagner*/*Wenzel*, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, S. 61 ff.

1384 *Gesellschaft für Informatik*, Stellungnahme zum Registermodernisierungsgesetz, S. 3.

1385 *Sorge*/*Leicht*, ZRP 2020, 242 (243).

1386 *Sorge*/*Leicht*, ZRP 2020, 242 (243); *Martini*/*Wagner*/*Wenzel*, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, S. 62 f, 36 ff; *Gesellschaft für Informatik*, Stellungnahme zum Registermodernisierungsgesetz, S. 4.

1387 Hierzu *Sorge*/*Leicht*, ZRP 2020, 242 (243). Weitere europäische Alternativmodelle prüfend *Nationaler Normenkontrollrat*, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren., S. 26 ff.

1388 So *Gesellschaft für Informatik*, Stellungnahme zum Registermodernisierungsgesetz, S. 4; *Sorge*/*Leicht*, ZRP 2020, 242 (243).

1389 Begründung des RegModG-E (Fn. 1371), S. 2/3, 38 f.

1390 *Nationaler Normenkontrollrat*, Stellungnahme zum Registermodernisierungsgesetz, S. 13 f.

1391 *Nationaler Normenkontrollrat*, Stellungnahme zum Registermodernisierungsgesetz, S. 13.

Identifikations- oder Personenkennziffer nicht grundlegend verschließt. Bei Lichte besehen gibt das Volkszählungsurteil durchaus Hinweise einer verfassungskonformen Umsetzung und Verwendung eines einheitlichen Identifikationsmerkmals. Unter Rückgriff auf die im Rahmen dieser Arbeit dargestellten in Art. 2 Abs. 1 iVm 1 Abs. 1 GG inkorporierten Datenschutzgrundsätze[1392] weist das Bundesverfassungsgericht auf eine enge Zweckbindung für die Erfüllung öffentlicher Aufgaben hin[1393] und fordert geeignete technische und organisatorische Maßnahmen zum Schutz der erhobenen Daten, beispielsweise eine frühe faktische Anonymisierung[1394] oder ein räumlich-technisches Abschotten der Systeme zur Erhöhung des Vertrauens in die (staatliche) Datenverarbeitung[1395]. Während das Vorhaben der Volkszählung nach Ansicht des Gerichts auch ohne Personenbezug erreichbar ist[1396], erscheint das Vorhaben des RegModG zur Minimierung des Verarbeitungs- und Kostenaufwands plausibel. Dies entbindet den Gesetzgeber allerdings nicht von der Berücksichtigung verfassungsrechtlicher Grundsätze wie den Grundsatz der Verhältnismäßigkeit aus Art. 20 Abs. 3 GG. Insofern müssen zunächst weniger invasive Mittel zur Zweckerreichung berücksichtigt werden, bevor sich einer umfassenden Abwägung der widerstreitenden Interessen gewidmet werden kann.

Hinsichtlich der Zweckerreichung – der Digitalisierung der Verwaltung einschließlich einer Fehler- und Kostenminimierung – erscheint die durch das RegModG durchaus geeignet. Dennoch muss das mildeste, aber in gleichem Maß geeignete Mittel hierfür gewählt werden. Wie erwähnt führt die Literatur hier einheitlich das österreichische Modell der bereichsspezifischen Personenkennziffer an, dessen Prüfung an dieser Stelle nicht vertieft werden soll; für entsprechende Zweifel an der Erforderlichkeit mag die breite Rezeption ausreichen.

1392 Sub D.I.1.b)aa).
1393 BVerfGE 65, 1 (45, 47 f).
1394 BVerfGE 65, 1 (49/50).
1395 BVerfGE 65, 1 (49, 50).
1396 BVerfGE 65, 1 (49).

Bestätigen sich diese Zweifel nicht, bliebe es am Gesetzgeber eine Verhältnismäßigkeit des Vorhabens im engeren Sinne vorweisen zu können. Hierbei sind insbesondere verfassungsgerichtlich herausgehobene Datenschutzgrundsätze in den Blick zu nehmen.[1397] Der Gesetzentwurf des RegModG bleibt eine entsprechende Begründung schuldig und beschränkt sich auf die Gründe der Kosteneinsparung und die Minimierung bzw. Vereinfachung des Aufwands bei der Umsetzung des OZG. „Ein registerübergreifendes Identitätsmanagement kann zudem Grundlage für einen im Aufwand und Kosten verminderten Zensus sein und damit die Bürgerinnen und Bürger von bislang erforderlichen Befragungen entlasten und Bürokratie abbauen."[1398] Dahinter verbergen sich vor allem Aspekte der Vereinfachung der Teilhabe an staatlichen Leistungen (Sozialstaatsprinzip, Art. 20 Abs. 1 GG) und der Grundsatz der Wirtschaftlichkeit und Sparsamkeit (vgl. § 7 BHO). Das Vorhalten der Basisdaten weist allerdings wegen seiner aggregierten und zentralen Speicherung eine hohe Eingriffstiefe auf. Rein pragmatische Erwägungen mögen daher nicht ausreichen, um die dadurch entstehenden Gefahren auszugleichen. Vielmehr bedarf es – wie durch das Bundesverfassungsgericht gefordert – entsprechender eingriffsminimierender Maßnahmen: Die Grundlage der Identitätsnummer, das IDNrG, begrenzt in § 1 den Nutzungszweck expressis verbis auf das Verwaltungsverfahren und den Erhalt der Datenqualität – also die Richtigkeit und Aktualität der Daten. Insoweit genügt das RegModG dem verfassungsgerichtlichen Erfordernis eines engen und klaren Zwecks; auch sind die Institutionen durch die Verarbeitungssituationen der §§ 5-7 IDNrG hieran gebunden. Dass eine nachträgliche Änderung des Zwecks und damit ein Überwachungsszenario[1399] möglich ist, kann mit Blick auf eine dann notwendige verfassungsrechtliche Vereinbarkeit des Änderungsgesetzes dahingestellt bleiben. Risikomindernd kommt das RegModG dem verfassungsgerichtlichen Transparenzerfordernis nach, indem

1397 Diese Prüfstruktur etablierend BVerfG, Beschluss v. 27.05.2020 – Az. 1 BvR 1873/13 –, Rn. 127 ff.

1398 RegModG-E (Fn. 1371), S. 35.

1399 Derartige Befürchtungen äußernd *Gesellschaft für Informatik*, Stellungnahme zum Registermodernisierungsgesetz, S. 5.

das Datencockpit eine Übersicht über die jeweiligen Datenabrufe einzelner öffentlicher Stellen bietet.[1400] Weiter führt das RegModG die Datenminimierung an, weil die partikularen behördlichen Datenspeicher sodann an einem Ort gespeichert werden sollen und folglich weniger Daten verarbeitet und angesammelt werden.[1401] Richtiger ist hier jedoch der Terminus der Daten*satz*minimierung, da eben nur die jeweiligen Infrastrukturen wegfallen. Es kann sich schon nicht um eine Datenminimierung nach datenschutzrechtlichem Verständnis handeln, da diese eine andere Zielrichtung verfolgt: Nicht nur sollen weniger Daten gespeichert, sondern auch erhoben oder auf andere Weise verarbeitet werden iSe Datensparsamkeit.[1402] Der im Entwurf festgehaltene, ehrbare Ansatz versteht das datenschutzrechtliche Gebot damit grundlegend falsch. Würde der Aspekt der Datenminimierung tatsächlich berücksichtigt, fände eine dezentrale Speicherung, eine bereichsspezifische Personenkennziffer und eine darauf aufbauende bereichsspezifische Speicherung von personenbezogenen Daten größere Berücksichtigung im Regierungsentwurf. Zwar würden auf diese Weise quantitativ mehr personenbezogene Daten erhoben. Durch eine dezentrale Speicherung wäre das Risiko im Fall eines Datenleaks jedoch geringer, mit entsprechender Verschlüsselung durch Hash-Algorithmen und Speicherung bereichsspezifisch relevanter Merkmale – also einer Reduktion des Umfangs – sinkt das Niveau weiter. Insofern fände der Grundsatz der Datenminimierung zumindest bereichsspezifisch, auf behördlicher Ebene, Anklang. Ungeachtet dessen geht der Regierungsentwurf des RegModG nicht auf die Notwendigkeit der einzelnen, für die Identitätsnummer in § 4 Abs. 2 IDNrG ein und begründet das zur Zweckerreichung notwendige Maß.[1403] Den einzelnen Datenschutz-Grundsätzen als eingriffsminimierende Maximen genügt das RegModG damit nicht in allen Punkten.

1400 Dies stellt insoweit auch die Begründung des RegMod-E (Fn. 1371) heraus, S. 36.

1401 So RegMod-E (Fn. 1371), S. 1: „Außerdem widerspricht eine redundante Datenhaltung dem Gebot der Datenminimierung."

1402 Vgl. nur BVerfGE 65, 1 (46) sowie *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG, Art. 5, Rn. 123, 127.

1403 Der Entwurf verweist lediglich auf den vorhandenen Datenbestand gem. § 139b AO – siehe RegMod-E (Fn. 1371), S. 59.

Weiter münden die einzelnen Prinzipien in einer Abwägung kollidierender verfassungsrechtlicher Interessen. So bleibt zu fragen, ob sich die staatlichen Interessen mit der Maxime des Art. 2 Abs. 1 iVm 1 Abs. 1 GG vereinbaren lassen, also die Allgemeininteressen gegenüber dem Grundrecht auf informationelle Selbstbestimmung überwiegen. Als solche ist die informationelle Privatautonomie als Schutzgut des Grundrechts auf informationelle Selbstbestimmung zu begreifen.[1404] Der Grundrechtsträger muss sich also auch einer Datenverarbeitung entziehen können; ein Zwang zur Datenabgabe kann nur innerhalb enger Grenzen erfolgen. Nur so wird ein entsprechend tiefgreifender Eingriff dem Schutz des grundrechtlichen Kerns gerecht. Vorliegend lässt sich, wie dargelegt, schon an den Eingriffsschranken und der Milderung der Eingriffstiefe zweifeln. Hinzu kommt aber die mit Erstellung des Profils und der Identifikationsnummer entzogene Kontrolle über die personenbezogenen Daten selbst. Es ist dem Betroffenen, abgesehen von einer Datenänderung zugunsten der Aktualität und Richtigkeit, nicht möglich, auf den Datensatz einzuwirken. In seiner Unausweichlichkeit kommt dem RegModG bzw. IDNrG damit eine Zwangswirkung zu, die zwar die Digitalisierung der Verwaltungsprozesse und damit dem Allgemeininteresse dient. Dennoch ist fraglich, ob und inwieweit dies – erneut ganz im Lichte der Datenminimierung und Zweckausrichtung – zu ebenjener Digitalisierung notwendig ist. Schließlich könnte eine Entlastung der Bürgerinnen und Bürger auch auf andere Weise als die Digitalisierung der Prozesse erreicht werden. Auch könnte die Nutzung der Identitätsnummer oder damit verbundener digitalisierter Verwaltungsprozesse der Bürgerin bzw. dem Bürger überlassen werden. Der Entwurf deutet dies selbst an und sieht die Übermittlung der Daten zwischen staatlichen Institutionen nur auf Basis einer Einwilligung.[1405] Die Regelungen des §§ 6, 7 IDNrG lassen diese Äußerung jedoch obsolet erscheinen, wo die Erfüllung öffentlicher (gesetzlicher) Aufgaben doch einen eigenen Rechtfertigungsgrund gem. Art. 6 Abs. 1 lit. e, Abs. 3 DSGVO iVm entsprechenden Vorschriften des IDNrG darstellt. Ohne eine Berücksichtigung dieser kritischen Reduktion digitalisierter Verwaltungsprozesse auf das Nötigste oder die echte Berücksichtigung der Einwilligung der Betroffenen

1404 Sub D.I.1.b)aa)(3). Auch BVerfGE 65, 1 (42).
1405 So RegMod-E (Fn. 1371), S. 35.

über die erstmalige Datenspeicherung kann der Regierungsentwurf des RegModG folglich auch in der Tiefe nicht überzeugen.

Das Registermodernisierungsgesetz stellt damit schon in seiner Entwurfsfassung eine Herausforderung für den verfassungsrechtlichen Schutz der digitalen Identität dar. Die aufgrund der erst aufkommenden wissenschaftlichen Diskussion nur oberflächliche Darstellung zeigt die Schwierigkeit einer verfassungskonformen Konstruktion eines staatlichen Identitätsmanagements. Jedoch bleibt angesichts verfassungsgerichtlicher Kriterien nicht vor dem Ansatz zurückzuschrecken, sondern das vorgelegte Modell kritisch im Blick zu behalten. Ob sich das Unterfangen als effektiver Schutz der digitalen Identität erweist, hängt von der weiteren Entwicklung des nunmehr umgesetzten Regierungsentwurfes in puncto technischer und organisatorischer Maßnahmen zum Schutz der vorgesehenen Kommunikations- und Speicherstruktur von Registermodernisierungsbehörde, Vermittlungsstelle und sonstigen öffentlichen Stellen ab.

4. Die Charta der digitalen Grundrechte

Den aufgezeigten einfachgesetzlichen Änderungen und Vorhaben bleibt nunmehr eine Anpassung des Verfassungsrechts gegenüberzustellen. Diese Bestrebung stammt jedoch nicht aus der Mitte des Bundestages, sondern ist gesellschaftlicher Natur: Die Charta der digitalen Grundrechte ist auf Initiative von Bürgerinnen und Bürgern entstanden und „am 5.12.2016 dem Europäischen Parlament in Brüssel und der Öffentlichkeit zur weiteren Diskussion“ vorgelegt worden.[1406] Weitere Vorschläge und Kritikpunkte wurden dann in einer neuen Version am 25.4.2018 der Öffentlichkeit zugänglich gemacht.[1407] Eine umfangreiche, rechtswissenschaftliche Diskussion blieb aus.[1408]

1406 Siehe https://digitalcharta.eu/hintergrund/.
1407 Einsehbar unter https://digitalcharta.eu.
1408 Jüngeren Datums lediglich *Golla*, DÖV 2019, 673 (677 ff).

Im Folgenden soll diese Initiative daraufhin überprüft werden, ob sie zu einem besseren Schutz der digitalen Identität führt und die Verfassung um fehlende, aber notwendige Aspekte erweitert. Dabei sei sich auf die vornehmlich persönlichkeitsrechtlichen Artikel der digitalen Grundrechte-Charta von 2018 (nachfolgend: dGrC) beschränkt.

Die Präambel der dGrC zeigt die generelle Zielstellung auf. Sie wurde verfasst „im Bewusstsein, dass die Gestaltung der digitalen Welt auch eine europäische Aufgabe sein muss, damit es im europäischen Verbund gelingt, Freiheit, Gerechtigkeit und Solidarität im 21. Jahrhundert zu erhalten [...]". Grundrechte und der digitale Wandel sollen ineinandergreifen, den Wandel aktiv reflektieren. Auffallend ist, dass die dGrC „in Anerkennung der Allgemeinen Erklärung der Menschenrechte, der Europäischen Menschenrechtskonvention, der Charta der Grundrechte der Europäischen Union [und] der Grundrechts- und Datenschutzstandards der Europäischen Union und ihrer Mitgliedsstaaten", was die dGrC als gleichrangiges Werk einordnen lässt. Sie ist demnach nicht bestrebt, eine Änderung oder Erweiterung der bestehenden EU-Grundrechtecharta herbeiführen zu wollen.

Die anschließenden Artikel der dGrC priorisieren die Würde des Menschen – wohl im Vorbild an GG und GrC – qua Benennung an erster Stelle, erweitert um den Schutz vor technischen Entwicklungen. Dies ist schon verwunderlich, ist die aktuelle Fassung von GrC (und auch GG) technikneutral, sodass es besagten Nachsatzes schon nicht bedarf. Die dynamische Auslegung der Grundrechte zeigt damit keine Notwendigkeit der Digital-Charta in diesem Punkt.

Artikel 2 der dGrC soll scheinbar das Subsidiaritätsverhältnis des Art. 2 Abs. 1 GG, aber auch des Art. 6 GrC, aufgreifen und ein digitales Auffanggrundrecht manifestieren. Danach hat jeder „ein Recht auf freie Information und Kommunikation." Hierin münden die Informations- und Kommunikationsfreiheit des Art. 5 Abs. 1 S. 1 GG, Art. 11 Abs. 1 GrC. Auch diese Grundrechte sind technikneutral anzuwenden; überdies ist das kodifizierte „persönliche Recht auf Nichtwissen" bereits im status negativus der bestehenden Grundrechte aufgefangen. Eine dahingehende Notwendigkeit einer Umformulierung ist auch hier nicht zu sehen. Weshalb die Kommunikation sodann in Art. 4 dGrC durch ein Grundrecht auf

digitale Meinungsfreiheit konkretisiert bzw. gedoppelt wird ist nicht nachvollziehbar. Auch inwiefern Art. 1 und 2 dGrC zueinander stehen, ob diese in Verbindung ein digitales Persönlichkeitsrecht bilden und dadurch besondere Gefahrenlagen des digitalen Alltags reflektieren, ist nicht ersichtlich. Ein Immaterialgüterrecht ist zwar vorgesehen (Art. 16 dGrC), bezieht sich allerdings vielmehr auf urheberrechtliche bzw. wirtschaftliche Interessen. Entsprechende Bezüge können also auch nicht hieraus gewonnen werden.

Der Artikel 5 dGrC steht im Zeichen der künstlichen Intelligenz und fordert gem. Abs. 2: „Automatisierte Entscheidungen müssen von natürlichen und juristischen Personen verantwortet werden.“, verstärkt die Benennung des Menschen als Entscheidungstäger bzgl. Leben, körperliche Unversehrtheit und Freiheitsentzug in Abs. 5. In beiden Fällen sollen „[e]thisch-normative Prinzipien“ maßgeblich sein. Dass Eingriffe in Grundrechte nur von Menschen getroffen werden können – so statuiert Abs. 1 – ist vor dem Hintergrund der Gewalten und Bundesorgane, dem bestehenden Wahlsystem und exemplarisch der Bindungswirkung der Verfassung für diese Entscheidungsträger gem. Art. 1 Abs. 3, 20 Abs.2 GG nur logisch. Um hoheitliche automatisierte Entscheidungen zu ermöglichen bedürfe es zahlreicher Anpassungen, allein durch eine Änderung des § 15 BWahlG. Darüber hinaus schließt das Menschenbild des Grundgesetzes diese Art der Lebensform aus.[1409] Ein Schutz der digitalen Identität kann daher nur daraus folgen, dass die automatisierte Verarbeitung personenbezogener Daten zu Profilen ebenfalls ethisch-normativen Prinzipien unterliegt. Dies ist aber mit den Bestrebungen der Datenethikkommission[1410] und der durch GG und GrC vorgegebenen Normen- und Wertordnung bereits gegeben, sodass ein Hinwirken hierauf qua dGrC nicht sinnvoll erscheint.

In Artikel 7 und 8 dGrC widmet sich das Werk einer Reflexion des Grundrechts auf informationelle Selbstbestimmung und dem GGVIS. So statuiert Art. 7 Abs. 3

1409 Vgl. sub B.IV.1.

1410 Exemplarisch hierzu das Gutachten der Datenethikkommission, siehe https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf?__blob=publicationFile&v=5.

„Rechte auf Löschung, Berichtigung, Widerspruch, Information und Auskunft“ und Abs. 4 das „Recht auf digitalen Neuanfang“. Beide sind nunmehr umfassend durch Vorschriften der DSGVO einfachgesetzlich festgehalten und ohnehin Teil der verfassungsgerichtlichen Rechtsprechung bzw. der informationellen Selbstbestimmung des Art. 2 Abs. 1 iVm 1 Abs. 1 GG[1411]. Auch benennt Art. 7 Abs. 5 den Schutz der Privatsphäre innerhalb von Wohnungen – also Art. 13 Abs. 1 GG und Art. 7, 8 GrC – und aktiven Schutz der Kommunikation – also Art. 10 Abs. 1 GG und Art. 7, 8 GrC. Damit greift die Digital-Charta erneut nur bestehende Grundsätze auf, entwickelt sie aber nicht neu. Dies spiegelt sich auch in Art. 8 dGrC wieder, welcher die „Unversehrtheit, Vertraulichkeit und Integrität informationstechnischer Systeme und Infrastrukturen“ schützt. Er benennt im Wortlaut auch die gewährleistende Aufgabe des Staates. Die Definition des Grundrechts entspricht jedoch dem erläuterten Systemschutz des GGVIS[1412] gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG, auch in seiner gewährleistenden Aufgabe. Damit ergibt sich auch hier keine Differenz zwischen GG, GrC und Digital-Charta.

Schlussendlich muss sich mangels signifikanter Abweichung nicht eines neuen, innovativen Schutzniveaus zugunsten digitaler Identitäten bedient werden. Das Schutzniveau der dGrC entspricht bereits geltenden (unions-)verfassungsrechtlichen Grundsätzen und -rechten, sodass die Bestrebungen der Charta der digitalen Grundrechte weder praktikabel noch wertvoll erscheinen. Ein weiteres Gesetzeswerk mit speziellen Grundrechten ignoriert die bestehende Grundrechtsdogmatik und führt zu einer horizontalen und vertikalen Zweigleisigkeit. Diese ist jedoch inhaltlich eingleisig, weil es sich um selbige Grundrechte in neuer Anordnung oder Formulierung handelt. Es handelt sich also nicht um eine „echte“ Korrekturbestrebung, die den bestehenden Grundrechtsschutz inhaltlich oder systematisch

1411 So nach der hier vertretenen Auffassung, sub D.II.3.. Im Fall von personenbezogenen Berichten als Teil von Kommunikationsprozessen dem Allgemeinen Persönlichkeitsrecht zuordnend BVerfG, Beschluss vom 6.11.2019 – Az. 1 BvR 16/13 – Rn. 105 ff = K&R 2020, 51 (54 f).

1412 Sub D.II.3.

erweitert. Mit den Worten von *Golla*: „[D]as Projekt Digitalcharta insgesamt erscheint in seiner aktuellen Form nur noch wenig aussichtsreich."[1413]

5. Zusammenfassung der Korrekturansätze

Insgesamt betrachtet, finden sich in den Korrekturansätzen nur punktuell zu befürwortende Maßnahmen, die die im Rahmen der Untersuchung herausgearbeiteten verfassungsrechtlichen Schutzrichtungen einfachgesetzlich abbilden. Allen Ansätzen gemein ist die breite Adressierung an personenbezogene wie nichtpersonenbezogene Datensätze. Jedoch ebenso sehen alle Vorhaben keine konkreten Maßnahmen oder Ansätze vor, diese Begriffe durch gesetzliche Regelungen oder untergesetzliche Maßnahmen voneinander zu trennen und so Rechtsklarheit für Unternehmen oder Wissenschaft und Forschung zu schaffen. Vielmehr beschränken sich die Vorhaben national wie auf europäischer Ebene auf die Einrichtung eines Datenmarktes. Diesen auf einer bis dato ungeklärten Sachlage für die mit den Märkten zu erreichenden Kräfte einzurichten erscheint überaus gewagt. Ähnlich fraglich wirkt der Ansatz, das BSI durch ein IT-Sicherheitsgesetz 2.0 mit Zugriffsbefugnissen auf ungeschützte Systeme auszustatten, ohne das verfassungsrechtliche Zitiergebot gem. Art. 19 Abs. 1 S. 2 GG oder verfassungsgerichtliche Vorgaben zu berücksichtigen. Die beabsichtigte verbraucherschützende Ausrichtung des Ministeriums vermag nicht die mangelnde Unabhängigkeit oder fehlende Mindeststandards zum Schutz auch nicht-technikaffiner Bürgerinnen und Bürger ausgleichen. Die überdies geplante Einführung einer einheitlichen Identifikationsnummer ergänzt diese Schattenseiten der Vorhaben, wenn das Vorhaben aufgrund seiner technische wie organisatorisch fragwürdigen Umsetzung nicht mit den Grundsätzen der Volkszählungsentscheidung des BVerfG in Einklang steht. Auch wenn es sich dabei um staatlich eingeführte digitale Identitäten handelt, weißt der gesetzliche Rahmen bislang keinen hinreichenden Schutz auf. Die

1413 *Golla*, DÖV 2019, 673 (681); ähnlich bereits *Engeler* zur Version von 2016 im Telemedicus-Blog unter https://www.telemedicus.info/article/3154-Unstable-Der-Digitalcharta-fehlt-ihr-Datenschutz-Fundament.html.

dargestellten Korrekturansätze de lege ferenda halten damit – soweit ersichtlich – eher Gefährdung als effektiven Schutz der digitalen Identität bereit.

IV. Postremo: Die Zukunft der digitalen Identität

Der verfassungsrechtliche Boden, durch den die digitale Identität gesichert ist, scheint vor dem Hintergrund einfachgesetzlicher Korrekturvorhaben ins Wanken zu geraten. Es scheint ungewiss, ob entsprechende klärungsbedürftige Punkte berücksichtigt werden und darüber hinaus eine effektive Gewährleistung im Rahmen der Datenstrategien eintritt. Schon in dieser Hinsicht bleibt die begriffliche Klärung zwischen Anonymität und Pseudonymität inter- und intradisziplinär zu diskutieren, auch wiederholt in den Diskurs einzubringen. Unbeständig bleibt ebenso das Schutzniveau in technischer Hinsicht für Jedermann, da trotz datenschutzrechtlicher Prinzipien ein technischer Datenschutz von finanziellem Leistungsvermögen (z.B. Apple-Geräte mit eingebautem T2-Sicherheitschip für die sog. Secure Enclave[1414]) oder Technikkenntnissen (z.B. eigene Implementierung von Open-Source-Lösungen) abhängt. Diese Beobachtung läuft dem Schutzsystem des Art. 2 Abs. 1 iVm 1 Abs. 1 GG zuwider und erschwert eine technische wie informationelle Selbstbestimmung über die eigene digitale Identität.

Exemplarisch für diese Erschwernis können die Ereignisse um den Coronavirus COVID-19 in den Blick genommen werden: Zur Durchbrechung der Infektionsketten sollte eine Applikation für Mobiltelefone entwickelt werden, die auf dem Bluetooth-Low-Energy-Standard aufsetzt und nicht-personenbezogene Schlüsselketten als sog. Beacon versendet. Wiederum zeichnet das Gerät selbst die erhaltenen Ketten auf und bildet – wenn auch nicht auflösbar – ein Abbild über die

1414 Siehe hierzu nur https://support.apple.com/de-de/HT208862.

Kontakte mit anderen Menschen,[1415] also eine digitale Identität auf Basis sozialer Kontakte. Vermieden werden sollte aber eine Speicherung personenbezogener Daten, da das Datum der Infektion mit dem Virus ein gesellschaftlich bedeutendes wie rechtlich besonderes personenbezogenes Datum darstellt. Wann es sich jedoch nicht mehr um ein personenbezogenes Datum handelt, wurde unterschiedlich aufgefasst; auch wurde in der Berichterstattung Pseudonymisierung mit Anonymisierung und anonymen Daten stets vermischt.[1416] Die fehlende terminologische Klarstellung führte so zu mangelndem Vertrauen in die eingangs erläuterte, rechtskonforme Variante der Applikation sowie auf wissenschaftlicher Ebene zu Ungewissheit.[1417] Mit Blick auf die Bluetooth-Schnittstelle bleibt zu bedenken, dass diese nur mit Bluetooth 4.0 kompatiblen Chips möglich ist. Ältere Geräte unterstützen die Anwendung folglich nicht; Menschen mit nicht kompatiblen Geräten oder gar ohne Smartphone sind „technisch abgeschnitten". Damit kann die Anwendung auch nicht in der breiten Masse verwendet oder gar hierzu verpflichtet werden. Die Pandemie offenbart folglich die bereits im Rahmen dieser Arbeit herausgearbeiteten Kulminationspunkte: Fehlende terminolgische Klarstellung, keine einheitlichen oder offene Standards oder eine entsprechende Verbreitung dieser zwecks Interoperabilität, und eine rechtliche Regulierung der Verwendung dieser Daten durch Private. Schließlich könnte die Anwendung ohne eine entsprechende Regelung zur unkontrollierbaren Zugangsschranke für lebenswichtige Güter wie Nahrungsmittel werden.

Die Zukunft der digitalen Identität ist damit keine ruhige, sondern eine turbulente und spannende. Sie bleibt weiterhin Forschungs-, Diskussions-, Legislativ- und

1415 Zur Funktionsweise im Detail siehe https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf.

1416 Vgl. hierzu die Berichterstattung um die erhobenen Daten der COVID-19-Applikation des Robert-Koch-Instituts, z.B. bei t3n (https://t3n.de/news/uebersicht-so-funktionieren-drei-corona-apps-datenspende-rki-pepp-pt-1272238/), Deutschlandfunk Nova (https://www.deutschlandfunknova.de/beitrag/ccc-kritisiert-rki-app-datenspende-app-ist-zu-freigiebig) anonym und nach Tagesschau (https://www.tagesschau.de/inland/app-rki-101.html) und Webseite des Robert-Koch-Instituts pseudonym (https://corona-datenspende.de/faq/).

1417 Hierzu ausführlich die Erhebung im Rahmen des Forschungsprojekts PANDIA: *Meyer/Fröhlich/von Holdt*, Corona-Warn-App – Erste Ergebnisse einer Online-Umfrage zur (Nicht-)Nutzung und Gebrauch, 27 f.

Schutzgegenstand. Diese Arbeit schließt daher mit dem abgewandelten Zitat zu Beginn dieser Arbeit:

Die **digitale Identität** ist **nicht** nur ein Hype.

Thesen der Arbeit

Die nachfolgenden Thesen fassen diese wissenschaftliche Arbeit zusammen und heben die eigenen Forschungsergebnisse der Untersuchung hervor.

1. Digitale Identitäten sind miteinander verknüpfte Daten (dann: Teilidentität) oder Datensätze (dann: Gesamtidentität), die sich durch ihren hohen Aussagegehalt in ihrer aggregierten Form auszeichnen. Meistens sind sie mit einer Kennung bzw. einem Identifier versehen, können aber auch selbst als solches fungieren (dann: Quasi-Identifier).

2. In ihrem Aussagegehalt bilden sie Teile und Wesenszüge der analogen Identität ab, können aber ebenfalls fiktive Züge oder Charaktere widerspiegeln. Letztere Variante kann aber einem eigenständigen Schutz unterliegen, wenn diese sich als Alter Ego in Form einer virtuellen Identität ohne Bezug zum Persönlichkeitskern konkretisieren.

3. Sowohl natürliche als auch juristische Personen des Privatrechts iSd Art. 19 Abs. 3 GG können über digitale Identitäten verfügen.

4. Der Begriff der digitalen Identität ist nicht kongruent mit dem (datenschutzrechtlichen) Konstrukt des Persönlichkeitsprofils, da sich dieses ausschließlich auf natürliche Personen erstreckt. Ebenso deckt es nicht das Spektrum an Datentypen sowie den Datenlebenszyklus ab.

5. Der in der Literatur gelegentlich verwendete Begriff der virtuellen Identität, also die wiederholte und konsistente Repräsentation einer Person im digitalen Raum, geht in der Definition der digitalen Identität auf; vielmehr ist eine digitale Identität „virtuell“, wenn digitale und analoge Persönlichkeit

voneinander losgelöst sind, z.B. mangels Personenbezug oder Persönlichkeitskern.

6. Die digitale Identität richtet sich am Lebenszyklus von Daten sowie den einzelnen Lebensabschnitten des Menschen aus; sie bildet auch die pränatale wie postmortale Phase ab.

7. Das Verfassungsrecht schützt pränatale Aspekte der digitalen Identität, jedoch zunächst mittelbar als Teil des elterlichen Erziehungsrechts gem. Art. 6 Abs. 2 GG. Hinzu tritt ein Schutz der pränatalen Persönlichkeit (z.B. in Form von Ultraschall-Bildern) gem. Art. 1 Abs. 1 GG als Vorwirkung des später erwachsenden Persönlichkeitsrechts.

8. Postmortale Aspekte der digitalen Identität schützt die Verfassung über eine prämortale Reflexwirkung des Grundrechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Weiter besteht für Datenhüllen oder -reste Verstorbener ein postmortales Datenschutzrecht, das ebenfalls in Art. 2 Abs. 1 iVm 1 Abs. 1 GG verankert ist.

9. Digitale Identitäten juristischer Personen des Privatrechts bilden die Corporate Identity eines Unternehmens im digitalen Raum ab. Ein Schutz erfolgt hier ebenfalls über die Dauer eines Datenlebenszyklus gem. Art. 19 Abs. 3 GG iVm dem spezifischen, im Einzelfall wesensmäßig anwendbaren Grundrecht.

10. Öffentlich-rechtliche juristische Personen können zwar über digitale Identitäten verfügen. Allerdings finden sich keine geeigneten Schutzkonzepte im Rahmen des Art. 19 Abs. 3 GG; sowohl die grundrechtliche Gefährdungslage oder die Durchgriffsthese lassen sich nicht erfolgreich anwenden. Insofern besteht rechtliche Ungewissheit.

11. Künstliche digitale Identitäten – deren Identität sich rein aus einem Quellcode speist oder die im Fall künstlicher Intelligenzen generiert wird – sind nicht mit bestehenden verfassungsrechtlichen Schutzkonzepten vereinbar. Weder Aspekte der Menschenwürde des Art. 1 Abs. 1 GG noch jene des Art. 19 Abs. 3 GG sind übertragbar. Auch die mangelnde Kontrolle über

diese Identitäten führt nicht dazu, dass der Tierschutz des Art. 20a GG übertragbar ist. Der Ansatz der ePerson vermag hieran nichts zu ändern.

12. Schon die übergeordneten Schutzkonzepte der verfassungsrechtlichen Grundrechte – status negativus, status positivus und Schutzpflichten-Dogmatik – kommen dem Schutz der digitalen Identität zugute. Sie unterstützen in ihrer heutigen Ausformung ein dynamisches Verständnis der Verfassung und ermöglichen im Einzelfall Möglichkeiten der Abwehr und Teilhabe am digitalen Leben mittels digitaler Identitäten.

13. Das Grundrecht auf informationelle Selbstbestimmung schützt die digitale Identität natürlicher Personen in den einzelnen Facetten. Es erstreckt sich über das gesamte Spektrum an Datentypen, also auf anonyme und anonymisierte, pseudonyme und pseudonymisierte sowie unmittelbare Informationen bzw. personenbezogene Daten. Anonyme bzw. anonymisierte Datensätze sind aufgrund ihres Restrisikos und der damit verbundenen Gewährleistung des aus der Anonymität erwachsenden Schutzes mit in den Schutzbereich aufzunehmen und der genuine, fließende Übergang zwischen den Arten in der Prüfung der Verhältnismäßigkeit im engeren Sinne zu berücksichtigen. Als Leitlinie kann hier das etablierte Prüfungsmuster der Sphärentheorie des Allgemeinen Persönlichkeitsrechts übernommen werden: Je näher der informationelle Gehalt der digitalen Identität der Menschenwürde ist, desto schützenswürdiger ist das Interesse des Grundrechtsträgers und desto höher ist es zu gewichten.

14. Ein besonderer Schwerpunkt im Schutz der digitalen Identität durch das Grundrecht auf informationelle Selbstbestimmung liegt in der Variante des Schattenprofils. Beispielsweise entsteht diese Variante durch den (kombinierten) Einsatz von Browser-Fingerprinting, Cookie-Analyse und weiteren Formen des Webtrackings. Wegen seines Anknüpfungspunktes in der Unkenntnis des Inhabers der digitalen Identität und der darauf basierenden weitreichenden Aussagekraft aggregierter Datensätze und Verhaltensanalyse über Webseiten hinweg entsteht ein Abbild der Persönlichkeit, also eine besonders schutzwürdige digitale Identität.

15. Nicht stets dem verfassungsrechtlichen Schutz unterliegen synthetisierte Datensätze aufgrund ihres mangelnden Persönlichkeitskerns. Ist durch die Angreifbarkeit der Synthetisierung allerdings eine Auflösbarkeit möglich, gilt das zu anonymisierten Datensätzen Gesagte. Ein eigenständiger Schutz iSe Alter Ego – z.B. durch das Urheberrecht und das Eigentumsgrundrecht des Art. 14 Abs. 1 GG – bleibt hiervon unberührt.

16. Die digitale Identität natürlicher Personen findet keinen Schutz in der Gestalt eines Dateneigentums über den Eigentumsschutz des Art. 14 Abs. 1 GG. Die unter dem Stichwort des Dateneigentums geführte Diskussion verfehlt den eigentlichen Kern der Debatte, das Schutzgut der Datensouveränität als Kulminationspunkt des Grundrechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 iVm 1 Abs. 1 GG. Der Ansatz eines Eigentums an personenbezogenen Daten ist grundlegend abzulehnen; für nicht-personenbezogene (Maschinen-)Daten besteht eine Prärogative des Gesetzgebers.

17. Eine postmortale Schutzrichtung in Form des digitalen Nachlasses ist in eine vermögensrechtliche Komponente des Art. 14 Abs. 1 GG sowie eine persönlichkeitsrechtliche bzw. datenschutzrechtliche Komponente des Art. 2 Abs. 1 iVm 1 Abs. 1 GG aufzugliedern. Ersteres bedarf mit Blick auf die Diskussion um § 2047 Abs. 2 und § 2373 S. 2 BGB einer erbrechtlichen Klarstellung durch die Gesetzgebung. Informationell ist dagegen (erneut) auf die Leitlinie der Sphärentheorie zurückzugreifen, um eine Einschätzung von persönlichen Accounts vorzunehmen zu können. Beispielsweise könnte so zwischen öffentlich zugänglichen Inhalten und privaten oder intimen Teilen des Dienstes (z.B. Messenger) differenziert werden. Im Übrigen sollte die prämortale Reflexwirkung des postmortalen Daseins der digitalen Identität in der Gesetzgebung stärker berücksichtigt werden, um einer Zersplitterung der Umsetzung etwaiger Nachlass-Modi in Sozialen Netzwerken vorzubeugen.

18. Eine mögliche Schutzrichtung kann sich bei entsprechender Ausgestaltung aus der Berufsfreiheit des Art. 12 Abs. 1 GG ergeben, wenn die digitale Identität natürlicher Personen im Beschäftigtenkontext Teil der Arbeitsleistung wird. Die dafür notwendigen Grundlagen müssen die unternehmerischen Interessen der Art. 12 Abs. 1, 14 Abs. 1 GG mit den kollidierenden Interessen von Beschäftigten aus Art. 2 Abs. 1 iVm 1 Abs. 1 GG entsprechend in Einklang gebracht werden.

19. Die digitale Identität juristischer Personen des Privatrechts iSv Art. 19 Abs. 3 GG findet ihren Schutz ausgehend von einem Unternehmenspersönlichkeitsrecht. Verfassungsrechtlich ist dieses reflektiert in einem Trias aus Art. 14 Abs. 1 (vermögensrechtliche Aspekte, insbes. Recht am eingerichteten und ausgeübten Gewerbebetrieb), 12 Abs. 1 (Aspekte einer unternehmerischen Handlungsfreiheit, z.B. in der Außendarstellung) und 2 Abs. 1 (persönlichkeitsrechtliche bzw. privatautonome Aspekte – ohne Bezüge zu Art. 1 Abs. 1 GG) des Grundgesetzes. Die digitale Identität entsprechender juristischer Personen ist in informationeller Hinsicht allerdings nur mittelbar über die Aspekte aus Art. 14 Abs. 1 und 12 Abs. 1 GG geschützt. Artikel 2 Abs. 1 GG fängt als subsidiäres Unternehmensrecht dagegen die (digitale) Geschäftsehre und etwaige neuartige Gefahrenlagen des Online-Diskurses auf. Letztlich fungiert Art. 2 Abs. 1 GG damit als Bindeglied zwischen Art. 12 Abs. 1 und 14 Abs. 1 GG.

20. In technischer Hinsicht deckt das Verfassungsrecht den Schutz digitaler Identitäten vornehmlich durch die beiden Grundrechte des Art. 2 Abs. 1 iVm 1 Abs. 1 GG – namentlich das Grundrecht auf informationelle Selbstbestimmung sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (kurz: GGVIS) – ab. Beide Grundrechte wirken zusammen und ergänzen einander in Form der Schutzrichtung der Datensicherheit (dann Teil des Grundrechts auf informationelle Selbstbestimmung) und der Systemsicherheit (dann GGVIS). Die Datensicherheit ist dabei nur ein flankierendes Element, das die Möglichkeit der Autonomie über die eigenen personenbezogenen Daten technisch unterstützt. Die Systemsicherheit bildet dagegen die Integrität des technischen

Korpus ab, aus der sich ein Vertrauen in das System als solches speist – definiert sich jedoch weiter als der dem GGVIS eigene Fokus auf potentiell persönlichkeitsbezogene IT-Systeme. Ein bloß mittelbarer Schutz ergibt sich aus der Vertraulichkeit der fernmeldetechnischen Kommunikation (z.B. von Identitätsdatensätzen) gem. Art. 10 Abs. 1 Var. 3 GG. Kaum von Relevanz ist der Schutzumfang des Art. 13 Abs. 1 GG, da dieser nur die räumlich umgrenzte Privatheit der Kommunikation berücksichtigt.

21. Die einfachen Gesetze decken den Schutz digitaler Identitäten natürlicher Personen sowie juristischer Personen des Privatrechts de lege lata nur partiell ab. Offen bleiben eine Begriffsklärung hinsichtlich anonymer bzw. anonymisierter Daten sowie eine Vereinheitlichung der IT-Sicherheits-Standards zugunsten des Verbraucherschutzes. Diese muss sich aber sowohl auf Systeme mit wie ohne Persönlichkeitsbezug erstrecken, um letztere nicht als Einfalltore in private, vernetzte Endgeräte umzufunktionieren. Insgesamt besteht also entsprechender legislativer Spielraum, der angesichts der grundrechtsgewährleistenden Aufgabe qua Schutzpflichten auszufüllen ist.

22. Die datenstrategischen Vorhaben der EU sowie Bundesregierung deuten eine Fokussierung auf die Nutzung und Kommerzialisierung digitaler Identitäten und persönlichkeitsbezogener Datensätze an. Die europäische Strategie setzt daher einen deutlich wirtschaftlichen Schwerpunkt und fokussiert sich auf die Interoperabilität und Zugänglichmachung personenbezogener Daten. Erste Ansätze zeigen sich jedoch in der breiten Offensive der EU Ende 2020 durch Digital Services Act, Digital Markets Act und den Data Governance Act. Gerade letzterer benennt das Vorhaben einer Datentreuhand-Stelle sowie die aktive Förderung von Plattformen zur Verwaltung persönlicher Informationen bzw. Daten (sog. personal information management systems, kurz PIMS). Hierauf aufbauend plant auch die Bundesregierung nunmehr die Förderung von Forschung in diesem Bereich, allerdings keine weiteren Gesetzesvorhaben. Höchstens in der Vermittlungsstelle des Registermodernisierungsgesetzes kann eine solche Datentreuhand gesehen werden. Dieser infrastrukturelle Ansatz wird jedoch durch das Kernstück, die einheitliche Identifikationsnummer, in Rekurs auf

die Volkszählungsentscheidung des BVerfG in seiner verfassungsrechtlichen Konformität untergraben. Die datenschutzrechtlichen Vorhaben deuten also auch einen Schutz de lege ferenda an, wenngleich dieser hinsichtlich des Registermodernisierungsgesetzes mit kritischem Blick zu verfolgen ist.

23. Aus der Richtung des IT-Sicherheitsrechts existieren zwar relevante Vorhaben, die jedoch einen ambivalenten Schutz der digitalen Identität in technischer Hinsicht erahnen lassen. Ambivalent, weil das IT-Sicherheitsgesetz 2.0 in der Kabinettsfassung mit einem freiwilligen IT-Sicherheitskennzeichen und dem BSI als allgemeine Meldestelle für IT-Sicherheitsvorfälle durchaus einen schützenden Charakter ausstrahlt. Dem wirken jedoch Eingriffsbefugnisse auf potentiell maliziöse IT-Systeme entgegen. Auch die weiterhin fehlende Unabhängigkeit der Behörde lässt die Meldestellen-Eigenschaft nur minder positiv wirken, wo die Nähe zum Bundesministerium des Innern eine Verbindung von IT-Sicherheits-Schwachstellen und dem Ministerium unterstellten Ermittlungsbehörden entsprechendes Misstrauen weckt. Ein Schutz der digitalen Identität de lege ferenda ist damit kaum ersichtlich.

Literaturverzeichnis

Abdollahpouri, Alireza/Qavami, Reyhan/Moradi, Parham: On the synthetic dataset generation for IPTV services based on user behavior, Multimedia Tools and Applications 2018, 8475.

Ahlberg, Hartwig/Götting, Horst-Peter/Lauber-Rönsberg, Anne (Hrsg.): BeckOK Urheberrecht, 32. Aufl., C.H. Beck, Stand: 15.09.2021 (zit.: *Bearbeiter* in: Ahlberg/Götting/Lauber-Rönsberg, BeckOK UrhR).

Albers, Marion: Grundrechtsschutz durch Privatheit, DVBl 2010, 1061–1069.

Albrecht, Jan Philipp/Jotzo, Florian: Das neue Datenschutzrecht der EU, Nomos Verlag 2017.

Alexander, Christian: Digitaler Nachlass als Rechtsproblem?, K&R 2016, 301–307.

Alexy, Robert: Theorie der Grundrechte, suhrkamp taschenbuch wissenschaft 1994.

Arens, Tobias: Postmortaler Datenschutz und die Datenschutz-Grundverordnung, RDV 2018, 127–132.

Artikel 29-Datenschutzgruppe: Opinion 4/2007 on the concept of personal data, 2007 – abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

Artikel 29-Datenschutzgruppe: Guidelines on the implementation of The Court of Justice of the European Union Judgment on „Google Spain and Inc v.

Agencia Española de Protección de Datos (AEPD) and Mario Costeja González“ C-131/12, 2014 – abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (zit.: *Artikel 29-Datenschutzgruppe*, WP 225).

Artikel 29-Datenschutzgruppe: Opinion 05/2014 on Anonymisation Techniques, 2014 – abrufbar unter https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Artikel 29-Datenschutzgruppe: Guidelines on the right to data portability, 2017 – abrufbar unter http://ec.europa.eu/newsroom/document.cfm?doc_id=44099 (zit.: *Artikel 29-Datenschutzgruppe*, WP 242 rev.01).

Auer-Reinsdorff, Astrid: Schutz von Datenbanken und Datenbankwerken, in: Conrad, Isabell/Grützmacher, Malte (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, Otto Schmidt Verlag 2014, S. 205–228 (zit.: *Auer-Reinsdorff*, FS Schneider).

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.): Handbuch IT- und Datenschutzrecht, 3. Aufl., C.H. Beck 2019.

Axer, Peter: Eigentumsschutz für wirtschafliche Betätigung – Zum Grundrechtsschutz von Unternehmen gegen staatliche Wirtschaftsregulierung, in: Depenheuer, Otto et al. (Hrsg.), Nomos und Ethos: Hommage an Josef Isensee zum 65. Geburtstag von seinen Schülern, Duncker & Humblot Verlag 2002, S. 121–148 (zit.: *Axer*, FS Isensee (2002)).

Bachof, Otto/Heigl, Ludwig/Redeker, Konrad (Hrsg.): Verwaltungsrecht zwischen Freiheit, Teilhabe und Bindung – Festgabe aus Anlaß des 25jährigen Bestehens des Bundesverwaltungsgerichts, C.H. Beck 1978 (zit.: *Bearbeiter* in: Bachof/Heigl/Redeker, Festgabe BVerwG).

Badura, Peter: Grundpflichten als verfassungsrechtliche Dimension, DVBl 1982, 861–870.

Balaban, Silvia et al.: Whitepaper zur Rechtslage der IT-Sicherheitsforschung, FZI Karlsruhe 2021 – abrufbar unter https://sec4research.de/assets/Whitepaper.pdf.

Bantlin, Franziska: Grundrechtsschutz bei Telekommunikationsüberwachung und Online-Durchsuchung, JuS 2019, 669–673.

Bartsch, Michael: Daten als Rechtsgut nach § 823 Abs. 1 BGB, in: Conrad, Isabell/Grützmacher, Malte (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, Otto Schmidt Verlag 2014, S. 297–302 (zit.: *Bartsch*, FS Schneider).

Baumann, Horst: Die Vereinigungs- und Berufsfreiheit der juristischen Person, BB 1997, 2281–2288.

Baumbach, Adolf/Hopt, Klaus (Hrsg.): Handelsgesetzbuch, 40. Aufl., C.H. Beck 2021 (zit.: *Bearbeiter* in: Baumbach/Hopt, HGB).

Baumgartner, Ulrich/Hansch, Guido: Onlinewerbung und Real-Time-Bidding, ZD 2020, 435–439.

Baumgartner, Ulrich/Sitte, Konstantin: Abmahnungen von DS-GVO-Verstößen, ZD 2018, 555–560.

Bäumler, Helmut/Mutius, Albert von (Hrsg.): Anonymität im Internet, vieweg Verlag 2003.

Becker, Maximilian: Ein Recht auf datenerhebungsfreie Produkte, JZ 2017, 170–181.

Beise, Clara: Datensouveränität und Datentreuhand, RDi 2021, 597–604.

Benassi, Günter/Eichholz, Reinald: Grundgesetz und Kinderrechte, DVBl 2017, 614–620.

Bender, Albrecht: Das postmortale allgemeine Persönlichkeitsrecht: Dogmatik und Schutzbereich, VersR 2001, 815–825.

Berberich, Matthias: Virtuelles Eigentum, Mohr Siebeck 2010.

Berberich, Matthias/Golla, Sebastian J.: Zur Konstruktion eines „Dateneigentum" – Herleitung, Schutzrichtung, Abgrenzung, PinG 2016, 165–176.

Berger, Ariane: Digitales Vertrauen – Eine Verfassungs- und verwaltungsrechtliche Perspektive, DVBl 2017, 804–808.

Berghäuser, Gloria: Sach- und Datenhehlerei – eine vergleichende Gegenüberstellung der §§ 202d, 259 StGB, JA 2017, 244–251.

Bethge, Herbert: Aktuelle Probleme der Grundrechtsdogmatik, Der Staat 24 (1985), 351–382.

Bethge, Herbert: Die Grundrechtsberechtigung juristischer Personen nach Art. 19 Abs. 3 Grundgesetz, Universitätsverlag Passavia 1985 (zit.: *Bethge*, Grundrechtsberechtigung juristischer Personen).

Bethge, Herbert: Der Grundrechtseingriff, VVDStRL 57 (1998), 7–52.

Bethge, Nadine: Die verfassungsrechtliche Zulässigkeit des Grundrechtsverzichts, Verlag Dr. Kovač 2014.

Beyerer, Jürgen/Müller-Quade, Jörn/Reussner, Ralf: Karlsruher Thesen zur Digitalen Souveränität Europas, DuD 2018, 277–280.

Bisges, Marcel: Personendaten, Wertzuordnung und Ökonomie – Kein Vergütungsanspruch Betroffener für die Nutzung von Personendaten, MMR 2017, 301–306.

BITKOM (Hrsg.): Web Identitäten – Begriffsbestimmung und Einführung in das Thema, 2005 (zit.: *BITKOM*, Web Identitäten).

BITKOM: Digitale Souveränität, DuD 2018, 294.

Bizer, Johann: Kryptokontroverse – Der Schutz der Vertraulichkeit in der Telekommunikation, DuD 1996, 5–14.

Bizer, Johann: Datenschutz als Gestaltungsaufgabe, DuD 2007, 725–730.

Bleckat, Alexander: Das Dateneigentum und die E-Person, RDV 2019, 114–116.

Bleckmann, Albert: Probleme des Grundrechtsverzichts, JZ 1988, 57–108.

Bleckmann, Albert/Helm, Franziska: Die Grundrechtsfähigkeit juristischer Personen, DVBl 1992, 9–15.

Bleuler, Manfred: Schizophrenie als besondere Entwicklung, in: Dörner, Klaus (Hrsg.), Neue Praxis braucht neue Theorie, Verlag Jakob van Hoddis im Förderkreis Wohnen, Arbeit, Freizeit 1987, S. 13 ff.

Bock, Kirsten: Schutzgut des Datenschutzrechts – eine Replik auf Veil, Schutzgutmisere – Teil I, 2019 – abrufbar unter https://www.cr-online.de/blog/2019/03/22/schutzgut-des-datenschutzrechts-eine-replik-auf-veil-schutzgutmisere-teil-i/ (zit.: *Bock*, Schutzgut des Datenschutzrechts (Teil I)).

Bock, Kirsten: Schutzgut des Datenschutzrechts – eine Replik auf Veil, Schutzgutmisere – Teil II, 2019 – abrufbar unter https://www.cr-online.de/blog/2019/03/29/schutzgut-des-datenschutzrechts-eine-replik-auf-veil-schutzgutmisere-teil-ii/ (zit.: *Bock*, Schutzgut des Datenschutzrechts (Teil II)).

Böckenförde, Ernst-Wolfgang: Grundrechtstheorie und Grundrechtsinterpretation, NJW 1974, 1529–1535.

Böckenförde, Ernst-Wolfgang: Grundrechte als Grundsatznormen, Der Staat 29 (1990), 1–31.

Böckenförde, Thomas: Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, 925–939.

Boda, Károly et al.: User Tracking on the Web via Cross-Browser Fingerprinting, in: Laud, Peeter (Hrsg.), Information Security Technology for Applications, Springer 2012, S. 31–46.

Boehm, Franziska: Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358–387.

Boehme-Neßler, Volker: Das Rating von Menschen – Onlinebewertungsportale und Grundrechte, K&R 2016, 637–644.

Bohley, Peter: Identität: Wie sie entsteht und warum der Mensch sie braucht, Tectum Wissenschaftsverlag 2016.

Börding, Andreas et al.: Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht – Praxis und Rechtsdogmatik, CR 2017, 134–140.

Borges, Georg: Der neue Personalausweis und der elektronische Identitätsnachweis, NJW 2010, 3334–3339.

Brauer, Manfred: Das Persönlichkeitsrecht der juristischen Person, G. Figel 1962.

Braun, Steffen: Datenschutz im Smart Office – Gestaltung von Energiemanagementsystemen für vernetzte Gebäudeautomation, ZD 2018, 71–76.

Bräutigam, Peter: Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, 635–641.

Brehm, Robert/Brehm-Kaiser, Alexandra: Das Dritte Numers-Clausus-Urteil des BVerfG, NVwZ 2018, 543–545.

Brink, Stefan: Twexit: Warum öffentliche und private Stellen ihre Auftritte in „sozialen Medien" prüfen sollten, DSB 2020, 43–45.

Brinkert, Maike/Stolze, Michael/Heidrich, Joerg: Der Tod und das soziale Netzwerk – Digitaler Nachlass in Theorie und Praxis, ZD 2013, 153–157.

Brisch, Klaus/Müller-ter Jung, Marco: Digitaler Nachlass – Das Schicksal von E-Mail- und De-Mail-Accounts sowie Mediencenter-Inhalten, CR 2013, 446–455.

Britz, Gabriele: Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 411–415.

Britz, Gabriele: Europäisierung des grundrechtlichen Datenschutzes, EuGRZ 2009, 1–11.

Broadnax, Brandon et al.: Sicherheit auf festem Fundament – Starke Sicherheit durch vertrauenswürdige Hardware, DuD 2018, 74–78.

Brost, Lucas/Conrad, Christian: Anonymitätsschutz in der Sozialsphäre, AfP 2017, 286–290.

Brunotte, Nico: Virtuelle Assistenten – Digitale Helfer in der Kundenkommunikation, CR 2017, 583–589.

Buchmann, Erik: Wie kann man Privatheit messen?, DuD 2015, 510–514.

Buchner, Benedikt: Informationelle Selbstbestimmung im Privatrecht, Mohr Siebeck 2006.

Buchner, Benedikt: Die Einwilligung im Datenschutzrecht, DuD 2010, 39–43.

Buchner, Benedikt: Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155–161.

Buchner, Benedikt/Kühling, Jürgen: Die Einwilligung in der Datenschutzgrundverordnung 2018, DuD 2017, 544–548.

Buermeyer, Ulf: Zum Begriff der „laufenden Kommunikation" bei der Quellen-Telekommunikationsüberwachung, StV 2013, 470–476.

Bullinger, Martin: Wettbewerbsgerechtigkeit bei präventiver Wirtschaftsaufsicht, NJW 1978, 2173–2181.

Buttarelli, Giovanni: Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, EDPS 2017 – abrufbar unter https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf (zit.: *Buttarelli*, Opinion 4/2017).

Calliess, Christian/Ruffert, Matthias (Hrsg.): EUV/ AEUV, Kommentar, 5. Aufl., C.H. Beck 2016 (zit.: *Bearbeiter* in: Calliess/Ruffert, EUV/AEUV).

Camenisch, Jan/Leenes, Ronald/Sommer, Dieter (Hrsg.): Digital Privacy, Springer 2011.

Canaris, Claus-Wilhelm: Grundrechte und Privatrecht, De Gruyter 1999.

Cao, Yinzhi/Li, Song/Wijmans, Erik: (Cross-)Browser Fingerprinting via OS and Hardware Level Features, Network & Distributed System Security Symposium 2017, 1 – abrufbar unter http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf.

Caspar, Johannes: Herrschaft der Maschinen oder Herrschaft des Rechts?, PinG 2019, 1–4.

Caspar, Johannes/Schröter, Michael W.: Das Staatsziel Tierschutz in Art. 20a GG, Nomos Verlag 2003.

Classen, Claus: Die Menschenwürde ist – und bleibt – unantastbar, DÖV 2009, 689–698.

Conrad, Isabell/Grützmacher, Malte (Hrsg.): Recht der Daten und Datenbanken im Unternehmen, Otto Schmidt Verlag 2014.

Couzinet, Daniel: Die Prinzipientheorie der Grundrechte – Einführung, Strukturhinweise, Anwendung in der Fallbearbeitung, JuS 2009, 603–608.

Culmsee, Thorsten: Postmortaler Datenschutz und postmortale Datennutzung, DSRITB 2013, 413–429.

Damm, Werner/Kalmar, Ralf: Autonome Systeme – Fähigkeiten und Anforderungen, Informatik Spektrum 2017, 400–408.

Dann, Matthias/Markgraf, Jochen W.: Das neue Gesetz zum Schutz von Geschäftsgeheimnissen, NJW 2019, 1774–1779.

Datenschutzkonferenz des Bundes und der Länder: Das Standard-Datenschutzmodell (Version 1.1), 2019 – abrufbar unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V1.1.pdf.

Datenschutzkonferenz des Bundes und der Länder: Das Standard-Datenschutzmodell (Version 2.0b), 2019 – abrufbar unter https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

Datenschutzkonferenz des Bundes und der Länder: Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, 2021 – abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf.

Degenhart, Christoph: Das allgemeine Persönlichkeitsrecht, Art. 2 I i Vm 1 I GG, JuS 1992, 361–368.

Dengel, Andreas: Künstliche Intelligenz in Anwendungen, KI 2011, 317–319.

Derin, Benjamin/Golla, Sebastian J.: Der Staat als Manipulant und Saboteur der IT-Sicherheit?, NJW 2019, 1111–1116.

Determann, Lothar: Gegen Eigentumsrechte an Daten, ZD 2018, 503–508.

Determann, Lothar: Kein Eigentum an Daten, MMR 2018, 277–278.

Deusch, Florian: Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2–8.

Deusch, Florian/Eggendorfer, Tobias: Das Fernmeldegeheimnis im Spannungsfeld aktueller Kommunikationstechnologien, K&R 2017, 93–99.

Deusch, Florian/Eggendorfer, Tobias: Intrusion Detection und DSGVO, K&R 2018, 753–759.

Deusch, Florian/Eggendorfer, Tobias: Penetrationstest bei Auftragsverarbeitung, K&R 2018, 223–230.

Deutscher Anwaltverein (Hrsg.): Stellungnahme zum Digitalen Nachlass, 2013 – abrufbar unter https://anwaltverein.de/files/anwaltverein.de/downloads/newsroom/stellungnahmen/2013/SN-DAV34-13.pdf.

Deutscher Anwaltverein (Hrsg.): Stellungnahme zum Gesetzentwurf der Bundesregierung zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze, 2020 – abrufbar unter https://anwaltverein.de/de/newsroom/sn-75-20-zum-registermodernisierungsgesetz?scope=modal&target=modal_reader_24&file=files/anwaltverein.de/downloads/newsroom/stellungnahmen/2020/dav-sn-75-2020.pdf.

Dickmann, Roman: Nach dem Datenabfluss: Schadenersatz nach Art. 82 der Datenschutz-Grundverordnung und die Rechte des Betroffenen an seinen personenbezogenen Daten, RuS 2018, 345–355.

Dietlein, Johannes: Die Lehre von den grundrechtlichen Schutzpflichten, Duncker & Humblot Verlag 1992.

Djeffal, Christian: IT-Sicherheit 3.0: Der neue IT-Grundschutz, MMR 2019, 289–294.

Döring, Boro: Der Rufname – jeder kennt ihn, nur das Gesetz nicht, DVBl 2018, 560–567.

Doring, Nicola: Sozialpsychologie im Internet, Hogrefe Verlag 2003.

Dorner, Michael: Big Data und „Dateneigentum", CR 2014, 617–628.

Dörr, Dieter/Natt, Alexander: Suchmaschinen und Meinungsvielfalt, ZUM 2014, 829–847.

Dörr, Oliver/Grote, Rainer/Marauhn, Thilo (Hrsg.): EMRK-GG-Konkordanz-Kommentar, Band I, 2. Aufl., 2013 (zit.: *Bearbeiter* in: Dörr/Grote/Marauhn, EMRK-GG-Kommentar).

Drallé, Lutz: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Lorenz-von-Stein-Institut 2010 (zit.: *Drallé*, GGVIS).

Drechsler, Jörg/Jentzsch, Nicola: Synthetische Daten, Stiftung Neue Verantwortung 2018 – abrufbar unter https://www.stiftung-nv.de/sites/default/files/synthetische_daten.pdf.

Dreier, Horst: Subjektiv-rechtliche und objektiv-rechtliche Grundrechtsgehalte, JURA 1994, 505–513.

Dreier, Horst: Stufungen des vorgeburtlichen Lebensschutzes, ZRP 2002, 377–383.

Dreier, Horst: Bioethik – Politik und Verfassung, Mohr Siebeck 2013 (zit.: *Dreier*, Bioethik).

Dreier, Horst (Hrsg.): Grundgesetz, Kommentar, Band I, Präambel, Artikel 1–19, 3. Aufl., 2013 (zit.: *Bearbeiter* in: Dreier, GG).

Dreier, Thomas/Schulze, Gernot (Hrsg.): Urheberrechtsgesetz, Kommentar, 6. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: Dreier/Schulze, UrhG).

Drexl, Josef et al.: Ausschließlichkeits- und Zugangsrechte an Daten – Positionspapier des Max-Planck-Instituts für Innovation und Wettbewerb vom 16.8.2016 zur aktuellen europäischen Debatte, GRUR Int. 2016, 914–918.

Dreyfuß, Hubert L.: Was Computer nicht können – Die Grenzen künstlicher Intelligenz, athenäums taschenbücher 1989 (zit.: *Dreyfuß*, Grenzen künstlicher Intelligenz).

Dürig, Günter: Der Grundrechtssatz von der Menschenwürde, AöR 81 (1956), 117–157.

Ebers, Martin: Beeinflussung und Manipulation von Kunden durch Behavioral Microtargeting, MMR 2018, 423–428.

Ebersbach, Frank: Elektronische Gesundheitskarte – ein Dauer(streit)thema, DSB 2013, 272–274.

Eckert, Claudia: IT-Sicherheit, 10. Aufl., De Gruyter 2018.

Ehmann, Eugen/Selmayr, Martin (Hrsg.): Datenschutz-Grundverordnung, Kommentar, 2. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: Ehmann/Selmayr, DSGVO).

Eichenhofer, Johannes: Privatheit im Internet als Vertrauensschutz, Der Staat 55 (2016), 41–67.

Eidenmüller, Horst: Der homo oeconomicus und das Schuldrecht: Herausforderungen durch Behavioral Law and Economics, JZ 2005, 216–224.

Eifert, Martin: Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, 521–523.

Eikenberg, Ronald: Wie Sie Ihre digitale Identität schützen, c't 5 2019, 32 f.

Enders, Christoph: Die Menschenwürde in der Verfassungsordnung, Mohr Siebeck 1997.

Engeler, Malte: Der staatliche Twitter-Auftritt – Rechtliche Hürden und mögliche Lösungen, MMR 2017, 651–656.

Engeler, Malte: Das überschätzte Kopplungsverbot, ZD 2018, 55–62.

Ensthaler, Jürgen: Industrie 4.0 und die Berechtigung an Daten, NJW 2016, 3473–3478.

Epping, Volker/Hillgruber, Christian (Hrsg.): BeckOK Grundgesetz, 49. Aufl., C.H. Beck, Stand: 15.11.2021 (zit.: *Bearbeiter* in: Epping/Hillgruber, BeckOK GG).

Erichsen, Hans-Uwe: Grundrechtliche Schutzpflichten in der Rechtsprechung des Bundesverfassungsgerichts, JURA 1997, 85–89.

Ernst, Christian: Eine allgemeine Informationsordnung als Regelung der Zuordnung von Informationen zu Rechtssubjekten, in: Hill, Herrmann/Schliesky, Utz (Hrsg.), Auf dem Weg zum Digitalen Staat – auch ein besserer Staat?, Nomos Verlag 2015, S. 33–58 (zit.: *Ernst*, Weg zum Digitalen Staat).

Ernst, Christian: Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, 1026–1036.

Ernst, Stefan: Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110–114.

Eschenbach, Jürgen: Der verfassungsrechtliche Schutz des Eigentums, Duncker & Humblot Verlag 1996.

Esken, Saskia: Dateneigentum und Datenhandel, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Erich Schmidt Verlag 2019, S. 73–84.

Etteldorf, Christina: Medien als Kritische Infrastrukturen? AfP 2018, 114–119.

Europäischer Datenschutzbeauftragter: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of COVID-19 outbreak, 2021.

Faller, Rico: Staatsziel „Tierschutz" – Vom parlamentarischen Gesetzgebungsstaat zum verfassungsgerichtlichen Jurisdiktionsstaat?, Duncker & Humblot Verlag 2005.

Faust, Florian: Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, NJW-Beilage 2016, 29–32.

Faust, Florian: Ausschließlichkeitsrecht an Daten?, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Erich Schmidt Verlag 2019, S. 85–100.

Faustmann, Jörg: Der deliktische Datenschutz, VuR 2006, 260–263.

Federrath, Hannes/Gerber, Christoph/Herrmann, Dominik: Verhaltensbasierte Verkettung von Internetsitzungen, DuD 2011, 791–796.

Feldmann, Thomas: Zum Referentenentwurf eines NetzDG: Eine kritische Betrachtung, K&R 2017, 292–297.

Fezer, Karl-Heinz: Dateneigentum – Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten, MMR 2017, 3–5.

Fezer, Karl-Heinz: Dateneigentum der Bürger, ZD 2017, 99–105.

Fezer, Karl-Heinz: Repräsentatives Dateneigentum – Ein zivilgesellschaftliches Bürgerrecht, Konrad-Adenauer-Stiftung e.V. 2018 – abrufbar unter https://www.jura.uni-konstanz.de/typo3temp/secure_downloads/92986/0/7bf7a16e1374239b9b71e1f03dd7a2829b7879ed/18_04_23_Studie_Fezer_Repraese

ntatives_Dateneigentum_kas_52161-544-1-30.pdf (zit.: *Fezer*, Repräsentatives Dateneigentum).

Fezer, Karl-Heinz: Digitales Dateneigentum – ein grundrechtsdogmatisches Bürgerrecht in der Zivilgesellschaft, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Erich Schmidt Verlag 2019, S. 101–160.

Fezer, Karl-Heinz/Büscher, Wolfgang/Obergfell, Eva Inés (Hrsg.): Lauterkeitsrecht – Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), 3. Aufl., C.H. Beck 2016 (zit.: *Bearbeiter* in: Fezer/Büscher/Obergfell, UWG).

Fischer, Annette: Die Entwicklung des postmortalen Persönlichkeitsschutzes, Peter Lang Verlag 2004.

Fischer, Thomas: Strafgesetzbuch mit Nebengesetzen, Kommentar, 64. Aufl., 2017 (zit.: *Bearbeiter* in: Fischer, StGB-Kommentar).

Fischinger, Philipp S.: Der Grundrechtsverzicht, JuS 2007, 808–813.

Forster, Otto: Analysis I, Grundkurs Mathematik, 12. Aufl., 2016 (zit.: *Forster*, Analysis I).

Fox, Dirk: Webtracking, DuD 2010, 787.

Fox, Dirk: Digitale Souveränität, DuD 2018, 271.

Franck, Johannes/Müller-Peltzer, Philipp: Wettbewerbs- und datenschutzrechtliche Grenzen des Location Based Marketing mittels Geofencing, K&R 2016, 718–724.

Freimuth, Christoph: Die Gewährleistung der IT-Sicherheit Kritischer Infrastrukturen, Duncker & Humblot Verlag 2018 (zit.: *Freimuth*, Gewährleistung der IT-Sicherheit).

Friauf, Karl Heinrich/Wendt, Rudolf: Eigentum am Unternehmen, Otto A. Friedrich Kuratorium 1977.

Garcia, David: Leaking privacy and shadow profiles in online social networks, Science Advances 2017, e17011172.

Geddert-Steinacher, Tatjana: Menschenwürde als Verfassungsbegriff – Aspekte der Rechtsprechung des Bundesverfassungsgerichts zu Art. 1 Abs. 1 Grundgesetz, 1990 (zit.: *Geddert-Steinacher*, Menschenwürde als Verfassungsbegriff).

Gehrmann, Mareike/Voigt, Paul: IT-Sicherheit – Kein Thema nur für Betreiber Kritischer Infrastrukturen, CR 2017, 93–99.

Geiger, Andreas: Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung, NVwZ 1989, 35–38.

Geminn, Christian: Menschenwürde und menschenähnliche Maschinen und Systeme, DÖV 2020, 172–181.

Geminn, Christian/Laubach, Anne/Fujiwara, Shizuo: Schutz anonymisierter Daten im japanischen Datenschutzrecht, ZD 2018, 413–420.

Geminn, Christian L.: Daten für alle? – Zum Diskussionspapier der SPD, ZD-aktuell 2019, Nr. 06492.

Gercke, Marco: Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245–253.

Gerling, Rainer W.: Verschlüsselungsverfahren, DuD 1997, 197–202.

Gersdorf, Hubertus: Staatliche Kommunikationstätigkeit, AfP 2016, 293–301.

Gersdorf, Hubertus: Hate Speech in sozialen Netzwerken, MMR 2017, 439–447.

Gersdorf, Hubertus/Paal, Boris (Hrsg.): Beck'scher Online-Kommentar zum Informations- und Medienrecht, 34. Aufl., C.H. Beck, Stand: 01.05.2021 (zit.: *Bearbeiter* in: Gersdorf/Paal, BeckOK InfoMedienR).

Gesellschaft für Informatik (Hrsg.): Stellungnahme zum Registermodernisierungsgesetz, 2020 – abrufbar unter https://gi.de/fileadmin/GI/Allgemein/PDF/2020-09-04_GI-Stellungnahme_zum_Registermodernisierungsgesetz.pdf.

Gierke, Otto: Das Wesen der menschlichen Verbände, Mohr Siebeck 1902.

Gierschmann, Sibylle: Gestaltungsmöglichkeiten durch systematisches und risikobasiertes Vorgehen – Was ist schon anonym? ZD 2021, 482–486.

Giesen, Thomas: Das Grundrecht auf Datenverarbeitung, JZ 2007, 918–927.

Gola, Peter (Hrsg.): Datenschutz-Grundverordnung – VO (EU) 2016/679, 2. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: Gola, DS-GVO).

Gola, Peter: Das Geschäftsgeheimnisgesetz und die Datenschutz-Grundverordnung, DuD 2019, 569–574.

Golla, Sebastian J.: In Würde vor Ampel und Algorithmus – Verfassungsrecht im technologischen Wandel, DÖV 2019, 673–681.

Golla, Sebastian J./Mühlen, Nicloas von zur: Der Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei, JZ 2014, 668–674.

Golland, Alexander: Datenschutzrechtliche Fragen personalisierter Preise, CR 2020, 186–194.

Golland, Alexander/Kriegesmann, Torben: Der Schutz virtueller Identitäten durch die DSGVO, PinG 2017, 45–50.

Gomille, Christian: Information als Nachlassgegenstand, ZUM 2018, 660–667.

Gonscherowski, Susan/Hansen, Marit/Rost, Martin: Resilienz – eine neue Anforderung aus der Datenschutz-Grundverordnung, DuD 2018, 442–446.

González-Cabañas, José et al.: Unique on Facebook: Formulation and Evidence of (Nano)targeting Individual Users with non-PII Data, 2021 – abrufbar unter https://arxiv.org/abs/2110.06636.

Gostomzyk, Tobias: Äußerungsrechtliche Grenzen des Unternehmenspersönlichkeitsrechts – Die Gen-Milch-Entscheidung des BGH, NJW 2008, 2082–2084.

Götting, Horst-Peter/Schertz, Christian/Seitz, Walter (Hrsg.): Handbuch des Persönlichkeitsrechts, C.H. Beck 2008.

Grafenstein, Maximilian von: The Principle of Purpose Limitation in Data Protection Laws, Nomos Verlag 2018.

Gröpl, Christoph/Windthorst, Kay/Coelln, Christian von (Hrsg.): Studienkommentar Grundgesetz, 2013 (zit.: *Bearbeiter* in: Gröpl/Windthorst/von Coelln, StuKo GG).

Gropp, Stefanie: Schutzkonzepte des werdenden Lebens, Peter Lang Verlag 2005.

Grosskopf, Lambert: Rechte an privat erhobenen Geo- und Telemetriedaten, IPRB 2011, 259–261.

Grützmacher, Malte: Dateneigentum – ein Flickenteppich, CR 2016, 485–495.

Gsell, Beate et al. (Hrsg.): beck-online.GROSSKOMMENTAR BGB, C.H. Beck 2019 (zit.: *Bearbeiter* in: Gsell et al., BeckOGK BGB).

Gurlit, Elke: Verfassungsrechtliche Rahmenbedingungen des Datenschutzes, NJW 2010, 1035–1041.

Gusy, Christoph: Grundpflichten und Grundgesetz, JZ 1982, 657–663.

Häberle, Peter: Grundrechte im Leistungsstaat, VVDStRL 30 (1972), 43–131.

Hackenjos, Timon/Mechler, Jeremias/Rill, Jochen: IT-Sicherheit – ein rechtsfreier Raum? DuD 2018, 286–290.

Hagemeier, Heike: Kryptografie – heute und zukünftig, DuD 2019, 631–635.

Hagen, Othmar: Das Unternehmen als nach Art. 14 Abs. 1 GG geschütztes eigenständiges Rechtssubjekt, GewArch 2005, 402–408.

Hain, Karl-Eberhard: Der Gesetzgeber in der Klemme zwischen Übermaß- und Untermaßverbot?, DVBl 1993, 982–984.

Hammer, Volker/Knopp, Michael: Datenschutzinstrumente Anonymisierung, Pseudonyme und Verschlüsselung, DuD 2015, 503–509.

Hanloser, Stefan: Geräte-Identifier im Spannungsfeld von DS-GVO, TMG und ePrivacy-VO, ZD 2018, 213–218.

Hansen, Marit: Informationssicherheit: Aufgabe für die Datenschutzaufsicht? DuD 2021, 234–238.

Hansen, Marit/Meints, Martin: Digitale Identitäten – Überblick und aktuelle Trends, DuD 2006, 543–547.

Hansen, Marit/Walczak, Benjamin: Pseudonymisierung á la DS-GVO und verwandte Methoden, RDV 2019, 53–57.

Harks, Thomas: Der Schutz der Menschenwürde bei der Entnahme fötalen Gewebes, NJW 2002, 716–722.

Härting, Niko: Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065–2071.

Härting, Niko: „Dateneigentum" – Schutz durch Immaterialgüterrecht?, CR 2016, 646–649.

Hartmann, Bernd J.: Digitale Partizipation, MMR 2017, 383–386.

Hau, Wolfgang/Poseck, Roman (Hrsg.): BeckOK BGB, 60. Aufl., C.H. Beck, Stand: 01.11.2021.

Haustein, Berthold: Möglichkeiten und Grenzen von Dateneigentum, Nomos Verlag 2021.

Haverkate, Görg: Verfassungslehre: Verfassung als Gegenseitigkeitsordnung, C.H. Beck 1992 (zit.: *Haverkate*, Verfassungslehre).

Heckmann, Dirk: Persönlichkeitsschutz im Internet – Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderungen für Ehrschutz und Profilschutz, NJW 2012, 2631–2635.

Heckmann, Dirk/Wimmers, Jörg: Stellungnahme des DGRI zum Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG), CR 2017, 310–316.

Heinemann, Marcus: Grundrechtlicher Schutz informationstechnischer Systeme, Duncker & Humblot Verlag 2015.

Heintschel-Heinegg, Bernd von (Hrsg.): Beck'scher Online-Kommentar StGB, 51. Aufl., C.H. Beck, Stand: 01.11.2021 (zit.: *Bearbeiter* in: von Heintschel-Heinegg, BeckOK StGB).

Heißl, Gregor: Können juristische Personen in ihrem Grundrecht auf Datenschutz verletzt sein? — Persönlicher Schutzbereich von Art. 8 GRC, EuR 2017, 561–570.

Hellmann, Roland: Rechnerarchitektur, 2. Aufl., De Gruyter 2016.

Hellmann, Roland: IT-Sicherheit – Eine Einführung, De Gruyter 2018 (zit.: *Hellmann*, IT-Sicherheit).

Herberger, Maximilian: „Künstliche Intelligenz" und Recht – Ein Orientierungsversuch, NJW 2018, 2825–2829.

Herbst, Dieter Georg: Corporate Identity, 5. Aufl., 2012.

Herbst, Tobias: Was sind personenbezogene Daten?, NVwZ 2016, 902–906.

Herdegen, Matthias: Die Menschenwürde im Fluß des bioethischen Diskurses, JZ 2001, 773–779.

Hermes, Georg: Das Grundrecht auf Schutz von Leben und Gesundheit, C.F. Müller 1987.

Herold, Helmut/Lurz, Bruno/Wohlrab, Jürgen: Grundlagen der Informatik, 2. Aufl., Pearson 2012.

Herrmann, Christoph: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Peter Lang Verlag 2010 (zit.: *Herrmann*, GGVIS).

Herrmann, Dominik/Federrath, Hannes: Unbemerktes Tracking im Internet: Unsere unerwünschte Identität, in: Hornung, Gerrit/Engemann, Christoph (Hrsg.), Der digitale Bürger und seine Identität, Nomos Verlag 2016, S. 131–152.

Herrmann, Günter: Zum verfassungsrechtlichen Schutz der Persönlichkeit in ihrer Identität, Selbstbestimmung und Ehre, ZUM 1990, 541–544.

Herzog, Stephanie: Der digitale Nachlass — ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745–3751.

Heun, Sven-Erik/Assion, Simon: Internet(recht) der Dinge – Zum Aufeinandertreffen von Sachen- und Informationsrecht, CR 2015, 812–818.

Heymann, Thomas: Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen, CR 2016, 650–657.

Hilgendorf, Eric: Grundfälle zum Computerstrafrecht, JuS 1996, 509–513.

Hoeren, Thomas: Der Tod und das Internet – Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers, NJW 2005, 2113–2117.

Hoeren, Thomas: Was ist das „Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme“?, MMR 2008, 365–366.

Hoeren, Thomas: Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486–491.

Hoeren, Thomas: Big Data und Recht, C.H. Beck 2014.

Hoeren, Thomas: Datenbesitz statt Dateneigentum – Erste Ansätze zur Neuausrichtung der Diskussion um die Zuordnung von Daten, MMR 2019, 5–8.

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.): Handbuch Multimedia-Recht, , Stand: Januar 2017 (44. EL) (zit.: *Bearbeiter* in: Hoeren/Sieber/Holznagel, Handbuch MultimediaR).

Hoffmann, Christian et al.: Die digitale Dimension der Grundrechte, Nomos Verlag 2015.

Hoffmann, Jan Felix: „Dateneigentum“ und Insolvenz, JZ 2019, 960–968.

Hoffmann-Riem, Wolfgang: Grundrechtsanwendung unter Rationalitätsanspruch, Der Staat 43 (2004), 203–233.

Hoffmann-Riem, Wolfgang: Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009–1022.

Hoffmann-Riem, Wolfgang: Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, AöR 134 (2009), 513–541.

Hofmann, Franz: Der maßgeschneiderte Preis, WRP 2016, 1074–1081.

Hofmann, Franz/Freiling, Felix: Personalisierte Preise und das Datenschutzrecht, ZD 2020, 331–335.

Hofmann, Hasso: Die versprochene Menschenwürde, AöR 118 (1993), 353–377.

Hofmann, Johanna M./Johannes, Paul C.: DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs, ZD 2017, 221–226.

Hofmann, Manfred: Die Online-Durchsuchung – staatliches „Hacken“ oder zulässige Ermittlungsmaßnahme?, NStZ 2005, 121–125.

Hölzel, Julian: Anonymisierungstechniken und das Datenschutzrecht, DuD 2018, 502–509.

Holzinger, Andreas: Explainable AI, Informatik Spektrum 2018, 138–143.

Holznagel, Bernd/Beine, Heinrich: Rechtsrahmen staatlicher Breitbandförderung – Herausforderungen für Bund, Länder und Kommunen im „Regelungsgestrüpp“, MMR 2015, 567–571.

Holzwarth, Andreas: Das Recht auf ungestörte Familienplanung als Konkretisierung des zivilrechtlichen allgemeinen Persönlichkeitsrechts, 1997.

Hornung, Gerrit: Die digitale Identität, Nomos Verlag 2005 – abrufbar unter https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5-Institute/IWR/Hornung/hornung_die-digitale-identitaet_2005.pdf.

Hornung, Gerrit: Die Festplatte als Wohnung?, JZ 2007, 828–831.

Hornung, Gerrit: Der verfassungsrechtliche Schutz der „Vertraulichkeit und Integrität informationstechnischer Systeme", CR 2008, 299–306.

Hornung, Gerrit/Engemann, Christoph: Einleitung, in: Hornung, Gerrit/Engemann, Christoph (Hrsg.), Der digitale Bürger und seine Identität, Nomos Verlag 2016, S. 11–22.

Hornung, Gerrit/Goeble, Thilo: „Data Ownership" im vernetzten Automobil, CR 2015, 265–273.

Hornung, Gerrit/Schallbruch, Martin (Hrsg.): IT-Sicherheitsrecht – Praxishandbuch, Nomos Verlag 2021 (zit.: *Bearbeiter* in: Hornung/Schallbruch, IT-Sicherheitsrecht).

Hornung, Gerrit/Wagner, Bernd: Anonymisierung als datenschutzrelevante Verarbeitung?, ZD 2020, 223–228.

Hossenfelder, Martin: Pflichten von Internetnutzern zur Abwehr von Malware und Phishing in Sonderverbindungen, Nomos Verlag 2013.

Hubmann, Heinrich: Das Persönlichkeitsrecht, Böhlau Verlag 1967 (zit.: *Hubmann*, Persönlichkeitsrecht).

Hufen, Friedhelm: Erosion der Menschenwürde?, JZ 2004, 313–318.

Hufen, Friedhelm: Staatsrecht II, Grundrechte, 6. Aufl., 2017 (zit.: *Hufen*, Staatsrecht II).

Hühnlein, Detlef: Identitätsmanagement – Eine visualisierte Begriffsbestimmung, DuD 2008, 161–163.

Humer, Stephan: Digitale Identitäten, CSW-Verlag 2008.

Humer, Stephan: Hier bin ich Mensch, hier darf ich's sein: Identitätsarbeit in digitalen Systemen, in: Ternes, Bernd (Hrsg.), Menschen formen Menschenformen: zum technologischen Umbau der conditio humana, 2009, S. 149–160 (zit.: *Humer*, Identitätsarbeit in digitalen Systemen).

Ibara, Imanol Arrieta et al.: Should We Treat Data as Labor, 2018 – abrufbar unter https://www.aeaweb.org/conference/2018/preliminary/paper/2Y7N88na.

Ipsen, Jörn: Gesetzliche Einwirkungen auf grundrechtlich geschützte Rechtsgüter, JZ 1997, 473–480.

Ipsen, Jörn: Verfassungsrecht und Biotechnologie, DVBl 2004, 1381–1386.

Isensee, Josef: Die verdrängten Grundpflichten des Bürgers, DÖV 1982, 609–618.

Isensee, Josef: Das Grundrecht auf Sicherheit, De Gruyter 1983.

Isensee, Josef/Kirchhof, Paul (Hrsg.): Handbuch des Staatsrechts, Band VII, 3. Aufl., C.F. Müller 2009 (zit.: *Bearbeiter* in: Isensee/Kirchhof, HStR VII).

Isensee, Josef/Kirchhof, Paul (Hrsg.): Handbuch des Staatsrechts, Band VIII, Grundrechte: Wirtschaft, Verfahren, Gleichheit, 3. Aufl., C.F. Müller 2010 (zit.: *Bearbeiter* in: Isensee/Kirchhof, HStR VIII).

Isensee, Josef/Kirchhof, Paul (Hrsg.): Handbuch des Staatsrechts, Band IX, Allgemeine Grundrechtslehren, 3. Aufl., C.F. Müller 2011 (zit.: *Bearbeiter* in: Isensee/Kirchhof, HStR IX).

Jäncke, Lutz: Lehrbuch Kognitive Neurowissenschaften, hogrefe 2017.

Jandt, Silke: Datenschutz durch Technik in der DS-GVO, DuD 2017, 562–566.

Jandt, Silke: Online-Tracking – viele Fragen, viele Antworten, viele Meinungen, PinG 2019, 145–148.

Jandt, Silke/Steidle, Roland (Hrsg.): Datenschutz im Internet, Nomos Verlag 2018.

Jarass, Hans D.: Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, 857–862.

Jarass, Hans D. (Hrsg.): Charta der Grundrechte der EU, 3. Aufl., C.H. Beck 2016 (zit.: *Bearbeiter* in: Jarass, GrC-Kommentar).

Jarass, Hans D./Pieroth, Bodo (Hrsg.): Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 16. Aufl., C.H. Beck 2020 (zit.: *Bearbeiter* in: Jarass/Pieroth, GG-Kommentar).

Jeand'Heur, Bernd: Grundrechte im Spannungsverhältnis zwischen subjektiven Freiheitsgarantien und objektiven Grundsatznormen, JZ 1995, 161–167.

Jellinek, Georg; Kersten, Jens (Hrsg.): System der subjektiv öffentlichen Rechte, 2. Aufl., Mohr Siebeck 1905.

Jülicher, Tim/Röttgen, Charlotte/Schönfeld, Max von: Das Recht auf Datenübertragbarkeit – Ein datenschutzrechtliches Novum, ZD 2016, 358–362.

Käde, Lisa/Maltzan, Stephanie von: Die Erklärbarkeit von Künstlicher Intelligenz, CR 2020, 66–72.

Kahl, Wolfgang/Waldhoff, Christian/Walter, Christian (Hrsg.): Bonner Kommentar zum Grundgesetz, 1991, Stand: 186. EL (September 2017) (zit.: *Bearbeiter* in: Kahl/Waldhoff/Walter, BonnK GG).

Kalscheuer, Fiete/Hornung, Christian: Das Netzwerkdurchsetzungsgesetz – Ein verfassungswidriger Schnellschuss, NVwZ 2017, 1721–1725.

Kalscheuer, Fiete/Jacobsen, Annika: Das digitale Hausrecht von Hoheitsträgern, NJW 2018, 2358–2362.

Kapsner, Andreas/Sandfuchs, Barbara: Nudging as a Threat to Privacy, Review of Philosophy and Psychology 2015, 455–468.

Karaboga, Murat et al.: White Paper Selbstdatenschutz, forum privatheit 2014 – abrufbar unter https://www.researchgate.net/publication/283504593_White_Paper_Selbstdatenschutz.

Karg, Moritz: Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520–526.

Karg, Moritz/Thomsen, Sven: Tracking Analyse durch Facebook, DuD 2012, 729–736.

Karl, Winfried/Hummert, Christian: Digitale Souveränität: Die Rolle der ZITiS in der deutschen Cybersicherheitsarchitektur, DuD 2021, 223–228.

Kerber, Wolfgang: A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int. 2016, 989–998.

Kersten, Jens: Menschen und Maschinen – Rechtliche Konturen instrumenteller, symbiotischer und autonomer Konstellationen, JZ 2015, 1–8.

Kersten, Jens: Anonymität in der liberalen Demokratie, JuS 2017, 193–203.

Kielmansegg, Sebastian Graf: Die Grundrechtsprüfung, JuS 2008, 23–29.

Kiessling, Waldemar F./Spannagl, Peter: Corporate Identity, 1996.

Kim, Daria: No One's Ownership as the Status Quo and a Possible Way Forward: A Note on the Public Consultation on Building a European Data Economy, GRUR Int. 2017, 697–705.

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich (Hrsg.): Strafgesetzbuch, 5. Aufl., Nomos Verlag 2017 (zit.: *Bearbeiter* in: Kindhäuser/Neumann/Paeffgen, StGB).

Kingreen, Thorsten/Poscher, Ralf: Staatsrecht II, Grundrechte, 33. Aufl., 2017 (zit.: *Kingreen*/*Poscher*, Staatsrecht II).

Kipker, Dennis-Kenji (Hrsg.): Cybersecurity, C.H. Beck 2020.

Kipker, Dennis-Kenji: Datensicherheit in der DSGVO, <kes> 2021, 61–67.

Kipker, Dennis-Kenji/Scholz, Dario E.: Das IT-Sicherheitsgesetz 2.0 – Eine kritische Analyse, DuD 2021, 40–45.

Kirchgässner, Gebhard: Homo Oeconomicus, 4. Aufl., Mohr Siebeck 2013.

Klas, Benedikt/Möhrke-Sobolewski, Christine: Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473–3478.

Klein, Eckart: Grundrechtliche Schutzpflicht des Staates, NJW 1989, 1633–1640.

Kleiner, Cornelius: Die elektronische Person, Nomos Verlag 2021.

Klippel, Diethelm: Der zivilrechtliche Persönlichkeitsschutz von Verbänden, JZ 1988, 625–635.

Kloepfer, Michael: Humangenetik als Verfassungsfrage, JZ 2002, 417–428.

Kloepfer, Michael: Verfassungsrecht, Band II, 2010 (zit.: *Kloepfer*, VerfR II).

Kloepfer, Michael/Greve, Holger: Das Informationsfreiheitsgesetz und der Schutz von Betriebs- und Geschäftsgeheimnissen, NVwZ 2011, 577–584.

Kluge, Vanessa/Müller, Anne-Kathrin: Autonome Systeme – Überlegungen zur Forderung nach einer „Roboterhaftung“, InTeR 2017, 24–31.

Knellwolf, Esther: Postmortaler Persönlichkeitsschutz – neuere Tendenzen der Rechtsprechung, ZUM 1997, 783–789.

Knoll, Alois/Christaller, Thomas: Robotik, S. Fischer Verlag 2003.

Knopp, Michael: Pseudonym – Grauzone zwischen Anonymisierung und Personenbezug, DuD 2015, 527–530.

Kochheim, Dieter: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2. Aufl., C.H. Beck 2018 (zit.: *Kochheim*, Cybercrime in IuK).

Körber, Torsten: „Ist Wissen Marktmacht?“ – Überlegungen zum Verhältnis von Datenschutz, „Datenmacht“ und Kartellrecht (Teil 1), NZKart 2016, 303–310.

Koreng, Ansgar: Das „Unternehmenspersönlichkeitsrecht“ als Element des gewerblichen Reputationsschutzes, GRUR 2010, 1065–1070.

Korneeva, Ekaterina: Das Persönlichkeitsrecht des Unternehmens, Oldenburger Verlag für Wirtschaft, Informatik und Recht 2014.

Kraaibeek, Peter: Sicherung kritischer Infrastrukturen im Gesundheitswesen, in: Holznagel, Bernd/Hanßmann, Anika/Sonntag, Matthias (Hrsg.), IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen, LIT 2011, S. 79–88.

Kraft, Alfons: Gedanken zum allgemeinen Persönlichkeitsrecht juristischer Personen, in: Forkel, Hans/Kraft, Alfons (Hrsg.), Beiträge zum Schutz der Persönlichkeit und ihrer schöpferischen Leistung – Festschrift für Heinrich Hubmann zum 70. Geburtstag, Alfred Metzner Verlag 1985, S. 201–220 (zit.: *Kraft*, FS Hubmann).

Krasemann, Henry: Identitäten in Online-Spielen, DuD 2008, 194–196.

Kraul, Torsten: „Recht an Daten“: Aktuelle Gesetzeslage und vertragliche Ausgestaltung, GRUR-Prax 2019, 478–480.

Krings, Günter: Grund und Grenzen grundrechtlicher Schutzansprüche, Duncker & Humblot Verlag 2003.

Krohm, Niclas: Abschied vom Schriftformgebot der Einwilligung, ZD 2016, 368–373.

Krohm, Niclas/Müller-Peltzer, Philipp: Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung – Das Aus für das Modell „Service gegen Daten“?, ZD 2017, 551–556.

Krug, Paul-Eberhard: Ehre und Beleidigungsfähigkeit von Verbänden, Duncker & Humblot Verlag 1965.

Krügel, Tina: Der Einsatz von Angriffserkennungssystemen im Unternehmen, MMR 2017, 795–799.

Krügel, Tina: Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455–460.

Krüger, Philipp-L.: Datensouveränität und Digitalisierung, ZRP 2016, 190–192.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung, 2. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: Kühling/Buchner, DSGVO).

Kühling, Jürgen/Buchner, Benedikt (Hrsg.): Datenschutz-Grundverordnung, 3. Aufl., C.H. Beck 2020 (zit.: *Bearbeiter* in: Kühling/Buchner, DSGVO).

Kühling, Jürgen/Klar, Manuel/Sackmann, Florian: Datenschutzrecht, 5. Aufl., C.F. Müller 2021.

Kühling, Jürgen/Sackmann, Florian: Rechte an Daten – Regulierungsbedarf aus Sicht des Verbraucherschutzes?, vzbv 2018 – abrufbar unter https://www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_kuehling-sackmann-rechte-an-daten.pdf (zit.: *Kühling/Sackmann*, vzbv-Gutachten).

Kühling, Jürgen/Sackmann, Florian: Irrweg „Dateneigentum“, ZD 2020, 24–30.

Kuhn, Thomas: Digitaler Zwilling, Informatik Spektrum 2017, 440–444.

Kühnl, Christina: Persönlichkeitsschutz 2.0, De Gruyter 2016.

Kunig, Philip: Der Grundsatz informationeller Selbstbestimmung, Jura 1993, 595–604.

Kutscha, Martin: Verdeckte „Online-Durchsuchung“ und Unverletzlichkeit der Wohnung, NJW 2007, 1169–1172.

Kutscha, Martin: Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042.

Kutscher, Antonia: Der digitale Nachlass, V&R unipress 2015.

Lackner, Karl/Kühl, Kristian: Strafgesetzbuch, Kommentar, 29. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: Lackner/Kühl, StGB-Kommentar).

Lambach, Daniel/Oppermann, Kai: Narratives of digital sovereignty in German political discourse, Governance 2022, 1–17.

Lange, Knut Werner/Holtwiesche, Marian: Digitaler Nachlass – eine Herausforderung für Wissenschaft und Praxis (Teil 1), ZErb 2016, 125–131.

Lange, Knut Werner/Holtwiesche, Marian: Digitaler Nachlass – eine Herausforderung für Wissenschaft und Praxis (Teil 2), ZErb 2016, 157–162.

Langhanke, Carmen: Daten als Leistung, Mohr Siebeck 2018.

Laufhütte, Heinrich Wilhelm/Saan, Ruth Rissing-van/Tiedemann, Klaus (Hrsg.): Leipziger Kommentar StGB, Band 10, 12. Aufl., De Gruyter 2008.

Leeb, Christina-Maria: Bekannt verstorben – Rechtsfragen des Umgangs mit Social Media Daten Verstorbener, K&R 2014, 693–699.

Lehmann, Michael: Abgrenzung der Schutzgüter im Zusammenhang mit Daten, in: Conrad, Isabell/Grützmacher, Malte (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, Otto Schmidt Verlag 2014, S. 133–142 (zit.: *Lehmann*, FS Schneider).

Leisner, Walter: Grundrechte und Privatrecht, C.H. Beck 1960.

Leisner, Walter; Isensee, Josef (Hrsg.): Eigentum – Schriften zu Eigentumsrecht und Wirtschaftsverfassung 1970-1996, Duncker & Humblot Verlag 1996 (zit.: *Leisner*, Eigentum).

Lenaerts, Koen: Die EU-Grundrechtecharta: Anwendbarkeit und Auslegung, EuR 2012, 3–17.

Leßmann, Herbert: Persönlichkeitsschutz juristischer Personen, AcP 170 (1970), 266–294.

Lewinski, Kai von: Wert von personenbezogenen Daten, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Erich Schmidt Verlag 2019, S. 209–220.

Liesching, Marc: Was sind „rechtswidrige Inhalte“ im Sinne des Netzwerkdurchsetzungsgesetzes?, ZUM 2017, 809–815.

Lilienfeld-Toal, Roland von: Das allgemeine Persönlichkeitsrecht juristischer Personen des Zivilrechts, Peter Lang Verlag 2003.

Linke, Tobias: Die Menschenwürde im Überblick: Konstitutionsprinzip, Grundrecht, Schutzpflicht, JuS 2016, 888–893.

Lotz, Benjamin/Wendler, Julia: Datensicherheit als datenschutzrechtliche Anforderung: Zur Frage der Abdingbarkeit des § 9 BDSG, CR 2016, 31–37.

Luch, Anika D.: Das neue „IT-Grundrecht“ – Grundbedingung einer „Online-Handlungsfreiheit“, MMR 2011, 75–79.

Luch, Anika Dorthe: Das Medienpersönlichkeitsrecht, Schranke der vierten „Gewalt“, Peter Lang Verlag 2008 (zit.: *Luch*, Medienpersönlichkeitsrecht).

Ludwigs, Markus/Friedmann, Carolin: Die Grundrechtsberechtigung juristischer Personen nach Art. 19 III GG, JA 2018, 807–815.

Ludyga, Hannes: „Digitales Update“ für das Erbrecht im BGB?, ZEV 2018, 1–6.

Luther, Christoph: Die juristische Analogie, JURA 2013, 449–453.

Lutterotti, Markus von: Schutz des menschlichen Lebens an seinem Beginn und seinem Ende im Bereich von Naturwissenschaft und Medizin, in: Essener Gespräche zum Thema Staat und Kirche, Band 22, 1988, S. 12 ff (zit.: *von Lutterotti*, Schutz des menschlichen Lebens).

Mainzer, Klaus: Leben als Maschine? – Von der Systembiologie zur Robotik und Künstlichen Intelligenz, mentis Verlag 2010 (zit.: *Mainzer*, Leben als Maschine).

Maltzan, Stephanie von: The concept of identifiability in ML Models, IoTBDS 2022, 215–222.

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian (Hrsg.): Kommentar zum Grundgesetz, Band I, Präambel, Artikel 1 bis 19, 7. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band I).

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian (Hrsg.): Kommentar zum Grundgesetz, Band III, 7. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: von Mangoldt/Klein/Starck, GG-Kommentar, Band III).

Manssen, Gerrit: Staatsrecht II – Grundrechte, 14. Aufl., C.H. Beck 2017.

Markendorf, Merih: Recht an Daten in der deutschen Rechtsordnung – Blockchain als Lösungsansatz für eine rechtliche Zuordnung?, ZD 2018, 409–413.

Marsch, Nikolaus: Das europäische Datenschutzgrundrecht, Mohr Siebeck 2018.

Martens, Wolfgang: Grundrechte im Leistungsstaat, VVDStRL 30 (1972), 7–34.

Martini, Mario: Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145–1155.

Martini, Mario/Kienle, Thomas: Facebook, die Lebenden und die Toten, JZ 2019, 235–241.

Martini, Mario et al.: Datenhoheit – Annäherung an einen offenen Leitbegriff, MMR-Beil 2021, 3–22.

Martini, Mario/Wagner, David/Wenzel, Michael: Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Universität für Verwaltungswissenschaften Speyer 2017 – abrufbar unter https://www.normenkontrollrat.bund.de/resource/blob/72494/476034/eebab686008cfec0a7919ca03e51abe3/2017-10-06-download-nkr-gutachten-2017-anlage-untersuchung-datenschutz-data.pdf?download=1.

Martini, Mario/Weinzierl, Quirin: Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251–1259.

Masood, Rahat et al.: Touch and You're Trapp(ck)ed: Quantifying the Uniqueness of Touch Gestures for Tracking, Proceedings on Privacy Enhancing Technologies

2018, 122–142 – abrufbar unter https://petsymposium.org/2018/files/papers/issue2/popets-2018-0016.pdf.

Matthias, Andreas: Automaten als Träger von Rechten – Ein Plädoyer für eine Gesetzesänderung, 2007 (zit.: *Matthias*, Automaten als Träger von Rechten).

Maunz, Theodor/Dürig, Günter (Hrsg.): Grundgesetz, Kommentar, 91. Aufl., C.H. Beck, Stand: April 2020 (zit.: *Bearbeiter* in: Maunz/Dürig, GG-Kommentar).

Maunz, Theodor/Dürig, Günter (Hrsg.): Grundgesetz, Kommentar, Band I, Art. 1-69, 2. Aufl., C.H. Beck 1968 (zit.: *Bearbeiter* in: Maunz/Dürig, GG-Kommentar (1968)).

Maunz, Theodor/Dürig, Günter (Hrsg.): Grundgesetz, Kommentar, Band II, Art. 12-20 GG, 3. Aufl., C.H. Beck 2003 (zit.: *Bearbeiter* in: Maunz/Dürig, GG-Kommentar (2003)).

Maurer, Hartmut: Staatsrecht I, 5. Aufl., C.H. Beck 2007.

Meier, Klaus/Wehlau, Andreas: Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585–1591.

Meints, Martin/Reimer, Helmut: Identität – eine sichere Sache?, DuD 2006, 528.

Meissner, Michael: Persönlichkeitsschutz juristischer Personen im deutschen und US-amerikanischen Recht, Peter Lang Verlag 1998.

Merten, Detlef: Das konfuse Konfusionsargument, DÖV 2019, 41–47.

Merten, Detlef/Papier, Hans-Jürgen (Hrsg.): Handbuch der Grundrechte, Band I, Entwicklung und Grundlagen, C.H. Beck 2004 (zit.: *Bearbeiter* in: Merten/Papier, HGr I).

Merten, Detlef/Papier, Hans-Jürgen (Hrsg.): Handbuch der Grundrechte, Band II, Grundrechte in Deutschland: Allgemeine Lehren I, 2006 (zit.: *Bearbeiter* in: Merten/Papier, HGr II).

Merten, Detlef/Papier, Hans-Jürgen (Hrsg.): Handbuch der Grundrechte, Band III, Grundrechte in Deutschland: Allgemeine Lehren II, C.H. Beck 2009 (zit.: *Bearbeiter* in: Merten/Papier, HGr III).

Merten, Detlef/Papier, Hans-Jürgen (Hrsg.): Handbuch der Grundrechte, Band IV, Grundrechte in Deutschland: Einzelgrundrechte I, 2011 (zit.: *Bearbeiter* in: Merten/Papier, HGr IV).

Merten, Detlef/Papier, Hans-Jürgen (Hrsg.): Handbuch der Grundrechte, Band V, Grundrechte in Deutschland: Einzelgrundrechte II, C.H. Beck 2013 (zit.: *Bearbeiter* in: Merten/Papier, HGr V).

Meyer, Jochen/Fröhlich, Thomas/Holdt, Kai von: Corona-Warn-App – Erste Ergebnisse einer Online-Umfrage zur (Nicht-)Nutzung und Gebrauch, 24.11.2020 – abrufbar unter https://arxiv.org/abs/2011.11317.

Meyer, Julia: Identität und virtuelle Identität natürlicher Personen im Internet, 2011 (zit.: *Meyer*, Virtuelle Identität).

Meyer, Jürgen/Hölscheidt, Sven (Hrsg.): Charta der Grundrechte der Europäischen Union, 5. Aufl., Nomos Verlag 2019 (zit.: *Bearbeiter* in: Meyer/Hölscheidt, GrC-Kommentar).

Meyer, Stephan: Landesrechtliche Legaldefinitionen der „Anonymisierung" im Anwendungsbereich der DS-GVO, ZD 2021, 669–674.

Meyer-Abich, Jann: Der Schutzzweck der Eigentumsgarantie, Duncker & Humblot Verlag 1980.

Meyer-Ladewig, Jens/Nettesheim, Martin/Raumer, Stefan von (Hrsg.): Europäische Menschenrechtskonvention, Handkommentar, 4. Aufl., Nomos Verlag 2017 (zit.: *Bearbeiter* in: Meyer-Ladewig/Nettesheim/von Raumer, EMRK-Kommentar).

Michael, Lothar: Grundfälle zur Verhältnismäßigkeit, JuS 2001, 764–767.

Michl, Fabian: „Datenbesitz" – ein grundrechtliches Schutzgut? NJW 2019, 2729–2733.

Moos, Flemming: Unzulässiger Handel mit Persönlichkeitsprofilen? – Erstellung und Vermarktung kommerzieller Datenbanken mit Personenbezug, MMR 2006, 718–723.

Möstl, Markus: Probleme der verfassungsprozessualen Geltendmachung gesetzgeberischer Schutzpflichten, DÖV 1998, 1029–1039.

Muckel, Stefan: Begrenzung grundrechtlicher Schutzbereiche durch Elemente außerhalb des Grundrechtstatbestandes, in: Dörr, Dieter et al. (Hrsg.), Die Macht des Geistes, Festschrift für Hartmut Schiedermair, C.F. Müller 2001, S. 347–361 (zit.: *Muckel*, FS Schiedermair).

Müller-Franken, Sebastian: Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Verfassungsrechtliche Fragen, AfP 2018, 1–4.

Müller-Terpitz, Ralf: Der Schutz des pränatalen Lebens, 2007 (zit.: *Müller-Terpitz*, Schutz pränatalen Lebens).

Münch, Ingo von/Kunig, Philip (Hrsg.): Grundgesetz, Kommentar, Band I, Band 1: Präambel bis Art. 69, 6. Aufl., C.H. Beck 2012 (zit.: *Bearbeiter* in: von Münch/Kunig, GG).

Münch, Ingo von/Mager, Ute: Staatsrecht II – Grundrechte, 6. Aufl., Kohlhammer 2014.

Murswiek, Dietrich: Die staatliche Verantwortung für die Risiken der Technik, Duncker & Humblot Verlag 1985.

Murswiek, Dietrich: Grundrechtsdogmatik am Wendepunkt, Der Staat 45 (2006), 474–500.

Nahles, Andrea: Digitaler Fortschritt durch ein Daten-für-Alle-Gesetz, 2018 – abrufbar unter https://www.spd.de/fileadmin/Dokumente/Sonstiges/Daten_fuer_Alle.pdf.

Nationaler Normenkontrollrat (Hrsg.): Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren. 2017 – abrufbar

unter https://www.normenkontrollrat.bund.de/resource/blob/300864/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-download-nkr-gutachten-2017-data.pdf?download=1https://www.normenkontrollrat.bund.de/resource/blob/300864/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-download-nkr-gutachten-2017-data.pdf?download=1.

Nationaler Normenkontrollrat (Hrsg.): Stellungnahme zum Registermodernisierungsgesetz, 2020 – abrufbar unter https://www.normenkontrollrat.bund.de/resource/blob/72494/1791996/c768a4f68b89917b1c6ef904180bf6ed/20200915-stellungnahme-zum-regmodg-data.pdf.

Nebel, Maxi: Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung?, ZD 2015, 517–522.

Nettesheim: Grundrechtsschutz der Privatheit, VVDStRL 70 (2010), 7–49.

Nettesheim, Martin: „Leben in Würde“: Art. 1 Abs. 1 als Grundrecht hinter den Grundrechten, JZ 2019, 1–11.

Nettleton, David: A synthetic data generator for online social network graphs, Social Network Analysis and Mining 2016 – abrufbar unter https://link.springer.com/article/10.1007/s13278-016-0352-y.

Neuhäuser, Christian: Künstliche Intelligenzen und ihr moralischer Standpunkt, in: Beck, Susanne (Hrsg.), Jenseits von Mensch und Maschine, Nomos Verlag 2012, S. 23–42.

Neumann, Franz/Nipperdey, Hans Carl/Scheuner, Ulrich (Hrsg.): Die Grundrechte, Band II, 1954 (zit.: *Bearbeiter* in: Neumann/Nipperdey/Scheuner, Grundrechte II).

Nipperdey, Hans Carl (Hrsg.): Festschrift für Erich Molitor zum 75. Geburtstag, C.H. Beck 1962 (zit.: *Bearbeiter* in: Nipperdey, FS Molitor (1962)).

Nolte, Georg: Hate-Speech, Fake-News, das „Netzwerkdurchsetzungsgesetz“ und Vielfaltsicherung durch Suchmaschinen, ZUM 2017, 552–565.

Obergfell, Eva Inés: Personalisierte Preise im Lebensmittelhandeln – Vertragsfreiheit oder Kundenbetrug, ZLR 2017, 290–301.

Oetker, Hartmut: Unverhältnismäßige Herstellungskosten und das Affektionsinteresse im Schadensersatzrecht, NJW 1985, 345–351.

Ohly, Ansgar: Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441–451.

Olejnik, Lukasz/Castelluccia, Claude/Janc, Arthur: On the uniqueness of Web browsing history patterns, Annals of Telecommunications 2014, 63 ff – abrufbar unter https://hal.inria.fr/hal-00917042/document.

Paal, Boris: Missbrauchstatbestand und Algorithmic Pricing, GRUR 2019, 43–53.

Paal, Boris P./Pauly, Daniel A. (Hrsg.): Beck'sche Kompakt-Kommentare Datenschutz-Grundverordnung, 3. Aufl., C.H. Beck 2021 (zit.: *Bearbeiter* in: Paal/Pauly, DSGVO).

Peifer, Karl-Nikolaus: Individualität im Zivilrecht, Mohr Siebeck 2001.

Peifer, Karl-Nikolaus: Eigenheit oder Eigentum – Was schützt das Persönlichkeitsrecht?, GRUR 2002, 495–500.

Peifer, Karl-Nikolaus: Verhaltensorientierte Nutzeransprache – Tod durch Datenschutz oder Moderation durch das Recht?, K&R 2011, 543–547.

Peifer, Karl-Nikolaus: Fake News und Providerhaftung, CR 2017, 809–813.

Peifer, Karl-Nikolaus: Netzwerkdurchsetzungsgesetz: Selbstbehauptung des Rechts oder erster Schritt in die selbstregulierte Vorzensur? – Zivilrechtliche Aspekte, AfP 2018, 14–23.

Pesch, Paulina Jo: Cryptocoin-Schulden, C.H. Beck 2017.

Peschel, Christopher/Rockstroh, Sebastain: Big Data in der Industrie – Chancen und Risiken neuer datenbasierter Dienste, MMR 2014, 571–576.

Petrlic, Ronald/Sorge, Christoph: Datenschutz, Springer 2017.

Pieper, Fritz-Ulli: Künstliche Intelligenz: Im Spannungsfeld von Recht und Technik, DSRITB 2017, 555–573.

Pietrzak, Alexandra: Die Schutzpflicht im verfassungsrechtlichen Kontext – Überblick und neue Aspekte, JuS 1994, 748–753.

Plath, Kai-Uwe/Grages, Jan-Michael: „Let's Stay in Touch" – Direktwerbung unter der DSGVO, CR 2018, 770–782.

Platon; Guth, Karl-Maria (Hrsg.): Das Gastmahl (Symposion), Contumax 2016.

Podszun, Rupprecht/Schwalbe, Ulrich: Digitale Plattformen und GWB-Novelle: Überzeugende Regeln für die Internetökonomie?, NZKart 2017, 98–106.

Pollmann, Maren/Kipker, Dennis-Kenji: Informierte Einwilligung in der Online-Welt, DuD 2016, 378–381.

Popp, Andreas: Informationstechnologie und Strafrecht, JuS 2011, 385–392.

Poscher, Ralf: Grundrechte als Abwehrrechte, Mohr Siebeck 2003.

Pritzel, Monika/Brand, Matthias/Markowitsch, Hans J.: Gehirn und Verhalten, Spektrum Verlag 2009.

Privacy International: How Apps on Android Share Data with Facebook (even if you don't have a Facebook account), 2018 – abrufbar unter https://privacyinternational.org/report/2647/how-apps-android-share-data-facebook-report.

Prütting, Hanns: Sachenrecht, 36. Aufl., C.H. Beck 2017.

Quante, Frank: Das allgemeine Persönlichkeitsrecht juristischer Personen, Peter Lang Verlag 1999.

Quinn, Regina Ammicht et al.: White Paper Tracking, forum privatheit 2018 – abrufbar unter http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-4972611.pdf.

Rabe, Christian: Zur Begrenzung des sachlichen Anwendungsbereiches der DSGVO, K&R 2019, 464–467.

Radke, Tristan: Datengestützte Wahlwerbung wie Microtargeting aus datenschutzrechtlicher Perspektive, K&R 2020, 479–486.

Raji, Behrang: Rechtliche Bewertung synthetischer Daten für KI-Systeme, DuD 2021, 303–309.

Raue, Benjamin: Die Rechte des Sacheigentümers bei der Erhebung von Daten, NJW 2019, 2425–2430.

Rauer, Nils/Ettig, Diana: Rechtskonformer Einsatz von Cookies – Aktuelle Rechtslage und Entwicklungen, ZD 2018, 255–258.

Redeker, Helmut: Information als eigenständiges Rechtsgut, CR 2011, 634–639.

Regenthal, Gerhard: Ganzheitliche Corporate Identity, 2. Aufl., Springer 2009.

Richter, Heiko: Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance", ZEuP 2021, 634–667.

Richter, Heiko/Hilty, Reto M.: Die Hydra des Dateneigentums – eine methodische Betrachtung, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, Erich Schmidt Verlag 2019, S. 241–260.

Riehm, Thomas: Nein zur ePerson – Gegen die Anerkennung einer digitalen Rechtspersönlichkeit, RDi 2020, 42–48.

Rixen, Stephan: Die Bestattung fehlgeborener Kinder als Rechtsproblem, FamRZ 1994, 417–425.

Robbers, Gerhard: Der Grundrechtsverzicht, JuS 1985, 925–931.

Robbers, Gerhard: Sicherheit als Menschenrecht, Nomos Verlag 1987.

Rocher, Luc/Hendrickx, Julien M./Montjoye, Yves-Alexandre de: Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications 10 2019, Nr. 1, 3069 ff – abrufbar unter https://doi.org/10.1038/s41467-019-10933-3.

Roesler, Christian: Individuelle Identitätskonstitution und kollektive Sinnstiftungsmuster, Universität Freiburg 2001 – abrufbar unter https://freidok.uni-freiburg.de/data/527 (zit.: *Roesler*, Identitätskonstruktion).

Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht, C.H. Beck 2003.

Roßnagel, Alexander: Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71–75.

Roßnagel, Alexander (Hrsg.): Allgegenwärtige Identifizierung?, Nomos Verlag 2006.

Roßnagel, Alexander: Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht?, ZD 2018, 339–344.

Roßnagel, Alexander: Pseudonymisierung personenbezogener Daten, ZD 2018, 243–247.

Roßnagel, Alexander: Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht – Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff, NJW 2019, 1–5.

Roßnagel, Alexander/Geminn, Christian L.: Vertrauen in Anonymisierung – Regulierung der Anonymisierung zur Förderung Künstlicher Intelligenz, ZD 2021, 487–490.

Roßnagel, Alexander/Scholz, Philip: Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721–731.

Röttgen, Charlotte/Jülicher, Tim: Der Bot, das unbekannte Wesen – Ein rechtlicher Überblick, DSRITB 2017, 227–241.

Rüscher, Daniel: Alexa, Siri und Google als digitale Spione im Auftrag der Ermittlungsbehörden?, NStZ 2018, 687–692.

Rux, Johannes: Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, 285–295.

Sachs, Michael (Hrsg.): Grundgesetz, Kommentar, 8. Aufl., 2018 (zit.: *Bearbeiter* in: Sachs, GG).

Sachs, Michael/Krings, Thomas: Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, JuS 2008, 481–486.

Säcker, Franz Jürgen et al. (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 4, 8. Aufl., C.H. Beck 2019 (zit.: *Bearbeiter* in: Säcker et al., MüKo BGB, Bd. IV).

Säcker, Franz Jürgen et al. (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 6, 8. Aufl., C.H. Beck 2020 (zit.: *Bearbeiter* in: Säcker et al., MüKo BGB, Bd. VI).

Säcker, Franz Jürgen et al. (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 7, 8. Aufl., C.H. Beck 2020 (zit.: *Bearbeiter* in: Säcker et al., MüKo BGB, Bd. VII).

Säcker, Franz Jürgen et al. (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 10, 8. Aufl., C.H. Beck 2020 (zit.: *Bearbeiter* in: Säcker et al., MüKo BGB, Bd. X).

Säcker, Franz Jürgen et al. (Hrsg.): Münchener Kommentar zum Bürgerlichen Gesetzbuch, Band 1, 9. Aufl., C.H. Beck 2021 (zit.: *Bearbeiter* in: Säcker et al., MüKo BGB, Bd. I).

Sandfuchs, Barbara: Privatheit wider Willen? – Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht, Mohr Siebeck 2015 (zit.: *Sandfuchs*, Privatheit wider Willen).

Sattler, Andreas: Personenbezogene Daten als Leistungsgegenstand, JZ 2017, 1036–1046.

Schallaböck, Jan: Identitätsmanagement als Grundlage von Verhaltenssteuerung, in: Hornung, Gerrit/Engemann, Christoph (Hrsg.), Der digitale Bürger und seine Identität, Nomos Verlag 2016, S. 103–130.

Schallbruch, Martin: Mehr Unabhängigkeit für das BSI? DuD 2021, 229–233.

Schaub, Renate: Interaktion von Mensch und Maschine, JZ 2017, 342–349.

Schefzig, Jens: Die Datenlizenz, DSRITB 2015, 551–567.

Schertz, Christian: Der Schutz des Individuums in der modernen Mediengesellschaft, NJW 2013, 721–728.

Schläger, Uwe/Thode, Jan-Christoph (Hrsg.): Handbuch Datenschutz und IT-Sicherheit, Erich Schmidt Verlag 2018.

Schleipfer, Stefan: Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, 460–466.

Schleipfer, Stefan: Pseudonymität in verschiedenen Ausprägungen, ZD 2020, 284–291.

Schliesky, Utz et al.: Schutzpflichten und Drittwirkung im Internet, Nomos Verlag 2014.

Schlink, Bernhard: Aktuelle Fragen des pränatalen Lebensschutzes, De Gruyter 2002.

Schmehl, Arndt/Richter, Eike: Referendarexamensklausur – Öffentliches Recht: Virtuelles Hausverbot und Informationsfreiheit, JuS 2005, 817–824.

Schmidl, Michael: IT-Recht von A-Z, C.H. Beck 2008.

Schmidt-Bleibtreu, Bruno/Hofmann, Hans/Henneke, Hans-Günter (Hrsg.): Grundgesetz, Kommentar, 13. Aufl., 2014 (zit.: *Bearbeiter* in: Schmidt-Bleibtreu/Hofmann/Henneke, GG-Kommentar).

Schmidt-Jortzig, Edzard: IT-Revolution und Datenschutz, DÖV 2018, 10–15.

Schmitz, Barbara: Der Abschied vom Personenbezug, ZD 2018, 5–8.

Schmitz, Peter: E-Privacy-VO – unzureichende Regeln für klassische Dienste, ZRP 2017, 172–175.

Schnabel, Christoph: Rechtswidrige Praktiken als Betriebs- und Geschäftsgeheimnisse?, CR 2016, 342–348.

Schnabel, Christoph: Das Recht der informationellen Selbstbestimmung für Unternehmen, WM 2019, 1384–1389.

Schnabel, Christoph/Freund, Bernhard: „Ach wie gut, dass niemand weiß...“ – Selbstdatenschutz bei der Nutzung von Telemedienangeboten, CR 2010, 718–721.

Schneider, Uwe Klaus: Einrichtungsübergreifende elektronische Patientenakten, Springer 2016.

Schönke, Adolf/Schröder, Horst (Hrsg.): Strafgesetzbuch, Kommentar, 30. Aufl., C.H. Beck 2019 (zit.: *Bearbeiter* in: Schönke/Schröder, StGB-Kommentar).

Schröder, Ulrich Jan: Der Schutzbereich der Grundrechte, JA 2016, 641–648.

Schulz, Sebastian: Datenschutz durch Technikgestaltung im nationalen und europäischen kontext, CR 2012, 204–208.

Schulz, Sönke E.: Dateneigentum in der deutschen Rechtsordnung, PinG 2018, 72–79.

Schumacher, Pascal: Breitband-Universaldienst: Möglichkeiten und Grenzen deutscher Politik – Funktionales Internet endlich für alle?, MMR 2011, 711–715.

Schuppert, Gunnar Folke: Funktionell-rechtliche Grenzen der Verfassungsinterpretation, Athenäum 1980.

Schuster, Fabian: Sicherheit von Daten und Geheimnis im Vertrag, CR 2020, 726–730.

Schwabe, Jürgen: Probleme der Grundrechtsdogmatik, 2. Aufl., 1997.

Schwabenbauer, Thomas: Kommunikationsschutz durch Art. 10 GG im digitalen Zeitalter, AöR 137 (2012), 1–41.

Schwartmann, Rolf (Hrsg.): Praxishandbuch Medien-, IT- und Urheberrecht, 3. Aufl., C.F. Müller 2014.

Schwartmann, Rolf/Hentsch, Christian-Henner: Parallelen aus dem Urheberrecht für ein neues Datenverwertungsrecht, PinG 2016, 117–126.

Schwartmann, Rolf et al. (Hrsg.): DS-GVO/BDSG, Kommentar, 2. Aufl., C.F. Müller 2020 (zit.: *Bearbeiter* in: Schwartmann et al., DSGVO/BDSG).

Schwartmann, Rolf/Weiß, Steffen (Hrsg.): Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung, Fokusgruppe Datenschutz des Digital-Gipfels 2019 – abrufbar unter https://www.gdd.de/downloads/aktuelles/whitepaper/Fokusgruppe_DatenschutzEntwurf_CoC_Pseudonymisierung_V1.0.pdf.

Schwarze, Jürgen (Hrsg.): EU-Kommentar, 3. Aufl., 2012.

Schweitzer, Heike/Peitz, Martin: Ein europäischer Ordnungsrahmen für Datenmärkte?, NJW 2018, 275–280.

Seidel, Ulrich: Das Grundrecht auf Datensouveränität, ZG 2014, 153–165.

Seidler, Katharina: Der digitale Nachlass – ein Zwischenstand, NZFam 2020, 141–145.

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra (Hrsg.): Datenschutzrecht, DSGVO mit BDSG, Nomos Verlag 2019 (zit.: *Bearbeiter* in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG).

Simmel, Georg: Soziologie – Untersuchungen über die Formen der Vergesellschaftung, 7. Aufl., Duncker & Humblot Verlag 2013.

Singelnstein, Tobias: Ausufernd und fehlplatziert: Der Tatbestand der Datenhehlerei (§ 202d StGB) im System des strafrechtlichen Daten- und Informationsschutzes, ZIS 2016, 432–439.

Smart, Andrew: Beyond Zero and One – Machines, Psychedelics and Conciousness, OR Books 2015 (zit.: *Smart*, Beyond Zero and One).

Söbbing, Thomas: Der Datenskandal bei Facebook und die rechtliche Zulässigkeit von künstlicher Intelligenz zur Beeinflussung der politischen Willensbildung (sog. Microtargeting), InTeR 2018, 182–188.

Sorge, Christoph: Digitaler Nachlass als Knäuel von Rechtsverhältnissen, MMR 2018, 372–377.

Sorge, Christoph/Leicht, Maximilian: Registermodernisierungsgesetz – eine datenschutzgerechte Lösung? ZRP 2020, 242–244.

Specht, Louisa: Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288–296.

Specht, Louisa/Herold, Sophie: Roboter als Vertragspartner?, MMR 2018, 40–44.

Specht, Louisa/Rohmer, Rebecca: Zur Rolle des informationellen Selbstbestimmungsrechts bei der Ausgestaltung eines möglichen Ausschließlichkeitsrechts an Daten, PinG 2016, 127–132.

Spektrum (Hrsg.): Lexikon der Psychologie, Spektrum Akademischer Verlag 2000 – abrufbar unter http://www.spektrum.de/lexikon/psychologie/identitaet/6968.

Sperlich, Tim: Das Recht auf Datenübertragbarkeit, DuD 2017, 377.

Spilker, Bettina: Postmortaler Schutz durch das Grundgesetz, DÖV 2014, 637–642.

Spilker, Bettina: Postmortaler Datenschutz, DÖV 2015, 54–60.

Spindler, Gerald: Rechtsdurchsetzung von Persönlichkeitsrechten, GRUR 2018, 365–373.

Spindler, Gerald/Schmitz, Peter/Liesching, Marc (Hrsg.): Telemediengesetz mit Netzwerkdurchsetzungsgesetz, 2. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: Spindler/Schmitz/Liesching, TMG).

Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 3. Aufl., 2015.

Spranger, Tade Matthias/Wegmann, Henning: Öffentlich-rechtliche Dimensionen der Robotik, in: Beck, Susanne (Hrsg.), Jenseits von Mensch und Maschine, Nomos Verlag 2012, S. 105–118.

Stadler, Theresa/Oprisanu, Bristena/Troncoso, Carmela: Synthetic Data – Anonymisation Groundhog Day, – abrufbar unter https://arxiv.org/abs/2011.07018.

Starck, Christian: Praxis der Verfassungsauslegung, Nomos Verlag 1994.

Steinbach, Armin: Social Bots im Wahlkampf, ZRP 2017, 101–105.

Steiner, Anton/Holzer, Anna: Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262–266.

Steinrötter, Björn: Vermeintliche Ausschließlichkeitsrechte an binären Codes, MMR 2017, 731–736.

Stender-Vorwachs, Jutta/Steege, Hans: Wem gehören unsere Daten? – Zivilrechtliche Analyse zur Notwendigkeit eines dinglichen Eigentums an Daten, der Datenzuordnung und des Datenzugangs, NJOZ 2018, 1361–1367.

Stern, Klaus (Hrsg.): Das Staatsrecht der Bundesrepublik Deutschland, Band III/1, C.H. Beck 1988 (zit.: *Stern*, StaatsR III/1).

Stern, Klaus; Siekmann, Helmut (Hrsg.): Der Staat des Grundgesetzes, Carl Heymanns Verlag KG 1992.

Stern, Klaus (Hrsg.): Das Staatsrecht der Bundesrepublik Deutschland, Band III/2, C.H. Beck 1994 (zit.: *Stern*, StaatsR III/2).

Stern, Klaus (Hrsg.): Das Staatsrecht der Bundesrepublik Deutschland, Band IV/1, 2006 (zit.: *Stern*, StaatsR IV/1).

Stiemerling, Oliver: „Künstliche Intelligenz" – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge, CR 2015, 762–765.

Stober, Rolf: Grundpflichten und Grundgesetz, Duncker & Humblot Verlag 1979.

Stober, Rolf: Grundpflichten als verfassungsrechtliche Dimension, NVwZ 1982, 473–479.

Stranz, Natalia: Eigentumsrecht an personenbezogenen Daten, 2016.

Strauß, Stefan: Datenschutzimplikationen staatlicher Identitätsmanagement-Systeme, DuD 2010, 99–103.

Strauß, Stefan: Identifizierbarkeit in soziotechnischen Systemen, DuD 2018, 497–501.

Streinz, Rudolf: EUV/AEUV-Kommentar, 3. Aufl., 2018.

Strubel, Michael: Anwendungsbereich des Rechts auf Datenübertragbarkeit, ZD 2017, 355–361.

Stuckenberg, Carl-Friedrich: Der missratene Tatbestand der neuen Datenhehlerei (§ 202d StGB), ZIS 2016, 526–533.

Stürmer, Verena: Löschen durch Anonymisieren? – Mögliche Erfüllung der Löschpflicht nach Art. 17 DS-GVO, ZD 2020, 626–631.

Sydow, Gernot (Hrsg.): Europäische Datenschutzgrundverordnung, 2. Aufl., Nomos Verlag 2018 (zit.: *Bearbeiter* in: Sydow, DS-GVO).

Taeger, Jürgen/Pohle, Jan (Hrsg.): Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, 36. Aufl., C.H. Beck, Stand: Februar 2021 (zit.: *Bearbeiter* in: Taeger/Pohle, Computerrechts-Handbuch).

Taraz, Daniel: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und die Gewährleistung digitaler Privatheit im grundrechtlichen Kontext, Verlag Dr. Kovač 2016 (zit.: *Taraz*, GGVIS und Gewährleistung digitaler Privatheit).

Tillmann, Tristan Julian/Vogt, Verena: Personalisierte Preise im Big-Data-Zeitalter, VuR 2018, 447–455.

Trappl, Robert: A Construction Manual for Robots' Ethical Systems, Springer 2015.

Tucker, Patrick: Has Big Data Made Anonymity Impossible?, MIT Technology Review 4 2013, 64 ff – abrufbar unter https://www.technologyreview.com/2013/05/07/178542/has-big-data-made-anonymity-impossible/.

Turing, Alan: Computing Machinery and Intelligence, Mind 1950, 433–460.

Tzemos, Vasileios: Das Untermaßverbot, Peter Lang Verlag 2004.

Uhrenbacher, Pia Elisa: Digitales Testament und digitaler Nachlass, Peter Lang Verlag 2017.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Hrsg.): Verkettung digitaler Identitäten, 2007 – abrufbar unter https://www.datenschutzzentrum.de/projekte/verkettung/.

Unruh, Peter: Zur Dogmatik der grundrechtlichen Schutzpflichten, Duncker & Humblot Verlag 1996.

Veil, Winfried: Die Schutzgutmisere des Datenschutzrechts (Teil I), 2019 – abrufbar unter https://www.cr-online.de/blog/2019/02/06/die-schutzgutmisere-des-datenschutzrechts-teil-i/ (zit.: *Veil*, Schutzgutmisere des Datenschutzrechts (Teil I)).

Venkatadri, Giridhari et al.: Investigating sources of PII used in Facebooks targeted advertising, Proceedings on Privacy Enhancing Technologies 2018, 227–244 – abrufbar unter https://www.researchgate.net/publication/330121178_Investigating_sources_of_PII_used_in_Facebook%27s_targeted_advertising.

Venzke-Caprarese, Sven: Retargeting in der Onlinewerbung, DuD 2017, 577–582.

Venzke-Carparese, Sven: Haftungsrisiko Webtracking, DuD 2018, 156–158.

Vettermann, Oliver: BSI-Sicherheitstest revisited: Besserer Schutz durch DSGVO und Co. möglich?, in: Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung:

Tagungsband zum 16. Deutschen IT-Sicherheitskongress, Secumedia 2019, S. 253–263.

von Ulmenstein, Ulrich: Datensouveränität durch repräsentative Rechtswahrnehmung, DuD 2020, 528–534.

Wagner, Gerald: Vertrauen in Technik, Zeitschrift für Soziologie 1994, 145–157.

Wahl, Rainer/Masing, Johannes: Schutz durch Eingriff, JZ 1990, 553–563.

Wahlster, Wolfgang: Künstliche Intelligenz als Grundlage autonomer Systeme, Informatik Spektrum 2017, 409–418.

Wamser, Christoph/Fink, Dietmar H. (Hrsg.): Marketing-Management mit Multimedia, Gabler 1997.

Wandtke, Arthur-Axel: Ökonomischer Wert von persönlichen Daten, MMR 2017, 6–12.

Wandtke, Arthur-Axel/Bullinger, Winfried (Hrsg.): Praxiskommentar zum Urheberrecht, 5. Aufl., C.H. Beck 2019 (zit.: *Bearbeiter* in: Wandtke/Bullinger, Praxiskommentar UrhR).

Wandtke, Arthur-Axel/Ohst, Claudia (Hrsg.): Medienrecht Praxishandbuch, Band IV, 3. Aufl., 2014.

Watteler, Oliver/Kinder-Kurlanda, Katharina E.: Anonymisierung und sicherer Umgang mit Forschungsdaten in der empirischen Sozialforschung, DuD 2015, 515–519.

Weberling, Johannes: Informations- und Auskunftspflichten der öffentlichen Hand gegenüber Medien in der Praxis, AfP 2003, 304–307.

Welp, Jürgen: Datenveränderung (§ 303a StGB) – Teil 1, iur 1988, 443–449.

Wendehorst, Christiane: Die Digitalisierung und das BGB, NJW 2016, 2609–2613.

Wenhold, Céline: Nutzerprofilbildung durch Webtracking, Nomos Verlag 2018.

Westermann, Harry: Steht der Genossenschaft das „Allgemeine Persönlichkeitsrecht“ zu?, in: Institut für Genossenschaftswesen (Hrsg.), Gegenwartsprobleme genossenschaftlicher Selbsthilfe, Buchdruckerei Universal 1960, S. 345–353.

Wick, Christoph: Deep Learning, Informatik Spektrum 2017, 103–107.

Wicki, Werner: Entwicklungspsychologie, UTB 2015.

Wiebe, Andreas/Schur, Nico: Ein Recht an industriellen Daten im verfassungsrechtlichen Spannungsverhältnis zwischen Eigentumsschutz, Wettbewerbs- und Informationsfreiheit, ZUM 2017, 461–473.

Willems, Constantin: Erben 2.0 – zur Beschränktbarkeit der Rechtsnachfolge in das „digitale Vermögen“, ZfPW 2016, 494–512.

Wilms, Jan/Roth, Jan: Die Anwendbarkeit des Rechts auf informationelle Selbstbestimmung auf juristische Personen i. S. von Art. 19 III GG, JuS 2004, 577–580.

Windley, Phillip J.: Digital Identity, O’Reilly 2005.

Winter, Christian/Battis, Verena/Halvani, Oren: Herausforderungen für die Anonymisierung von Daten, ZD 2019, 489–493.

Wolf, Fabiana: Der Schutz des Betriebs- und Geschäftsgeheimnisses, Nomos Verlag 2015.

Wolff, Heinrich Amadeus: Der verfassungsrechtliche Schutz der Betriebs- und Geschäftsgeheimnisse, NJW 1997, 98–101.

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.): BeckOK Datenschutzrecht, 33. Aufl., C.H. Beck, Stand: 01.05.2020 (zit.: *Bearbeiter* in: Wolff/Brink, BeckOK DatenschutzR).

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.): BeckOK Datenschutzrecht, 38. Aufl., C.H. Beck, Stand: 01.11.2021 (zit.: *Bearbeiter* in: Wolff/Brink, BeckOK DatenschutzR).

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.): BeckOK Datenschutzrecht, 28. Aufl., C.H. Beck 2017, Stand: 01.05.2017 (zit.: *Bearbeiter* in: Wolff/Brink, BeckOK DatenschutzR (28. Edition)).

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.): BeckOK Datenschutzrecht, 23. Aufl., C.H. Beck 2018 (zit.: *Bearbeiter* in: Wolff/Brink, BeckOK DatenschutzR (23. Edition)).

Wronka, Georg: Das Persönlichkeitsrecht juristischer Personen, Universität Bonn 1972.

Wybitul, Tim: Selbst- oder Fremdbestimmung – gilt das Freiheitsgrundrecht auch in der Datensicherheit?, ZD 2013, 539–542.

Zarr, Peter: Wann beginnt die Menschenwürde nach Art. 1 GG?, Nomos Verlag 2005 (zit.: *Zarr*, Menschenwürde).

Zech, Herbert: Information als Schutzgegenstand, Mohr Siebeck 2012.

Zech, Herbert: Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“, CR 2015, 137–146.

Ziegelmayer, David: Die Reputation als Rechtsgut, GRUR 2012, 761–765.

SCHRIFTEN DES ZENTRUMS FÜR ANGEWANDTE RECHTSWISSENSCHAFT

Karlsruher Institut für Technologie (KIT) | ISSN 1860-8744

Band 1 THOMAS DREIER | ELLEN EULER (Hrsg.)
Kulturelles Gedächtnis im 21. Jahrhundert. Tagungsband des internationalen Symposiums, 23. April 2005, Karlsruhe.
ISBN 3-937300-56-2

Band 2 CHRISTOPH SORGE
Softwareagenten. Vertragsschluss, Vertragsstrafe, Reugeld.
ISBN 3-937300-91-0

Band 3 JOSÉ LUIS CÁRDENAS T.
Rolle, Kriterien und Methodik der kartellrechtlichen Marktabgrenzung. Eine juristische und ökonomische Analyse.
ISBN 3-937300-93-7

Band 4 WOLFGANG W. GÖPFERT
Die Strafbarkeit von Markenverletzungen.
ISBN 3-937300-97-X

Band 5 CHRISTIAN KAU
Vertrauensschutzmechanismen im Internet, insbesondere im E-Commerce.
ISBN 3-86644-036-7

Band 6 ALEXANDER MOHR
Internetspezifische Wettbewerbsverstöße.
ISBN 3-86644-047-2

Band 7 FABIAN SCHÄFER
Der virale Effekt. Entwicklungsrisiken im Umfeld von Open Source Software.
ISBN 978-3-86644-141-5

Die Bände sind unter www.ksp.kit.edu als PDF frei verfügbar oder als Druckausgabe bestellbar.

Band 8 RETO MANTZ
Rechtsfragen offener Netze: Rechtliche Gestaltung und Haftung des Access Providers in zugangsoffenen (Funk-)Netzen.
ISBN 978-3-86644-222-1

Band 9 STEFAN BOLAY
Mehrwertgebührenpflichtige Telefon- und SMS-Gewinnspiele: Eine rechtliche Einordnung am Beispiel aktueller Erscheinungsformen des Rundfunks.
ISBN 978-3-86644-259-7

Band 10 OLIVER MEYER
Aktuelle vertrags- und urheberrechtliche Aspekte der Erstellung, des Vertriebs und der Nutzung von Software.
ISBN 978-3-86644-280-1

Band 11 SASCHA THEISSEN
Risiken informations- und kommunikationstechnischer (IKT-) Implantate im Hinblick auf Datenschutz und Datensicherheit.
ISBN 978-3-86644-343-3

Band 12 CHRISTIAN FUNK
Allgemeine Geschäftsbedingungen in Peer-to-Peer-Märkten.
ISBN 978-3-86644-504-8

Band 13 ANNE VAN RAAY
Gewinnabschöpfung als Präventionsinstrument im Lauterkeitsrecht: Möglichkeiten und Grenzen effektiver Verhaltenssteuerung durch den Verbandsanspruch nach § 10 UWG; Untersuchung unter vergleichender Heranziehung insbesondere der Verletzergewinnhaftung im Rahmen der dreifachen Schadensberechnung nach Immaterialgutsverletzungen.
ISBN 978-3-86644-811-7

Band 14 NADINE SCHÜTTEL
Streitbeilegung im Internet – Zukunft oder Irrweg?
ISBN 978-3-7315-0300-2

Band 15 THOMAS DREIER | INDRA SPIECKER GEN. DÖHMANN (Hrsg.)
Informationsrecht@KIT –
15 Jahre Zentrum für Angewandte Rechtswissenschaft.
ISBN 978-3-7315-0367-5

Band 16 STEFFEN ALBRECHT
Verwaiste Werke – Vom rechtlichen Problem zur rechtspraktischen Herausforderung bei der Nutzung vorbestehender Inhalte.
ISBN 978-3-7315-0687-4

Die Bände sind unter www.ksp.kit.edu als PDF frei verfügbar oder als Druckausgabe bestellbar.

Band 17 MIEKE LORENZ
Optimierung von Verfahren zur Lösung rechtsrelevanter Wissensprobleme in kritischen Infrastrukturen: Befunde im Smart Grid und technikrechtliche Empfehlungen.
ISBN 978-3-7315-0716-1

Band 18 THOMAS OTTER
Externalities and Enterprise Software: Helping and Hindering Legal Compliance.
ISBN 978-3-7315-0937-0

Band 19 OLIVER VETTERMANN
Der grundrechtliche Schutz der digitalen Identität unter Berücksichtigung von Datenschutz- und IT-Sicherheitsrecht.
ISBN 978-3-7315-1213-4

ZAR

KARLSRUHER INSTITUT FÜR TECHNOLOGIE (KIT)
INSTITUT FÜR INFORMATIONS- UND WIRTSCHAFTSRECHT

Die digitale Identität ist die unumgängliche Schnittstelle des Menschen bei der Interaktion im Internet oder mit IT-Systemen, um die Vielzahl von Dienstleistungen zu ermöglichen. Keine Plattform kann genutzt werden, ohne dass zum abrufenden Nutzer ein (zumindest temporäres) Datenkonstrukt geschaffen wird, welches die Identität des Nutzers widerspiegelt und eine Zuordnung der Anwendungsdaten ermöglicht. Die Omnipräsenz dieser Abbilder unserer Identität ist zugleich ein Problem in rechtlicher Hinsicht, denn trotz der eigentlichen Gewahrwerdung des Gesetzgebers hinsichtlich der Digitalisierung und einer möglichen industriellen Revolution durch neue Informationstechnik ist er bzw. das Volk kaum durch rechtliche Mittel gegen Gefahren aus der digitalen Welt gewappnet. Die bislang einzige Möglichkeit, bereits eingetretenen Verletzungen entsprechend Rechnung zu tragen und für kommende Gefahren eine Leitlinie zu forcieren, ist die Auslegung bestehender Gesetze im Lichte der Verfassung. Grundlegend muss daher gefragt werden: Bietet der grundrechtliche Rahmen hinreichenden Schutz für digitale Identitäten? Finden sich konkrete Ansatzpunkte der Ausgestaltung bereits im Datenschutz- und IT-Sicherheitsrecht? Und, wenn nicht, wie wirken sich mögliche Änderungen einfacher Gesetze oder eine Erweiterung des Grundgesetzes in der Zukunft darauf aus?

ISSN 1860-8744 | ISBN 978-3-7315-1213-4

ISBN 978-3-7315-1213-4
9 783731 512134

Gedruckt auf FSC-zertifiziertem Papier