FLORIAN NIKOLAS WITTNER

Verantwortlichkeit in komplexen Daten-Ökosystemen

Internet und Gesellschaft
27

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Matthias C. Kettemann,
Björn Scheuermann, Thomas Schildhauer
und Wolfgang Schulz

27

Florian Nikolas Wittner

Verantwortlichkeit in komplexen Daten-Ökosystemen

Versuch einer Weiterentwicklung des Datenschutzes im Kontext der verteilten Verarbeitungsrealität

Mohr Siebeck

Florian Nikolas Wittner, geboren 1990; Studium der Rechtswissenschaft mit dem Schwerpunkt Geistiges Eigentum an der Universität Freiburg i.Br. und der Nationalen und Kapodistrias-Universität Athen; Wissenschaftlicher Mitarbeiter am Leibniz-Institut für Medienforschung/Hans-Bredow-Institut (HBI) im Projekt „Information Governance Technologies"; 2021 Promotion; Rechtsreferendar am Hanseatischen Oberlandesgericht.
orcid.org/0000-0002-3835-0802

ISBN 978-3-16-161300-5 / eISBN 978-3-16-161301-2
DOI 10.1628/978-3-16-161301-2

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von epline in Böblingen aus der Times gesetzt und von Laupp & Göbel in Gomaringen auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Printed in Germany.

Meiner Familie

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2021 von der Rechtswissenschaftlichen Fakultät der Universität Hamburg als Dissertationsschrift angenommen. Gesetzgebung, Literatur und Rechtsprechung sind grundsätzlich auf dem Stand Januar 2021, vereinzelt konnte aktuelle Rechtsprechung und Literatur bis Januar 2022 berücksichtigt werden.

Mein herzlicher Dank gebührt zuvörderst meinem Doktorvater Prof. Dr. Wolfgang Schulz, der die Entwicklung dieser Arbeit durch seine stets wertvollen und kritischen Denkanstöße und Diskussionen sowie nicht zuletzt die begleitenden kulinarischen Impulse entscheidend geprägt und bereichert hat. Großer Dank gebührt außerdem Prof. Dr. Marion Albers für die zügige Erstellung des Zweitgutachtens.

Für die großzügige finanzielle Förderung der Veröffentlichung der Arbeit bedanke ich mich bei dem Publikationsfonds für Open-Access-Monografien der Leibniz-Gemeinschaft und bei der VolkswagenStiftung.

Die Arbeit ist das Ergebnis meiner Mitarbeit im interdisziplinären Forschungsprojekt „Information Governance Technologies: Ethics, Policies, Architecture“, finanziert von der Landesforschungsförderung Hamburg. Der Projektleitung und dem gesamten Kollegium, insbesondere Dr. Christian Kurtz, danke ich für die spannende und schöne Zeit, die mich neben vielen Grundlagen und Ideen für meine Arbeit auch die grundlegende Bedeutung interdisziplinärer Forschung gelehrt hat.

Auch das Kollegium am Leibniz-Institut für Medienforschung | Hans-Bredow-Institut hat meine Zeit dort fachlich wie menschlich mehr als bereichert und hatte so großen Anteil am erfolgreichen Abschluss meines Forschungsprojekts. Namentlich und nicht abschließend genannt werden sollen hier insbesondere Dr. Stephan Dreyer, Dr. Matthias K. Klatt, Keno C. Potthast, Johannes H. Schmees, Dr. Tobias Mast, Anne-Kristin Polster, Dr. Amélie Pia Heldt, und Prof. Dr. Matthias C. Kettemann, LL.M. (Harvard).

Zuletzt gebührt der größte Dank zum einen meinen Eltern, die mich entscheidend geprägt und auf dem Weg zum Abschluss dieser Arbeit immer unterstützt und gefördert haben; zum anderen Dr. Josephine Doll, die den mitunter steinigen Weg der Promotionszeit mit mir durchlaufen und durch ihre Unterstützung und Teilnahme immer zu etwas ganz Besonderem gemacht hat.

Hamburg, im Mai 2022 *Florian Nikolas Wittner*

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	anderer Ansicht
a. a. O.	am angegebenen Ort
a. E.	am Ende
a. F.	alte Fassung
ABl.	Amtsblatt
Abs.	Absatz
AcP	Archiv für die civilistische Praxis (Zeitschrift)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AK	Arbeitskreis
AIMag	AI Magazine (Zeitschrift)
allg.	allgemein
Alt.	Alternative
anh.	anhängig
Anm.	Anmerkung
AöR	Archiv des öffentlichen Rechts (Zeitschrift)
API	application programming interface
Arizona Law Rev.	Arizona Law Review (Zeitschrift)
Art.	Artikel (Singular und Plural)
Az.	Aktenzeichen
BayLDA	Das Bayerische Landesamt für Datenschutz
BayVBL	Bayerische Verwaltungsblätter
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck'scher Online-Kommentar
Begr.	Begründer
Berkeley Tech. L. J.	Berkeley Technology Law Journal (Zeitschrift)
Beschl.	Beschluss
BfDI	Bundesbeauftragte(r) für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
bspw.	beispielsweise
BT-Drs.	Bundestagsdrucksacke
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (amtliche Sammlung)

BVerwG	Bundesverwaltungsgericht
bzw.	beziehungsweise
California L. Rev.	California Law Review (Zeitschrift)
CCZ	Corporate Compliance Zeitschrift (Zeitschrift)
CLSR	Computer Law & Security Review (Zeitschrift)
Colum. Sci. & Tech. L. Rev.	Columbia Science and Technology Law Review (Zeitschrift)
CR	Computer und Recht (Zeitschrift)
CRi	Computer Law Review International (Zeitschrift)
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DSB	Datenschutzberater (Zeitschrift)
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Verkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung)
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)
DSM-RL	Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17.04.2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG (DSM-Richtlinie)
DSRL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr (Datenschutz-Richtlinie)
DuD	Datenschutz und Datensicherheit (Zeitschrift)
Durchsetzungs-RL	Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29.04.2004 zur Durchsetzung der Rechte des geistigen Eigentums (Durchsetzungs-RL)
DVBl	Deutsches Verwaltungsblatt (Zeitschrift)
eCommerce-RL	Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr)
EDPL	European Data Protection Law Review (Zeitschrift)
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragter
ePrivacy-RL	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation
Einf.	Einführung
Einl.	Einleitung
EJLT	European Journal of Law and Technology (Zeitschrift)
EJRR	European Journal of Risk Regulation (Zeitschrift)
EMRK	Europäische Menschenrechtskonvention

Erwg.	Erwägungsgrund
EU	Europäische Union
EuCML	Journal of European Consumer and Market Law (Zeitschrift)
EuGH	Europäischer Gerichtshof für Menschenrechte
EuGRZ	Europäische Grundrechte-Zeitschrift (Zeitschrift)
EuR	Zeitschrift Europarecht (Zeitschrift)
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
f./ff.	folgende Seite/Seiten
FAZ	Frankfurter Allgemeine Zeitung
Fn.	Fußnote/Fußnoten
Fortg. v.	Fortgeführt von
FS	Festschrift
FTC	Federal Trade Commission
G	Gesetz
GA	Goltdammer's Archiv für Strafrecht (Zeitschrift)
Geo. L. Tech. Rev.	Georgetown Law Technology Review (Zeitschrift)
GG	Grundgesetz
grds.	grundsätzlich
GRUR	Gewerblicher Rechtsschutz und Urheberrecht (Zeitschrift)
GRUR-Int.	Gewerblicher Rechtsschutz und Urheberrecht – Internationaler Teil (Zeitschrift)
GRUR-Prax.	Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter und Wettbewerbsrecht (Zeitschrift)
GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht – Rechtsprechungs-Report (Zeitschrift)
h.M	herrschende Meinung
Harv. J. Law Public Policy	Harvard Journal of Law & Public Policy (Zeitschrift)
Harv. J. L. & Tech.	Harvard Journal of Law & Technology (Zeitschrift)
Harv. L. Rev.	Harvard Law Review (Zeitschrift)
Hdb.	Handbuch
Hous. L. Rev.	Houston Law Review (Zeitschrift)
Hrsg.	Herausgeber
Hs.	Halbsatz
i. d. F.	in der Fassung
i. S. d.	im Sinne der/des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ICLQ	International and Comparative Law Quarterly (Zeitschrift)
IDPL	International Data Privacy Law (Zeitschrift)
IMK	Ständige Konferenz der Innenminister und -senatoren der Länder (Innenministerkonferenz)
InfoSoc-RL	Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22.05.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (InfoSoc-Richtlinie)
insb.	insbesondere

Int J Law Info Tech	International Journal of Law and Technology Review (Zeitschrift)
InTeR	Zeitschrift zum Innovations- und Technikrecht (Zeitschrift)
IIC	International Review of Intellectual Property and Competition Law (Zeitschrift)
ITRB	Der IT-Rechts-Berater (Zeitschrift)
J Economics Management Strategy	Journal of Economics & Management Strategy (Zeitschrift)
J. Bus. & Tech. L.	Journal of Business and Technology Law (Zeitschrift)
J. L. Inf. & Sci.	Journal of Law, Information and Science (Zeitschrift)
JA	Juristische Arbeitsblätter (Zeitschrift)
JICES	Journal of Information, Communication and Ethics in Society (Zeitschrift)
jipitec	Journal of Intellectual Property, Information Technology and Electronic Commerce Law (Zeitschrift)
JR	Juristische Rundschau (Zeitschrift)
JURA	Juristische Ausbildung (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	JuristenZeitung (Zeitschrift)
K&R	Kommunikation & Recht (Zeitschrift)
Kap.	Kapitel
KG	Kammergericht
KI	Künstliche Intelligenz
krit.	kritisch
LFD	Landesbeauftragter für Datenschutz
LG	Landgericht
Lit.	Literatur
Ls.	Leitsatz
LSE	London School of Economics and Political Science
m. E.	meines Erachtens
m. w. N.	mit weiteren Nachweisen
Md. L. Rev.	Maryland Law Review (Zeitschrift)
MMR	MultiMedia und Recht (Zeitschrift)
MMR-Beilage	MultiMedia und Recht – Beilage (Zeitschrift)
n. F.	neue Fassung
NBER	National Bureau of Economic Research
NetzDG	Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz)
NJOZ	Neue Juristische Online-Zeitschrift (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	NJW-Rechtsprechungs-Report (Zeitschrift)
Nw. U. L. Rev. Online	Northwestern University Law Review Online (Zeitschrift)
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NvwZ-Extra	Neue Zeitschrift für Verwaltungsrecht – Extra Aufsätze-Online (Zeitschrift)
NZKart	Neue Zeitschrift für Kartellrecht (Zeitschrift)
NZS	Neue Zeitschrift für Sozialrecht (Zeitschrift)
OBA	Online Behavioural Advertising

OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
Pace L. Rev.	Pace Law Review (Zeitschrift)
PET	Privacy Enhancing Technology
PinG	Privacy in Germany – Datenschutz und Compliance (Zeitschrift)
P2B-Verordnung	Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20.06.2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (Plattform-to-Business-Verordnung)
RabelsZ	Rabels Zeitschrift für ausländisches und internationales Privatrecht (Zeitschrift)
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegE	Regierungsentwurf
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
Rspr.	Rechtsprechung
RW	Rechtswissenschaft (Zeitschrift)
S.	Satz, Seite/Seiten
s. o.	siehe oben
s. u.	siehe unten
SDK	Software Development Kit
Seattle U. L. Rev.	Seattle University Law Review (Zeitschrift)
Seton Hall L. Rev.	Seton Hall Law Review (Zeitschrift)
sog.	sogenannte/r/s
st. Rspr.	ständige Rechtsprechung
Stanford Law Rev.	Stanford Law Review (Zeitschrift)
StV	Strafverteidiger (Zeitschrift)
SZ	Süddeutsche Zeitung
TechReg	Technology and Regulation (Zeitschrift)
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u. a.	unter anderem, und andere
U. C. D. L. Rev.	U. C. Davis Law Review (Zeitschrift)
UKlaG	Unterlassungsklagegesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
ULR	Utrecht Law Review (Zeitschrift)
Uni.	Universität
Univ. Pa. Law Rev.	University of Pennsylvania Law Review (Zeitschrift)
UNSW Law Journal	University of New South Wales Law Journal (Zeitschrift)
UrhG	Urhebergesetz
usw.	und so weiter
UVPG	Gesetz über die Umweltverträglichkeitsprüfung
UWG	Gesetz gegen den unlauteren Wettbewerb
v.	vom, von
Verf	Verfasser/in
VerwArch	Verwaltungsarchiv (Zeitschrift)
VG	Verwaltungsgericht

vgl.	vergleiche
VO	Verordnung
VR	Verwaltungsrundschau (Zeitschrift)
VuR	Verbraucher und Recht (Zeitschrift)
vzbv	Verbraucherzentrale Bundesverband e. V.
WI	WIRTSCHAFTSINFORMATIK (Zeitschrift)
WP	Working Paper
WRP	Wettbewerb in Recht und Praxis (Zeitschrift)
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz (Zeitschrift)
ZD-Aktuell	Zeitschrift für Datenschutz – Aktuell (Zeitschrift)
ZEuP	Zeitschrift für Europäisches Privatrecht (Zeitschrift)
ZGE	Zeitschrift für geistiges Eigentum (Zeitschrift)
zit.	zitiert
ZJS	Zeitschrift für das Juristische Studium (Zeitschrift)
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)
ZUM	Zeitschrift für Urheber- und Medienrecht (Zeitschrift)

Einleitung

A. Beschreibung der Thematik

Die Geschwindigkeit der technischen und gesellschaftlichen Entwicklungen im digitalen Bereich ist gewaltig. Technologien ändern sich in zunehmend kürzeren Abständen, werden obsolet und durch neue Standards ersetzt; teils werden die gleichen Technologien morgen bereits anders benutzt als heute und zeigen sich im Laufe ihrer Verwendung Vor- und Nachteile oder Anwendungsbereiche, die bei der Entwicklung gar nicht geplant oder vorherzusehen waren. Das Recht als inhärent statische und träge Materie versucht angesichts dieser Entwicklungen standzuhalten und aufkommende Gefahrenpotentiale normativ einzuhegen, ist aber naturgemäß immer (mindestens) einen Schritt hinterher.[1] Auch das Datenschutzrecht als stark technikbezogene Materie bleibt von diesem grundlegenden Konflikt nicht verschont. Es verfolgt dafür seit jeher die Herangehensweise, die mit regelmäßigen Nachjustierungen und Anpassungen an die veränderten Technologien und Entwicklungen einhergehenden Probleme und Aufwände durch technologieneutrale[2], risikosensible[3] und somit – so die Idealvorstellung – entwicklungsoffene Normen und Pflichten zu umgehen. So verwundert es nicht, dass bis vor wenigen Jahren die aus dem Jahre 1995 stammende und mit der Zeit (zuletzt 2013) nur geringfügig veränderte DSRL das EU-weit wichtigste datenschutzrechtliche Regelwerk war, dessen Grundpfeiler mitunter nochmals einige Jahre älter waren als die Richtlinie selbst.[4] Erst am 27.04.2016

---

[1] *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (320) spricht hier treffend von „unterschiedlichen Innovationszyklen der technisch-ökonomischen und der rechtlichen Entwicklung." Gleichzeitig wird die fortschreitende Technik zunehmend auch zur Unterstützung des Rechts, etwa in der Rechtsdurchsetzung, eingesetzt. Siehe zu dieser Wechselwirkung zwischen Recht und Technik im Bereich des Urheberrechts *Specht*, GRUR 2019, 253 (254 ff.).

[2] Siehe hierzu das in Erwg. 15 S. 1 der DSGVO explizit formulierte Ziel sowie die Ausführungen bei *Roßnagel*, in: Eifert/Hoffmann-Riem, Innovationsfördernde Regulierung, S. 323 (323 ff.); zur Technikneutralität bzw. der technologieneutralen Auslegung des Urheberrechts siehe erneut *Specht*, GRUR 2019, 253 (255 f.).

[3] Hierzu, durchaus kritisch, *Buchner*, DuD 2016, 155 (157 ff.); besonders ausführlich und instruktiv *Gellert*, The risk-based approach to data protection.

[4] Vorbild war hier nicht zuletzt die frühe deutsche Datenschutzgesetzgebung, insbesondere das erste Hessische Datenschutzgesetz von 1970, sowie die 1981 erlassene Datenschutzkonvention Nr. 108 des Europarats. Vgl. *Wolff/Brink*, in: BeckOK Datenschutzrecht, Einleitung

trat mit der DSGVO ein Nachfolgeregelwerk in Kraft, das nach zweijähriger Übergangsperiode am 25.05.2018 wirksam wurde. Die Erwartungen an dieses Monumentalwerk datenschutzrechtlicher Weiterentwicklung waren – und sind bis heute – riesig, und Lobpreisungen als datenschutzrechtlicher „Welt"-[5] oder „Goldstandard"[6] *made* in Europe oder als „Meilenstein"[7] wurden nicht selten bemüht. Dabei atmet auch die DSGVO in ihrem konzeptionellen Kern weiter dieselbe Luft, die schon die Lungen der DSRL füllte.[8] Grundlegende Konzepte wie die in Art. 5 DSGVO verankerten Grundprinzipien, die Ausgestaltung eines prinzipiellen Verbots mit Erlaubnisvorbehalt[9] oder die Voraussetzungen für eine Qualifikation als für eine Verarbeitung Verantwortlicher sind, von wenigen kleinen Veränderungen einmal abgesehen, identisch geblieben. Weiterentwicklungen fanden punktuell statt, von einer tiefgehenden Modernisierung oder gar Revolution des Datenschutzes kann jedoch keine Rede sein. Eine Regulierung konkreter Phänomene und Herausforderungen findet – ganz im Geiste des technologieneutralen Ansatzes – weiterhin nicht statt.

Gleichzeitig ist die Anzahl aktueller Entwicklungen und Gefahrenpotentiale heutzutage größer denn je zuvor. Es stellen sich etwa Fragen hinsichtlich der Legitimität des Einsatzes von selbstlernenden Algorithmen und Systemen (häufig unter dem Stichwort KI) in vielfältigen, staatlichen wie privaten, Anwendungsszenarien,[10] hinsichtlich des Betriebs von Big Data-Anwendun-

---

zur DS-GVO Rn. 8 f.; zur Entwicklungsgeschichte der DSRL siehe auch *Simitis*, NJW 1997, 281 (281 f.); auch international überwiegen größtenteils noch Datenschutzgesetze, die zu einer anderen Ära erlassen wurden. Vgl. *Westerlund/Enkvist*, jipitec 2016, 2: „Yet, across the world, privacy laws […] may have been devised during a time when the Internet was predominantly used in research and academia."

[5] Siehe etwa *Albrecht*, EuZW 2018, 433; zur Stellung der DSGVO im internationalen Wettbewerb der Datenschutzrechtsordnungen siehe *Hennemann*, RabelsZ 2020, 865 (870 ff.).

[6] So die EU-Kommisarin *Věra Jourová* im Interview mit dem Handelsblatt vom 11.07.2018 (https://www.handelsblatt.com/unternehmen/it-medien/eu-kommissarin-vra-jourov-im-interview-die-datenschutz-grundverordnung-ist-auf-gutem-weg-weltweit-zum-goldstandard-zu-werden/22781340.html). Zuletzt abgerufen am 14.01.2022.

[7] So die Bundesdatenschutzbeauftragte *Andrea Voßhoff*, zit. von heise online am 21.04.2016, Datenschützer bewerten EU-Grundverordnung als „Meilenstein" (https://www.heise.de/newsticker/meldung/Datenschuetzer-bewerten-EU-Grundverordnung-als-Meilenstein-3179872.html). Zuletzt abgerufen am 14.01.2022.

[8] Vgl. *Selmayr/Ehmann*, in: Ehmann/Selmayr, DSGVO, Einführung Rn. 61: „[…] bekräftigt die DS-GVO die wesentlichen Grundsätze des europäischen Datenschutzrechts." Ähnlich *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (13): „[…] zeigt indessen, dass inhaltlich keinesfalls alles völlig neu ist […]." Ebenso zur Ausgestaltung der datenschutzrechtlichen Verantwortlichkeit *Marosi*, K&R 2016, 389 (389).

[9] Wobei hier mit *Roßnagel*, NJW 2019, 1 (5) richtigerweise präzisiert werden muss, dass ein *echtes* Verbot mit Erlaubnisvorbehalt aufgrund der umfangreichen Ausnahmetatbestände und des Verzichts auf eine behördenseitliche Erlaubnis (etwa in Form einer Genehmigung) gar nicht vorliegt; a. A. *Veil*, NVwZ 2018, 686 (688 ff.).

[10] Vgl. hierzu etwa *Pasquale*, The black box society; *Hildebrandt*, Smart technologies and the end(s) of law; *Wischmeyer*, AöR 2018, 2 (2 ff.).

gen,[11] der spezifischen Gefahren zunehmend smarter Gegenstände[12] bzw. des Internet of Things[13] oder der Nutzung besonders sensibler, z. B. biometrischer oder Mobilitätsdaten.[14] Ob das Festhalten der DSGVO an ihrem technikneutralen[15] *one size fits all*-Konzept[16] der Regulierung solcher Technologien und Verarbeitungsszenarien unter diesen Umständen noch zeitgemäß ist, wird heiß debattiert.[17]

---

[11] Siehe hierzu etwa *Kuner* u. a., IDPL 2012, 47 (47f); zur möglichen Unvereinbarkeit von Big Data mit dem Ideal informierter Einwilligungen instruktiv *Cate/Mayer-Schönberger*, IDPL 2013, 67 (67 ff.); zum Konflikt mit dem Prinzip der Zweckbindung *Helbing*, K&R 2015, 145 (145 ff.); zu den Datenschutzprinzipien insgesamt *Hornung*, in: Hoffmann-Riem, Big Data: regulative Herausforderungen, S. 79 (81 ff.); einen guten Überblick zur Thematik gibt auch *Zarsky*, Seton Hall L. Rev. 2017, 995 (995 ff.).

[12] Ein aktuelles Thema hier ist etwa die Übertragung von Fahrtdaten des Autoherstellers *Tesla*, siehe *Joe Sperling*, Wenn der Tesla seinen Fahrer verpfeift, zdf.de vom 24.08.2021 (https://www.zdf.de/nachrichten/wirtschaft/tesla-videoueberwachung-dashcam-daten schutz-100.html). Zuletzt abgerufen am 14.01.2022.

[13] Siehe etwa zu Sportuhren und Fitnesstrackern *Dregelies*, VuR 2017, 256 (256 ff.); aufschlussreich zur Ubiqiuität alltäglicher Datenverarbeitungen *Roßnagel*, Datenschutz in einem informatisierten Alltag; ebenso *Roßnagel* u. a., Datenschutzrecht 2016 – „Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts; genereller zu Datenschutz bei dauerhaft stattfindenden Datenverarbeitungen *Feldman/Haber*, Berkeley Tech. L. J. 2020, 197 (216 ff.); *Matzner*, JICES 2014, 93 (93 ff.); *Lindqvist*, Int J Law Info Tech 2018, 45 (45 ff.).

[14] Siehe etwa zu den Gefahren biometrischer Videoüberwachung *Jandt*, ZRP 2018, 16 (16 ff.); generell zu sensiblen Daten *Weichert*, DuD 2017, 538 (538 ff.); zur Bedeutung von Standortdaten *Martin/Nissenbaum*, Berkeley Tech. L. J. 2020, 253 (258 ff.).

[15] Kritisch zur konkreten Ausgestaltung dieses Ideals in der DSGVO *Roßnagel*, MMR 2020, 222 (227): „In der DS-GVO wird diese Technikneutralität jedoch so überzogen, dass sie eine Risikoneutralität bewirkt: In keiner Regelung werden die spezifischen Grundrechtsrisiken zum Beispiel von smarten Informationstechniken im Alltag, von Big Data […] angesprochen oder gar gelöst."

[16] Hierunter verstanden wird der Ansatz, öffentliche wie nicht-öffentliche Stellen gleichermaßen zu regulieren und den Unterschieden zwischen kleinen und großen, privaten und kommerziellen Verarbeitern nicht durch jeweils eigene Pflichten, sondern nur durch eine ggf. angepasste Reichweite der Pflichten Rechnung zu tragen. Zur Tendenz einer solchen Ansatzes, große Unternehmen bei ihren Compliance-Bemühungen zu begünstigen *Evan Engstrom & Daphne Keller*, Only giant internet firms may be able to comply with one-size-fits-all rules, San Francisco Chronicle vom 11.05.2018 (https://www.sfchronicle.com/opinion/openforum/article/Only-giant-internet-firms-may-be-able-to-comply-12905469.php). Zuletzt abgerufen am 14.01.2022.

[17] Besonders kritisch hierzu, insbesondere mit Verweis auf die Belastung für kleinere Datenverarbeiter *Veil*, NVwZ 2018, 686 (692 ff.); optimistischer dagegen zum grundsätzlichen Konzept der Technikneutralität, nicht aber zu seiner Umsetzung in der DSGVO *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (329 f.): „Rechtliche Regeln müssen nicht auf jede technische Änderung reagieren, wenn und weil sie sich auf Anforderungen an technische Funktionalitäten beziehen, die durch unterschiedliche technische Designs erfüllt werden können. […] In der aktuellen Datenschutz-Grundverordnung werden jedoch auch keine technischen Funktionalitäten geregelt." Vgl. weiter *Marosi*, K&R 2016, 389 (389); zudem m. w. N. *Hennemann*, RabelsZ 2020, 865 (871).

Unabhängig von diesen punktuellen Fragen des Umgangs mit konkreten Verarbeitungsphänomenen zeichnet sich ein grundsätzlicher, auf einer tieferen Ebene liegender Konflikt ab. Werden im digitalen Raum Dienste angeboten, Inhalte angezeigt und Daten übermittelt, so ist dort immer häufiger eine immer größer werdende Gruppe an Akteuren beteiligt.[18] Gleiches gilt für die Verarbeitung personenbezogener Daten, ohne die kein digitaler Dienst mehr auskommt. Durch die damit einhergehende Verteilung arbeitsteiliger Beiträge, Einfluss- und Kontrollsphären sowie Ziele und Eigenmotivationen unter und zwischen den einzelnen Akteuren bildet sich eine komplexe Gemengelage, die mitunter – nicht nur für das betroffene Individuum – schwer zu durchschauen und noch schwerer zu vermeiden ist.[19] Gleichzeitig ist das Konzept der datenschutzrechtlichen Verantwortlichkeit, das bestimmt, welche Akteure bei der Verarbeitung personenbezogener Daten dafür verantwortlich sind, dass die Voraussetzungen für eine datenschutzkonforme Verarbeitung eingehalten werden, seit den Zeiten der DSRL unverändert. Ziel dieser Verantwortlichkeit ist es, diejenigen Akteure zu identifizieren und in die Pflicht zu nehmen, die den entscheidenden Einfluss auf die essenziellen Verarbeitungsumstände – die *Zwecke* und *Mittel* der Verarbeitung[20] – ausüben. Dabei hängt das Konzept, mit wenigen Ausnahmen, dem klassischen Gedanken nach, dass in der Regel *ein* Akteur diesen Einfluss vollständig in seiner Person vereint.[21] Ob dies im Angesicht der zunehmenden Pluralität der an einer Verarbeitung beteiligten Akteure und der Komplexität der zwischen ihnen vorherrschenden Verhältnisse noch als zeitgemäß angesehen werden kann, ist mehr als zweifelhaft.

Schon 2005 konstatierte *Roßnagel*: „Hinsichtlich der Regelungsadressaten ist die zunehmende Verantwortungsdiffusion zur Kenntnis zu nehmen."[22] Auch der EuGH erkannte in den vergangenen Jahren mehrfach die Notwendigkeit, die Verantwortlichkeit auf solche Akteure zu erweitern, die bis dahin nicht im Verdacht gestanden hatten, eine solche Rolle einzunehmen. In seiner Google

[18] Vgl. *Gürses/van Hoboken*, in: Selinger/Polonetsky/Tene, The Cambridge Handbook of Consumer Privacy, S. 579 (586): „The agile turn comes with an increase in modularity in software as a service environment."

[19] So zeigen etwa Studien, dass es nahezu keinen Unterschied zwischen kostenlosen und bezahlten Smartphone-Apps hinsichtlich der Anzahl einbezogener Drittparteien und an diese übermittelter Daten gibt, während ein solcher Unterschied gleichzeitig von großen Teilen der zahlenden Nutzer erhofft bzw. erwartet wird. Vgl. *Bamberger* u. a., Berkeley Tech. L. J. 2020, 327 (364); *Han* u. a., Proceedings on Privacy Enhancing Technologies 2020, 222.

[20] Vgl. Art. 4 Nr. 7 DSGVO.

[21] Siehe *van Alsenoy*, jipitec 2016, 271 (272 ff.) für eine Bestandsaufnahme der wenigen Änderungen zwischen DSRL und DSGVO.

[22] *Roßnagel*, MMR 2005, 71 (74); in dieselbe Richtung gehend *Gürses/van Hoboken*, in: Selinger/Polonetsky/Tene, The Cambridge Handbook of Consumer Privacy, S. 579 (590): „The modularization of services raises the question of who exactly is and should be responsible to ensure privacy as a matter of policy, law and principle. In the hyperconnected service environments that have emerged over the last decades, this question is nontrivial to answer, and policy makers continue to struggle to find the right answer."

Spain-Entscheidung betraf das zunächst Google in der Rolle als Suchmaschinenbetreiber, der Nutzern andere, personenbezogene Daten verarbeitende Artikel und sonstige Inhalte auffindbar macht und vermittelt.[23] In den noch jüngeren Wirtschaftsakademie- und Fashion ID-Entscheidungen[24] betraf die Erweiterung der Verantwortlichkeit sodann einzelne Betreiber von Websites und sog. Fanpages, die die von Facebook angebotene Infrastruktur und einzelne Bestandteile dieser nutzten und es Facebook dadurch ermöglichten, Daten mit Bezug zu den Besuchern der jeweiligen Websites und Fanpages zu erheben. Anhand dieser Urteile und der sie begleitenden (teils sehr kritischen) Auseinandersetzung im juristischen Schrifttum wie auch in der Praxis lässt sich erahnen, welche ungelösten Konflikte hier noch schlummern.

Ziel dieser Arbeit soll es sein, beide Seiten dieser Konfliktlinie – moderne Verarbeitungsrealität auf der einen und klassisch tradiertes Verantwortlichkeitsmodell auf der anderen Seite – zu beleuchten und analysieren und unter Berücksichtigung der vom EuGH eingeschlagenen Pfade eigene Vorschläge für eine Weiterentwicklung zu unterbreiten, um beide Seiten wieder stärker in Einklang zu bringen.

B. Methodische Herangehensweise

Eine solche Annäherung, Analyse und Fortentwicklung setzt – sowohl in Hinblick auf die Vielschichtigkeit des Datenschutzrechts als auch aufgrund der Komplexität des digitalen Raumes als zu regelnde Materie – methodisch verschiedene Ansätze voraus. Notwendig ist zwangsläufig ein geweiteter Blick, der sich von der Fixierung auf die unmittelbar beteiligten Akteure und ihre Einflussnahmen löst und das gesamte Ökosystem einschließt, in das sie eingebettet sind. Dazu gehören neben der Gesamtheit der beteiligten Akteure auch die Art und Weise ihrer Zusammenarbeit und die technische Ausgestaltung der Infrastruktur, in der sie sich bewegen und die ihr Handeln bedingt, aber auch die Eigenmotivationen und Handlungslogiken der einzelnen Akteure. Vor diesem Hintergrund wagt die Arbeit einen Blick über den juristischen Tellerrand, um Erkenntnisse aus der (Wirtschafts-)Informatik einfließen zu lassen, die Aufschluss über dieses Zusammenspiel und die Dynamik seiner einzelnen Komponenten gibt. Hierbei kommen dem Verfasser zahlreiche Einblicke aus der Arbeit in einem interdisziplinären Forschungsprojekt gemeinsam mit Informatiker*innen verschiedenster Fachrichtungen und Technikphilosoph*innen zugute.

---

[23] EuGH Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317.

[24] EuGH Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388; Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629.

Um eine seriöse Beurteilung dahingehend vorzunehmen, wie wirksam das Datenschutzrecht und sein tradiertes Verantwortlichkeitskonzept auf die veränderte Verarbeitungsrealität reagieren kann, bedarf es zudem einer grundlegenden Analyse dieses Konzepts und seiner Zielrichtung und (offen formulierten oder impliziten) Wirksamkeitsvoraussetzungen. Hier betrachtet die Arbeit das derzeit wichtigste europäische Regelwerk des Datenschutzes, die DSGVO, im Lichte ihrer unionsgrundrechtlichen Wurzeln und teilweisen Vorstrukturierung ebenso wie ihrer einzelnen Regulierungsinstrumente, um so die zugrundeliegenden Grundprämissen hinsichtlich ihrer erwarteten Wirksamkeit aufzudecken.

Die Linse, durch die diese Betrachtung stattfindet, ist einerseits die der klassischen Rechtsauslegung[25] und grundrechts- bzw. primärrechtsdogmatischen Analyse des einfachen bzw. Sekundärrechts: Welchen Inhalt und welche Bedeutung hat die DSGVO und haben ihre einzelnen Normen mit Blick auf die eigene Zielsetzung sowie die Unionsgrundrechte, deren Durchsetzung sie dienen. Andererseits ist es die Linse der Governance[26] und regulatorischen Rechtsdogmatik: Nicht (nur) die Ermittlung dessen, was eine Norm oder ein Gesetz auf Basis einer bestimmten Auslegungsmethode anordnet, sondern auch, welche Wirkungen damit im Einzelnen bezweckt, welche Verhaltensweisen bei den betroffenen Normunterworfenen hervorgerufen werden sollen, sowie die Frage, ob diese Wirkungen tatsächlich erreicht werden, steht hier ebenso im Mittelpunkt, wie die Frage, welche Rolle dabei klassische wie moderne Regulierungs- und Steuerungsinstrumente spielen können.[27] Vereinzelt wird bei der Betrachtung der Wirkungen und Folgen einzelner Instrumente auch auf die ökonomische Analyse des Rechts zurückgegriffen.[28]

Da speziell die regulatorische Dogmatik zusätzliche Erkenntnisse über die geregelte Materie und ihre Eigengesetzlichkeiten benötigt, um Aussagen über die aktuelle, aber auch die hypothetische Wirkweise und Wirksamkeit alternativer Normen treffen zu können, ist eine disziplinübergreifende Perspektive hier unabdingbar.[29] Denn nur die die jeweilige Materie betreffenden Disziplinen

---

[25] Vgl. *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, S. 25, 133 ff.

[26] Grundlegend hierzu *Schuppert*, Die Verwaltung 2007, 463 (464 ff.).

[27] Siehe hierzu für das Privatrecht *Hellgardt*, AcP 2016, 349 (350): „Eine regulatorisch erweiterte Rechtsdogmatik stellt die Frage, welche tatsächlichen Wirkungen eintreten würden, wenn eine Rechtsnorm einen bestimmten Inhalt hätte, um entscheiden zu können, ob sie einen solchen oder einen alternativen Inhalt haben soll." Zu den verschiedenen Arten öffentlich-rechtlicher Regulierung unter Einbezug staatlicher und privater Akteure siehe *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, S. 261 (300 ff.); siehe außerdem *Schuppert*, Wissen, Governance, Recht., S. 64 ff. m. w. N.

[28] Grundlegend hierzu *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts; *Eidenmüller*, Effizienz als Rechtsprinzip, S. 393 ff., 414 ff.

[29] Zur Bedeutung disziplinübergreifender Erkenntnisse am Beispiel der mittelbaren Verantwortlichkeit siehe *Hofmann*, JZ 2018, 746 (751 ff.).

können „mit hinreichender Sicherheit Aussagen darüber machen, wie sich die vorzuschlagende Regelung in den verschiedenen Bereichen der sozialen Realität auswirken wird, welche Alternativen von dem Sachbereich her überhaupt bestehen, welche Mittel in Frage kommen, welche Vorteile, welche Nachteile zu erwarten sind."[30] Die Arbeit greift daher auf interdisziplinäre Erkenntnisse aus dem Bereich der Wirtschaftsinformatik, namentlich die Methode der *boundary resources*,[31] zurück, und versucht, die dort vorgefundenen Konzepte, Rollenmodelle und Systematiken im Zusammenhang mit digitalen Plattformen in die Dogmatik des Datenschutzrechts zu überführen und so insgesamt für die Rechtswissenschaft fruchtbar zu machen.

Aufbauend auf diesen methodischen Herangehensweisen zeigt die Arbeit dann auf, wo und inwieweit der Abgleich zwischen der heutigen Verarbeitungsrealität und dem datenschutzrechtlichen Verantwortlichkeitskonzept Defizite zutage fördert, und macht konkrete Regelungsvorschläge für eine mögliche Ausweitung der Verantwortlichkeit, die diesen Defiziten entgegenwirken könnte.

C. Aktueller Stand in Forschung und Rechtsprechung

Die Menge an Akteuren, die an Datenverarbeitungen im digitalen Raum regelmäßig beteiligt sind, sowie das Ausmaß an Komplexität, das daraus für von der Verarbeitung betroffene oder zur Überwachung und Durchsetzung der Rechtsnormen beauftragte Akteure einhergeht, wurde in der Forschung bisher nur teilweise und in einem begrenzten Spektrum behandelt.

Grundsätzlich ist das arbeitsteilige Zusammenwirken verschiedener an einer Verarbeitung beteiligter Akteure dem Datenschutzrecht nicht fremd. Wo es um die heutzutage ubiquitäre Auslagerung einzelner Verarbeitungen und Verarbeitungsabschnitte an einen weisungsgebundenen Akteur mit besserem Sachverstand geht, ist es unter dem Stichwort *cloud computing* bereits sehr bekannt und im Zusammenhang mit der Figur des Auftragsverarbeiters (im deutschen Recht ehemals Auftragsdatenverarbeiter) gem. Art. 28 DSGVO auch gesetzlich verankert und ausgestaltet. Sowohl dem Phänomen *cloud computing*[32] als

[30] *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, S. 16.

[31] Vgl. *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (176 ff.); *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 4 ff.

[32] Siehe hier stellvertretend für viele *Jotzo*, Der Schutz personenbezogener Daten in der Cloud; *Barnitzke*, Rechtliche Rahmenbedingungen des Cloud Computing; *Busching*, Der Schutz „privater" Informationen bei Cloud Computing; *Hennrich*, Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz; *Kian*, Cloud Computing; *Schmid*, Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen; *Selzer*, Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit.

auch der Figur des Auftragsverarbeiters[33] wurde in der Forschung breitflächige Aufmerksamkeit zuteil. Auch diese Figur hängt aber dem klassischen Konzept eines zentralen Akteurs, der die Fäden der Verarbeitung vollkommen in seinen Händen hält, nach. Wo der Beauftragte die ihm überlassenen Daten auch für eigene Zwecke verarbeitet, findet die Figur ihre Grenze. Wo diese Grenze erreicht ist, ist der Konsens meist ein Verweis auf die, in Art. 28 Abs. 10 DSGVO explizit angeordnete, eigenständige Verantwortlichkeit des mit Eigenmacht oder im Exzess handelnden Auftragsverarbeiters[34] – eine systematische Behandlung der Adäquanz dieser Reaktion auf die Gefahrenpotentiale dort, wo eine solche Überschreitung stattfindet, ist hingegen die Ausnahme.[35]

Insbesondere im US-amerikanischen Raum wurde zudem bereits in den Nullerjahren erörtert, inwieweit die sog. *first generation* Datenschutzgesetze und Regulierungsbemühungen durch die im Web 2.0. bzw. durch das *generative* Internet[36] gegebenen Möglichkeiten der Mitgestaltung und Weiterverwendung von personenbezogene Daten inkludierenden Inhalten durch Privatpersonen und Nutzer an ihre Grenzen gelangt sein könnten.[37] Dabei lag der Fokus, ebenso wie auch in neuerer Zeit im Zusammenhang mit Datenverarbeitungen auf sozialen Netzwerken teils diskutiert,[38] auf unkoordinierten und gerade von Privatpersonen ausgehenden Datenverarbeitungen und Beteiligungen und den daraus resultierenden Gefahren:

„The heart of the next generation privacy problem arises from the similar but uncoordinated actions of individuals that can be combined in new ways thanks to the generative Net. Indeed, the Net puts private individuals in a position to do more to compromise privacy than the government and commercial institutions traditionally targeted for scrutiny and regulation."[39]

Diese Überlegungen bezogen sich jedoch noch größtenteils auf klassische Gefährdungsszenarien in Form von Veröffentlichungen privater Sachverhalte.[40] Der ihnen zugrundeliegende Betrachtungswinkel auf die unkoordinierten Ak-

---

[33] Siehe insbesondere unter dem Rechtsrahmen der DSGVO *Eckhardt*, CCZ 2017, 111 (111 ff.); *Petri*, ZD 2015, 305 (305 ff.); *von Holleben/Knaut*, CR 2017, 299 (299 ff.); *Schmitz/von Dall'Armi*, ZD 2016, 427 (427 ff.).

[34] Hierzu etwa *Jotzo*, Der Schutz personenbezogener Daten in der Cloud, S. 70 ff.; vgl. auch *Klug*, in: Gola, DSGVO, Art. 28 Rn. 19.

[35] Siehe hierzu etwa *Hon* u. a., IDPL 2012, 3 (3 ff.); *Kroschwald*, ZD 2013, 388 (388 ff.); *Maisch*, Informationelle Selbstbestimmung in Netzwerken; *Müller*, Cloud Computing.

[36] Vgl. *Zittrain*, Harv. L. Rev. 2006, 1974.

[37] Siehe etwa *Zittrain*, The University of Chicago Legal Forum 2008, 65 (65 ff.); auf diesen bezugnehmend *Burdon*, University of Illinois Journal of Law, Technology and Policy 2010, 1 (1 ff.).

[38] Siehe hierzu etwa *Golland*, ZD 2020, 397 (397 ff.); *Chmelik*, Social Network Sites – Soziale Netzwerke; *Wong*, Birkbeck Law Review 2014, 317 (317 ff.).

[39] *Zittrain*, The University of Chicago Legal Forum 2008, 65 (65).

[40] Siehe hierzu beispielhaft die bei *Burdon*, University of Illinois Journal of Law, Technology and Policy 2010, 1 (10 ff.) ausgeführten Szenarien.

tionen der einzelnen Individuen unterscheidet sich zudem stark von dem hier gewählten Blick auf das jedenfalls zu weiten Teilen koordiniert und arbeitsteilig ablaufende Zusammenspiel mehrerer Akteure.

Eine darüber hinausgehende Auseinandersetzung mit der Problematik der verschiedenen Beiträge, die unterschiedliche Akteure in jedenfalls dem Grunde nach koordinierter Form zu Datenverarbeitungen leisten, wurde mit der bereits erwähnten jüngeren EuGH-Rechtsprechung eingeleitet, die mit Google Spain ihren Anfang nahm und mit Wirtschaftsakademie und Fashion ID noch an Fahrt gewann. Ausgangspunkt ist hier die schon in der DSRL angelegte Figur der gemeinsamen Verantwortlichkeit, die in der DSGVO in Art. 4 Nr. 7 als Teil der Verantwortlichkeit definiert und in Art. 26 hinsichtlich ihrer Rechtsfolgen teilweise ausgeformt wird.[41] Infolge insbesondere der beiden letztgenannten, im Jahre 2018 respektive 2019 ergangenen Urteile, wurde, im deutschsprachigen Umfeld aufgrund der in beiden Fällen durch deutsche Gerichte vorgenommenen Vorlagen an den Gerichtshof teils bereits einige Jahre früher,[42] eine breite Diskussion hinsichtlich der Frage angestoßen, inwieweit die vom EuGH vorgenommene Ausweitung der Verantwortlichkeit als zielführend angesehen werden kann und sollte.[43] Im Zentrum dieser Diskussion stehen die befürchtete Gefahr einer ausufernden Verantwortlichkeit auf private und meist machtlose Akteure[44] sowie die mit einer bisher fehlenden Konturierung der Qualifikationsmerkmale einhergehende Unsicherheit darüber, wer alles als Verantwortlicher in Betracht kommt[45]. Was jedoch auch dieser Diskussion bisher in weiten Teilen fehlt, ist eine tiefergehende systematische Auseinandersetzung mit der *Notwendigkeit* einer solchen Ausweitung einerseits und den breiteren Implikationen der grundlegenden Problematik auch in anderen Akteurskonstellationen. Während sich hier die Notwendigkeit meist in der vom EuGH bemühten und selten weiter hinterfragten Floskel der Gewährleistung eines „wirksamen und

[41] Einen Überblick über die einzelnen Pflichten, die sich für gemeinsame Verantwortliche aus Art. 26 ergeben, verschaffen *Specht-Riemenschneider/Schneider*, MMR 2019, 503 (505 ff.).

[42] Die der Wirtschaftsakademie-Entscheidung zugrundeliegende Anordnung der zuständigen Aufsichtsbehörde zur Deaktivierung der Fanpage erging bereits am 03.11.2011, das erste Urteil des VG Schleswig wurde am 09.10.2013 erlassen. Diskussionen über denkbare Konstellationen der gemeinsamen Verantwortlichkeit begannen – jedenfalls im deutschsprachigen Schrifttum – bereits zu diesem Zeitpunkt. Siehe hierzu ausführlich *infra* in Kapitel 2 C. II. Vgl. stellvertretend für einige der dort zitierten Stimmen *Voigt/Alich*, NJW 2011, 3541 (3541 ff.); *Piltz*, CR 2011, 657 (657 ff.).

[43] Siehe auch hierzu *infra* in Kapitel 2 C. II. sowie stellvertretend für viele *Lindroos-Hovinheimo*, Information & Communications Technology Law 2019, 225 (225 ff.); *Petri*, EuZW 2018, 534 (540).

[44] Den Fokus hierauf legend *Edwards* u. a., Data subjects as data controllers; *Schulz*, ZD 2018, 357.

[45] Hierzu stellvertretend für die ebenfalls in Kapitel 2 C II. ausführlich behandelte Literatur *Paun*, EuCML 2020, 35 (37); *Marosi/Matthé*, ZD 2018, 357 (363); *Blanc*, EDPL 2018, 120 (124).

umfassenden Schutz[es] der betroffenen Personen“[46] erschöpft, wird die Übertragbarkeit auf andere Akteurskonstellationen bisher nahezu ausschließlich aus dem Gedanken der Sorge um unzumutbar belastete Akteure betrachtet, während es an einer konstruktiven und über die Fälle hinausgehenden Perspektive auf die weiteren Möglichkeiten extensiver Verantwortlichkeitsbeschreibung fehlt. In beiderlei Hinsicht besteht hier noch Bedarf an einer weiteren Behandlung der Thematik, die über reine Auslegungsfragen hinausgeht und sich auch der Ebene der Rechtsgestaltung widmet.

D. Gang der Untersuchung

Die vorliegende Arbeit unterteilt sich im Anschluss an diese Einleitung in vier Kapitel. In Kapitel 1 wird zunächst deskriptiv und unter Heranziehung von Erkenntnissen und Methoden aus Informatik und Wirtschaftsinformatik die heutzutage vorherrschende Akteurspluralität im digitalen Raum beleuchtet und werden die dabei typischerweise vorkommenden Akteure gruppiert und hinsichtlich ihrer Kontroll- und Einflusssphären im Zusammenhang mit der Verarbeitung personenbezogener Daten analysiert und systematisiert. Kapitel 2 widmet sich ausführlich der datenschutzrechtlichen Verantwortlichkeit in seiner Funktion als Herzstück des Regelungskonzepts der DSGVO. Dabei wird mit den unionsgrundrechtlichen Wurzeln des sekundärrechtlichen Datenschutzes begonnen und werden die Funktionen, Instrumente und Prämissen der Verantwortlichkeit Schritt für Schritt aufgedeckt. Zum Abschluss des Kapitels werden die Voraussetzungen der Verantwortlichkeit unter Berücksichtigung der aktuellen EuGH-Rechtsprechung analysiert und interpretiert sowie einer kritischen Beurteilung zugeführt. In Kapitel 3 werden die Erkenntnisse der ersten beiden Kapitel zusammengeführt, um die Frage nach möglichen Defiziten des tradierten Verantwortlichkeitskonzepts zu beantworten und Vorschläge für mögliche Weiterentwicklungsansätze zur teilweisen Behebung dieser Defizite zu unterbreiten. Den Abschluss der Arbeit bildet mit Kapitel 4 ein Resümee der gewonnenen Erkenntnisse und ein Ausblick auf die mögliche Zukunft der Verantwortlichkeit.

E. Begriffserläuterungen

Abschließend werden an dieser Stelle einige der zentralen Begriffe, die in dieser Arbeit verwendet werden, kurz erläutert und in ihrer hier verwendeten Bedeutung umschrieben. Dies erscheint insbesondere deshalb wichtig, weil einige

[46] Diese Formulierung hatte in EuGH Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317 Rn. 34 ihren Ursprung und wurde seither neben den bereits erwähnten Urteilen zur gemeinsamen Verantwortlichkeit unter anderem auch in Rs. C-25/17 (Jehovan todistajat), ECLI:EU:C:2018:551 Rn. 66 bemüht.

der Begriffe in unterschiedlichen Verwendungskontexten unterschiedliche, teils feststehende, Bedeutungen haben können. Auch werden innerhalb dieser Arbeit an verschiedenen Stellen und in verschiedenen Kontexten dieselben Begriffe teils unterschiedlich verwendet.

Das private Datenschutzrecht dient nach dem hier zugrunde gelegten Verständnis der *Regulierung*[47] der Verarbeitung personenbezogener Daten[48] und der Verarbeitungsfolgen durch die *Steuerung*[49] des Verhaltens der datenschutzrechtlichen Verantwortlichen und anderer Akteure[50] zum Zwecke des *Schutzes* betroffener Personen[51] vor den verschiedenartigen *Gefährdungen*, die sich im Zusammenhang mit der Verarbeitung der sie betreffenden Daten – teils unmittelbar, teils mit Verzögerung – ergeben können. Dabei stellen die Normen des privaten Datenschutzrechts und ihre Anwendung stets das Ergebnis eines Ausgleichs zwischen den Grundrechten des Betroffenen und denen des Verantwortlichen dar, der durch die Bedingungen, die an Datenverarbeitungen gestellt werden, in seiner grundrechtlich geschützten (insbesondere Berufs-)Freiheit eingeschränkt wird. Es ist daher, wenn es um das im Rahmen der DSGVO zum Tragen kommende Konzept des Datenschutzrechts geht, in dieser Arbeit meist vom *Schutz-*, *Regulierungs-* oder *Regelungskonzept* die Rede,[52] während jeder

---

[47] Im Rahmen dieser Arbeit mit *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts Band I: Methoden, Maßstäbe, Aufgaben, Organisation, S. 1319 (1323) sehr weit verstanden als „jede gewollte staatliche Beeinflussung gesellschaftlicher Prozesse […], die einen spezifischen, aber über den Einzelfall hinausgehenden Ordnungszweck verfolgt und dabei im Recht zentrales Medium und Grenze findet." Unter diesen Begriff bzw. dieses Begriffsverständnis fällt dabei nicht nur das öffentlich-rechtliche, sondern grundsätzlich ebenso das Privatrecht, vgl. *Hellgardt*, Regulierung und Privatrecht, S. 7 ff.

[48] In diese Richtung gehend auch *Krönke*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 1 (4): „Und in der Tat zeigt gerade das Datenschutzrecht inzwischen auch deutliche, wenn auch ausbaufähige Züge eines modernen Wirtschaftsverwaltungsrechts. Mit ihnen reagiert der Gesetzgeber auf die datenschutzrechtliche Verantwortlichkeit auch privater Wirtschaftssubjekte der digitalen Wirtschaft, deren Geschäftsmodelle vielfach auf der exzessiven Verarbeitung personenbezogener Informationen beruhen, und die damit verbundene Vervielfältigung der Regulierungsadressaten."

[49] Zur zunehmenden Tendenz zur Verhaltenssteuerung im Wirtschaftsverwaltungsrecht insgesamt siehe *Fehling*, JZ 2016, 540 (544 f.); grundlegend zu den Möglichkeiten und Vorzügen der Verhaltenssteuerung mittels Ordnungsrecht *Baehr*, Verhaltenssteuerung durch Ordnungsrecht, S. 25 ff., 73 ff.; zum Einsatz von Steuerungsinstrumenten als legislative Reaktion auf Risiken *Schwabenbauer*, in: Dalibor/Fröhlich/Rodi/Schächterle/Scharrer, Risiko im Recht – Recht im Risiko: 50. Assistententagung Öffentliches Recht, Greifswald 2010, S. 157 (164 ff.).

[50] Vgl. etwa *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (25): „Dem neuen Datenschutzrecht liegen vielmehr allgemeine, auch rechtspsychologische Überlegungen darüber zugrunde, wie man mit Recht Verhalten steuern kann." Siehe zu den erhofften Steuerungswirkungen und den Anknüpfungspunkten der Steuerung die Ausführungen in Kapitel 2 B. I. 2. und 3.

[51] Siehe hierzu die Ausführungen zum Regelungszweck in Kapitel 2 A. III.

[52] Siehe hierzu zusammenfassend in Kapitel 2 B. I. 4.

dieser Begriffe auf das eben geschilderte Verständnis verweist. Hinsichtlich der einzelnen, meist den Verantwortlichen betreffenden, *Instrumente* innerhalb der DSGVO ist von *Steuerungsinstrumenten* die Rede.[53]

Bzgl. der *Gefährdungen* und *Gefahren*, vor denen Betroffene geschützt werden sollen, werden in dieser Arbeit auch die Begriffe der *Risiko-* und *Gefahrenvorsorge* verwendet; gemeint sind damit mögliche, bisher nicht abschätzbare zukünftige Gefährdungen noch ungewisser Eintrittswahrscheinlichkeit und Konkretisierung durch die kontextbezogene Weiterverarbeitung von Daten und Verwendung von Informationen sowie die darauf basierenden Entscheidungen, die *Schäden* und andere Auswirkungen für die betroffenen Personen und ihre Rechtsgüter zeitigen (können), und denen vorgesorgt werden soll. Da das Datenschutzrecht hier an die Verarbeitung personenbezogener Daten anknüpft und deren Rechtskonformität an bestimmte Bedingungen knüpft, ist zudem in manchen Teilen der Arbeit von der grundsätzlichen (sehr diffusen) *Gefährlichkeit* die Rede, die die DSGVO Datenverarbeitungen zuschreibt.[54]

Abzugrenzen davon ist der *Risiko*[55]-Begriff der DSGVO, der – regelmäßig im Zusammenhang mit den Pflichten des Verantwortlichen – nach klassisch polizeirechtlicher Bedeutung die Wahrscheinlichkeit und Schwere des Eintritts eines konkreten schädigenden Ereignisses klassifiziert. Anders als im Polizeirecht ist er jedoch nicht zur Berechnung einer bestimmten Risikoschwelle für die Beurteilung einer konkreten Gefahr heranzuziehen, sondern stellt eine gleitende Skala dar, nach der sich der Handlungsbedarf des Verantwortlichen im Rahmen einer bestimmten Pflicht ergibt.[56] Daneben sind viele der weiteren DSGVO-Normen Ergebnisse legislativer Abwägungsentscheidungen, die typisiert die Risiken bestimmter Verarbeitungshandlungen unter Berücksichtigung der betroffenen Interessen für vertretbar oder nicht vertretbar einstufen: so etwa in besonders basaler Form in Art. 6 Abs. 1 DSGVO zu, in dem die (grundsätzlich) abschließenden Erlaubnistatbestände für Datenverarbeitungen festgehalten sind.[57]

---

[53] Siehe zu den einzelnen Steuerungsinstrumenten die Ausführungen in Kapitel 2 B. I. 1.

[54] *Bieker/Bremert*, ZD 2020, 7 (9) sprechen hier von „generischen Grundrechtsrisiken", welche sich nicht aus einem konkreten Verarbeitungsvorgang, sondern „grundsätzlich bei allen Verarbeitungsvorgängen ergeben könnten". Dass sie dabei von Risiken sprechen, verdeutlicht einmal mehr, wie uneinheitlich die Begrifflichkeiten in diesem Zusammenhang verwendet werden.

[55] Zum Risikobegriff m. w. N. *Schwabenbauer*, in: Dalibor/Fröhlich/Rodi/Schächterle/Scharrer, Risiko im Recht – Recht im Risiko: 50. Assistententagung Öffentliches Recht, Greifswald 2010, S. 157 (158 f.).

[56] Siehe hierzu *Schröder*, ZD 2019, 503 (504 f.). Neben der Pflicht zur Ergreifung bestimmter Abhilfe- und Schutzmaßnahmen kann das festgestellte Ergebnis auch darüber entscheiden, ob eine Verarbeitung überhaupt vorgenommen werden darf oder nicht, vgl. Art. 6 Abs. 1 lit. f DSGVO.

[57] Vgl. *Gellert*, EDPL 2016, 481 (485): „Article 6(1) GDPR embodies a similar stance since it determines from the outset whether a processing operation can take place at all."

Tabelle 1: Erläuterung der wichtigsten Begriffe.

Begriff	*Bedeutung*
Regulierung/Regulierungs- bzw. Regelungskonzept	Die Strukturierung des Umgangs mit personenbezogenen Daten durch das Knüpfen an rechtliche Pflichten und Bedingungen, die sich zu einem großflächigen Konzept zusammenfügen.
Steuerung	Die Art und Weise, wie (in erster Linie) Verantwortliche und Betroffene als Normadressaten im Rahmen der Regulierung zu bestimmtem verarbeitungsrelevanten Verhalten bewegt werden sollen.
Schutz(-konzept)	Der Zweck des Regulierungskonzepts, für den die Vorsorge vor Gefährdungen und Schädigungen des Betroffenen im Mittelpunkt steht.
Gefahren/ Gefährdungen	– Als Teil des Charakters des Datenschutzrechts als Vorfeldschutz: konkrete Gefährdungen für Schutzgüter des Betroffenen, die zum Zeitpunkt der als Anknüpfungspunkt dienenden Datenverarbeitung noch nicht abschätzbar sind, deren Eintrittswahrscheinlichkeit und Schwere aber durch generelle Strukturierung und Vorsichtsmaßnahmen gering gehalten werden sollen. – Als Umschreibung der Datenverarbeitung als Anknüpfungspunkt für grundlegende Regulierung und Strukturierung: sehr abstrakte und diffuse Gefährlichkeit in Form des Potentials für spätere konkrete Gefahren, das sich aus der kaum abschätzbaren und nahezu unbegrenzten Möglichkeit späterer Verwendung von Daten und aus ihnen gewonnen Informationen in unterschiedlichen Kontexten ergibt.
Risiko	– Als Teil der Gefahrenvorsorge: möglichst frühes Erkennen und Geringhalten von Risiken in Form noch nicht abschätzbarer Rechtsgutgefährdungen. – Als Teil der Verantwortlichenpflichten: je nach erkannten und bewerteten Risiken in Form von Eintrittswahrscheinlichkeit und Schwere konkreter Schädigungen eine abgestufte Erfordernis für pflichtgemäße Maßnahmen.

Gleichwohl wird diese Typisierung insofern teilweise relativiert, als einige Erlaubnistatbestände die risikobasierte Abwägung im Einzelfall auf den Verantwortlichen (vgl. Art. 6 Abs. 1 lit. f) oder den Betroffenen (vgl. Art. 6 Abs. 1 lit. a) delegieren. Auch diesem Delegieren geht aber eine weitere Risikoabwägung darüber voraus, wie eine tragfähige Entscheidung der jeweiligen Akteure sichergestellt werden kann (vgl. DSFA für Verantwortliche und Voraussetzungen bzgl. Informiertheit und Freiwilligkeit der Einwilligung). Hier zeigt sich, dass sich das Management von Risiken durch alle Ebenen des Datenschutzrechts zieht.

Kapitel 1

Die Akteurspluralität im digitalen Raum

Im Sammelbecken des Internets und der in ihm vorhandenen digitalen Dienstleistungen tummeln sich zahlreiche Akteure. Websites, mobile Applikationen (Apps) und jegliche Art anderer Programme sind in den allermeisten Fällen nicht mehr allein Ergebnis der Schöpfung ihrer jeweiligen Betreiber und Inhaber, sondern bestehen aus Versatzstücken unterschiedlicher Herkunft oder sind ihrerseits in fremde Infrastrukturen eingebettet. Sowohl bei ihrer grundlegenden Funktionsweise als auch bei ihren Geschäftsmodellen greifen sie auf die Unterstützung einer Vielzahl externer Anbieter zurück. Dabei stellt sich die Palette an Zwecken, die durch diese Unterstützung erfüllt werden sollen, als ein bunter Strauß verschiedenster Ausprägungen dar: die simple Anmietung von Server-Space; das Outsourcing unterschiedlicher Bestandteile des eigenen Angebots, für die interne Expertise fehlt; die Erleichterung der Nutzerbedienung oder die Absenkung der Hemmschwelle für Nutzerinteraktionen; die Einbindung von Inhalten wie Videos oder Tweets; die Monetarisierung anfallender Nutzerdaten, häufig in Verbindung mit dem Ausspielen personalisierter Werbung als einziges oder ergänzendes Geschäftsmodell; die Erstellung präziser Nutzungsanalysen zur Fehlerfindung und gezielten Weiterentwicklung des eigenen Dienstes; die Verknüpfung mit großen Plattformen zur besseren Auffindbarkeit und Präsenz gegenüber Nutzern. Die Bandbreite an denkbaren Szenarien ist groß und umfasst kleine Unternehmen und private, unkommerziell handelnde Akteure (man denke an Websites, die auf fremden Servern gehostet werden und vorgefertigte Wordpress-Instanzen oder Google Fonts[1] benutzen) ebenso wie große Konzerne. Dabei kann, insbesondere hinsichtlich der Monetarisierung von Nutzerdaten, ein enger Zusammenhang mit dem Bedeutungszuwachs gesehen werden, der unentgeltlichen Leistungen im digitalen Raum in den vergangenen Jahren zuteilwurde.[2]

Gleichzeitig zeichnet sich der Betrieb digitaler Dienste und Angebote heutzutage nahezu flächendeckend durch seine Datengetriebenheit aus.[3] Entsprechend konsequent ist es, dass bei aller Varianz hinsichtlich des Ausmaßes des

[1] Unter diesem Begriff sind Schriftarten zu verstehen, die von Google zur freien Benutzung für Websites zur Verfügung gestellt werden und dazu, wenn nicht explizit anders konfiguriert, bei jedem Besuch einer Website, die eine solche Schriftart benutzt, Quellcode von Google-Servern nachlädt und dabei Daten der Website-Besucher an Google übermittelt.

[2] Siehe dazu ausführlich *Schweitzer*, in: Körber/Kühling, Regulierung – Wettbewerb – Innovation, S. 269 (272 ff.).

[3] Vgl. *Finck*, Digital Regulation: Designing a Supranational Legal Framework for the Plat-

Einbezugs fremder Akteure und ihrer Leistungen und hinsichtlich des Ausmaßes der Einbettung von Diensten in fremde Infrastrukturen und Plattformen der Fokus aller Beteiligten auf die Verarbeitung personenbezogener Daten stets ein, wenn nicht gar *das* verbindende Element darstellt. Kaum ein beteiligter Akteur trägt nicht in irgendeiner Form zu Datenverarbeitungen bei oder führt sie selbst aus. Auch hier ist das Spektrum weit und kann die Nähe zu und der Einfluss auf Datenverarbeitungen unterschiedlich groß sein. Teilweise werden Daten unmittelbar von (aus Nutzerperspektive) peripheren Akteuren verarbeitet, etwa weil darin gerade deren Leistung gegenüber dem Diensteanbieter (so in Fällen der Nutzeranalyse) oder die Gegenleistung des Diensteanbieters für die von den Akteuren erbrachte Leistung liegt (so in Fällen des Einbezugs von sog. *social plugins*[4] oder bei der unmittelbaren Monetarisierung der Nutzerdaten). Teilweise tragen mehr oder weniger periphere Akteure in unterschiedlichem Maße zur Datenverarbeitung eines zentralen Diensteanbieters bei, etwa weil sie die technische Infrastruktur für die Verarbeitung bereitstellen (so in den zunehmenden Fällen der Präsenz von Diensten auf Plattformen). Während manche der Akteure für den Nutzer unmittelbar sichtbar sind oder ihre Existenz jedenfalls vermutet wird, bleiben andere völlig verborgen. Die sichtbaren bzw. vermuteten Akteure wiederum verarbeiten Daten für die vom Nutzer erwarteten oder erahnten Zwecke, gleichzeitig aber häufig auch zu solchen, die für den Nutzer völlig unerwartet sind, da sie den ursprünglichen Kontext des genutzten Dienstes vollständig verlassen.

In diesem Kapitel soll ein Querschnitt dieser vorherrschenden Akteurspluralität im digitalen Raum anhand beispielhafter Fälle porträtiert werden. Dabei sollen die typischen Akteure, ihre jeweiligen Beiträge sowie die Formen gemeinsamen Zusammenwirkens beleuchtet werden (A.). Auf Basis dessen wird im zweiten Abschnitt des Kapitels eine grobe Systematisierung typischer Fälle mitsamt Formulierung jeweiliger Charakteristika vorgenommen (B.). Dabei wird auch ein interdisziplinärer Blick über den Tellerrand gewagt, um die technischen und organisatorischen Hintergründe dessen, wie im digitalen Bereich Kontrolle über unmittelbar datenverarbeitungserhebliche Umstände, aber auch über das im Umfeld von Datenverarbeitungen stattfindende Verhalten von anderen Akteuren ausgeübt wird, zu beleuchten. Dies geschieht vor dem Hintergrund des – später noch ausführlich zu beleuchtenden – Regimes der datenschutzrechtlichen Verantwortlichkeit und seiner Pflichten.[5] Dieses knüpft in großem Maße an die Möglichkeit eines Akteurs zur Ausübung der Kontrolle über Zwecke und Mittel – und damit die primären Umstände – von Datenver-

---

form Economy, S. 3 ff.; siehe auch *Weichert*, ZD 2014, 605 (607): „Jede Nutzung eines Inhaltsangebots im Internet hat den Anfall von Nutzungsdaten zur Folge."

[4] Siehe hierzu ausführlich die folgende Fallbeschreibung unter A. II. sowie die Analyse des Fashion ID-Urteils des EuGH in Kapitel 2 unter C. II. 4. b) bb).

[5] Siehe dazu Kapitel 2.

arbeitungen an. Auch bei der nachfolgenden Betrachtung soll daher stets die Bedeutung der gemachten Erkenntnisse für Einfluss- und Kontrollmöglichkeiten der einzelnen Akteure mitgedacht werden.

Die Ubiquität der Fälle, in denen dem Nutzer eines Online-Dienstes neben seinem aktiv gewählten Anbieter zahlreiche weitere involvierte Akteure gegenüberstehen, macht die Auswahl beispielhafter Cases nicht leicht. Die Methodik der Fallauswahl ergibt sich daher auf Basis zweier Kriterien: Zum einen handelt es sich um Szenarien, die bereits öffentliche Aufmerksamkeit erregt haben und eingehend behandelt worden sind – sei es juristisch in Form von Gerichtsurteilen oder Behördenmaßnahmen, sei es in Form medialer Berichterstattung mit Fokus auf die datenschutzrechtlichen oder privatheitsrelevanten Konsequenzen. Zum anderen zeichnet sie aus, dass die Menge an beteiligten Akteuren, das unterschiedliche Ausmaß ihrer Erkennbarkeit und die Komplexität der Handlungsdynamiken zwischen ihnen grundlegende datenschutzrechtliche Prämissen vor Herausforderungen stellt und daher eine besondere Gefahr für betroffene Individuen darstellt, wie später noch ausführlich dargelegt werden soll.[6] Sie stehen damit stellvertretend für eine Vielzahl von Verarbeitungstechniken, Geschäftspraktiken und Szenarien, die strukturell ähnlich aufgebaut sind und daher eine vergleichbare datenschutzrechtliche Kritikalität mit sich bringen. Teilweise zeigen sich hier Überschneidungen zu den regelmäßig als spezifisch datenschutzrechtliche Herausforderungen herausgestellten Phänomenen, wie datengetriebene Geschäftsmodelle[7], Profiling[8] und soziale Netzwerke[9]. Der besondere Zuschnitt dieser Betrachtung liegt dabei in ihrem Fokus auf den diese einzelnen Phänomene transzendierenden Aspekt der Akteurspluralität, der den Phänomenen zudem insofern vorgelagert ist, als die über das gesamte Internet verteilte Praktik der Datenerhebung mittels Drittparteien diese erst ermöglicht.

A. Beispielhafte Cases

Bei der Betrachtung der medialen Berichterstattung über Datenskandale in den vergangenen Jahren kann sich wahrlich nicht über zu geringe Auswahl beklagt werden. Auch die Eingrenzung auf solche Fälle, in denen mehr als nur zwei Ak-

---

[6] Siehe dazu Kapitel 3 und 4.

[7] Siehe etwa zum omnipräsenten Modell des OBA ausführlich *Art. 29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting.

[8] Siehe hierzu *Hladjk*, Online-Profiling und Datenschutz; *Lorentz*, Profiling – Persönlichkeitsschutz durch Datenschutz?; *Wenhold*, Nutzerprofilbildung durch Webtracking; *Härting*, CR 2014, 528 (528 ff.); *Bosco* u. a., in: Gutwirth/Leenes/de Hert, Reforming European Data Protection Law, S. 3 (3 ff.).

[9] Hierzu ausführlich *Golland*, Datenverarbeitung in sozialen Netzwerken; *Chmelik*, Social Network Sites – Soziale Netzwerke; *Hain* u. a., K&R 2017, 433 (433 ff.); *Heberlein*, Datenschutz im Social Web; *Kipker/Voskamp*, DuD 2012, 737 (737 ff.); *Schunicht*, Informationelle Selbstbestimmung in sozialen Netzwerken.

teure beteiligt waren, also mehr als nur ein Akteur dem Individuum als Betroffenem gegenüberstand, und diese Tatsache im weitesten Sinne mit dem berichteten Skandal zusammenhing, minimiert die Auswahl nur unwesentlich.

Eine große Kategorie besteht hier aus Smartphone-Apps und den von ihnen implementierten Drittparteien. Im Januar 2020 veröffentlichte der norwegische Verbraucherrat (*Forbrukerrådet*) einen über 180 Seiten langen Bericht, der die Ergebnisse aus der Untersuchung von zehn Android-Apps hinsichtlich ihrer Datenflüsse zusammenfasst.[10] Unter den untersuchten Apps befanden sich unter anderem Dating-Apps wie Tinder, OkCupid und Grindr und Gesundheits-Apps wie Mydays und Period Tracker Clue, bei deren Nutzung besonders sensible Daten anfallen bzw. eingetragen werden. Dabei fanden die Autoren insgesamt 135 Drittparteien, an die die Apps personenbezogene Daten übermittelten, darunter IP-Adressen, GPS-Standortdaten, Daten bzgl. sexueller Ausrichtung und die zur einzigartigen Zuordnung der jeweiligen Individuen über Apps hinweg genutzten Werbe-IDs (sog. *Advertising IDs*).[11] Unter den erkannten Drittparteien befanden sich zahlreiche Adtech- und Datenbroker-Unternehmen, deren selbsternannter Zweck das Anfertigen von Persönlichkeitsprofilen über und generelle Tracking von App-Nutzer(n) ist.[12] Die vom Verbraucherrat unter anderem untersuchte App Grindr war bereits im Jahre 2018 negativ aufgefallen, als publik wurde, dass Drittparteien entgegen der App-eigenen Datenschutzerklärung Zugriff nicht nur auf die Standortdaten, sondern auch auf den HIV-Status von Nutzern hatten.[13] Auch Tinder geriet Anfang 2020 in die Schlagzeilen: Nachdem die App eigens einen sog. Panik-Button eingeführte hatte, der es Nutzern ermöglichen sollte, im Falle einer Gefährdungslage während eines Dates schnell und unkompliziert Polizei oder Notarzt zu rufen, stellte sich heraus, dass die dafür zwingend zu installierende App die funktionsnotwendigen Daten (Standort, Name, Telefonnummer etc.) nicht nur im Fall der Fälle mit den gerufenen Einsatzkräften, sondern generell mit zahlreichen Drittanbietern teilte.[14] Zu einem ähnlichen Ergebnis wie der norwegische Verbraucherrat kam

---

[10] *Norwegischer Verbraucherrat (Forbrukerrådet)*, Out of Control: How consumers are exploited by the online advertising industry.

[11] *Norwegischer Verbraucherrat (Forbrukerrådet)*, Out of Control: How consumers are exploited by the online advertising industry, S. 81 ff.

[12] Siehe als Beispiel die ausführliche Analyse der verschiedenen Akteure im Umfeld der Grindr-App bei *Norwegischer Verbraucherrat (Forbrukerrådet)*, Out of Control: How consumers are exploited by the online advertising industry, S. 123 ff.

[13] Vgl. *Azeen Ghorayshi* und *Sri Ray*, Grindr Is Letting Other Companies See User HIV Status and Location Data, Buzzfeed News vom 02.04.2018 (https://www.buzzfeednews.com/article/azeenghorayshi/grindr-hiv-status-privacy). Grindr hat den entsprechenden Zugriff inzwischen nach eigenen Angaben abgestellt, vgl. *Ina Fried*, Exclusive: Grindr to stop sharing HIV status with third parties, Axios vom 02.04.2018 (https://www.axios.com/exclusive-grindr-security-chief-on-hiv-disclosure-b5a64fdb-8c1d-4a08-a94e-67506d4a0d0b.html). Beide zuletzt abgerufen am 14.01.2022.

[14] Vgl. *Shoshana Wodinsky*, Tinder's New Panic Button Is Sharing Your Data With Ad-

eine Studie, die 2019 das Datenweitergabeverhalten von 24 Gesundheits-Apps untersuchte und in 19 von ihnen SDKs von Drittparteien fand, von denen wiederum 67 % erkennbar aus dem Bereich Analytics und Adtech stammten.[15] Weitere Studien kamen zu ähnlichen Ergebnissen.[16] Andere Fälle zeigen auf, dass die Handlungen von Drittparteien auch für die App-Anbieter selbst nicht immer absehbar und kontrollierbar sind. So kam es im Zusammenhang mit der Wetter-App AccuWeather zu einem Skandal,[17] als publik wurde, dass Reveal Mobile, ein auf Standortdaten spezialisiertes Marketing- und Analytics-Unternehmen, dessen SDK in die AccuWeather-App unter iOS eingebunden war, mittelbare und minimal unpräzisere Standortdaten selbst von denjenigen App-Nutzern erhoben hatte, die ihre Zustimmung zur Weitergabe solcher Daten explizit verweigert hatten.[18] Weil infolge dieser Verweigerung kein direkter Zugriff auf die GPS-Daten der Smartphones möglich war, erhob das SDK mittels der App die sog. BSSIDs (also Hardwareadressen) der mit den jeweiligen Smartphones verbundenen WLAN-Router, die sich mit Hilfe eines Abgleichs mit im Internet öffentlich zugänglichen Listen konkreten Standorten zuordnen ließen.[19] AccuWeather selbst betonte im Nachgang, sich selbst an die Entscheidungen der Nutzer gehalten zu haben und auch gegenüber Drittparteien wie Reveal Mobile den Rückgriff auf andere Möglichkeiten und damit das Unterlaufen des Nutzerwillens vertraglich untersagt zu haben.[20] Ob diese offizielle Aussage der

---

Tech Companies, Gizmodo vom 24.01.2020 (https://gizmodo.com/tinders-new-panic-button-is-sharing-your-data-with-ad-t-1841184919). Zuletzt abgerufen am 14.01.2022.

[15] *Grundy* u. a., BMJ 2019, l920; zur Adtech-Branche insgesamt siehe *Costello*, TechReg 2020, 11 (12 ff.).

[16] Siehe beispielsweise die Artikel von *Alex Hern*, Three quarters of Android apps track users with third party tools – study, The Guardian vom 28.11.2017 (https://www.theguardian.com/technology/2017/nov/28/android-apps-third-party-tracker-google-privacy-security-yale-university) sowie *Patrick Beuth*, Android-Apps verraten heikle Interessen an Facebook, SpiegelOnline vom 13.12.2018 (https://www.spiegel.de/netzwelt/apps/facebook-sdk-android-apps-geben-heikle-interessen-preis-a-1242898.html). Die zunehmende Entwicklung des Internet of Things führt zudem dazu, dass betroffene Apps teilweise unmittelbare Auswirkungen auf physische Objekte haben können, siehe *Bill Budington*, Ring Doorbell App Packed With Third-Party Trackers, Electronic Frontier Foundation vom 27.01.2020 (https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers). Alle zuletzt abgerufen am 14.01.2022.

[17] Siehe *infra* bei I. 2. für eine detailliertere Abhandlung dieses Falls.

[18] Vgl. *Will Strafach*, Advisory: AccuWeather iOS app sends location information to data monetization firm, Hackernoon vom 22.08.2017 (https://hackernoon.com/advisory-accuweather-ios-app-sends-location-information-to-data-monetization-firm-83327c6a4870). Zuletzt abgerufen am 14.01.2022.

[19] Siehe für nähere Details zu dieser Methode die Beschreibung eines ähnlich gelagerten Falls aus 2016, bei dem sich die dort betroffene Drittpartei *InMobi* mit der gegen sie ermittelnden *FTC* einigen konnte. *Nithan Sannappa & Lorrie Cranor*, Tech@FTC vom 09.08.2016 (https://www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement). Zuletzt abgerufen am 14.01.2022.

[20] Vgl. *Ashley Carman*, AccuWeather deflects blame after selling users' data, even if they opt out, The Verge vom 24.08.2017 (https://www.theverge.com/2017/8/24/16197262/accu

Wahrheit entspricht, lässt sich nicht überprüfen. Der Fall zeigt dennoch symptomatisch die Problematik dahinter, dass die Einbindung fremden (Programm-) Codes[21] mittels SDKs Drittparteien Zugriffsrechte ermöglicht, die vom App-Anbieter im Nachhinein kaum überprüft oder kontrolliert werden können.[22]

In eine ähnliche Richtung zeigt der viel diskutierte Fall um Facebook und Cambridge Analytica, bei dem die Daten von Facebook-Nutzern analysiert wurden, um präzise und teilweise manipulierende Wahlwerbung zielgerichtet an diese ausspielen zu können.[23] Zwar ging es hier um keine Smartphone-App, aber mit This is Your Digital Life um eine App innerhalb des Facebook-Ökosystems, die vordergründig einen Persönlichkeitstest als Quiz anbot, sich daneben aber nicht nur die Profildaten der App-Nutzer selbst, sondern auch die ihrer Facebook-Freunde von Facebook übermitteln ließ. Möglich war dies überall dort, wo die betroffenen Freunde es versäumt hatten, die entsprechende, standardmäßig aktivierte und nur schwer auffindbare, Option in ihren Privatsphäreeinstellungen zu deaktivieren. War dies im Grundsatz von Facebook im Rahmen des erlaubten Zugriffs zum Zwecke der Forschung noch erwünscht, entsprach die nachfolgende Übermittlung der erhobenen Daten zu gänzlich anderen Zwecken an Cambridge Analytica (wenn man den offiziellen Äußerungen glauben mag) nicht mehr der getroffenen Vereinbarung.[24] Mit ähnlichen Problemen hatte und hat auch Amazon zu kämpfen. Auf dessen (für den Endnutzer unsichtbaren) Plattform *Marketplace* können externe Händler, die auf Amazon ihre Produkte verkaufen, mittels Apps Zugriff auf Kundendaten erlangen, wenn sie diese – etwa für den Versand von Produkten oder für Steuerabrechnungen – benötigen. Während die weitergehende Nutzung der Daten nach Vereinbarung mit Amazon explizit nicht gestattet war, ermöglichten die Entwickler der entsprechenden Apps den Händlern mittels der von *Amazon* zur Verfügung gestellten Entwicklerschnittstelle weitreichenden Datenzugriff, sodass die betreffenden Daten etwa automatisiert genutzt wurden, um Käufer gezielt auch auf Facebook mit Werbung zu adressieren.[25] Auch hier zeigt sich ein – wenn

---

weather-app-mobile-sdk-collect-user-data-privacy). Siehe außerdem die gemeinsame Stellungnahme von AccuWeather und Reveal Mobile vom 22.08.2017 (https://www.accuweather.com/en/press/69041756). Beides zuletzt abgerufen am 14.01.2022.

[21] Hier verstanden als der Quelltext, der die Funktionsweise von Apps oder Diensten so beschreibt, dass das Endgerät des Nutzers diese umsetzen kann.

[22] Vgl. *Carlos Ribas*, The AccuWeather/Reveal Situation Is Really An iOS Privacy Problem, Medium vom 25.08.2017 (https://medium.com/@carlosribas/the-accuweather-reveal-situation-is-really-an-ios-privacy-problem-78e85a6f8539). Zuletzt abgerufen am 14.01.2022.

[23] Für eine ausführliche Behandlung des Falls und einen Definitionsansatz für digitale Manipulierung siehe *Susser* u. a., Geo. L. Tech. Rev. 2019, 1 (9 ff.).

[24] Zur Rolle von Facebook und dem hinter der betreffenden App stehenden Unternehmen Global Science Research siehe das Interview mit *Daphne Keller* auf Legal Aggregate vom 20.03.2018 (https://law.stanford.edu/2018/03/20/data-analytic-companies-app-developers-Facebooks-role-data-misuse/). Zuletzt abgerufen am 14.01.2022.

[25] Siehe *Louise Matsakis*, Amazon Cracks Down on Third-Party Apps Over Privacy Vio-

auch naheliegenderes und weniger drastisches – Kontrollproblem, wenn Facebook und Amazon einerseits den Zugriff auf Profil- und Kundendaten nur zu bestimmten Zwecken erlauben, gleichzeitig aber nur begrenzt Möglichkeiten haben, die Einhaltung dieser selbst gesetzten Limitierungen zu kontrollieren und durchzusetzen.

Andere Fälle zeigen auf, wie die Unübersichtlichkeit privater datenverarbeitender Akteure auch Auswirkungen auf den staatlichen Umgang mit Nutzerdaten haben kann. So deckten Recherchen im November 2020 auf, dass das US-Militär Standort- und andere Daten über ein Datenbrokerunternehmen namens X-Mode gekauft hatte, dessen SDK neben (nach eigenen Angaben) ungefähr 400 anderen Apps auch in Muslim Pro und Muslim Mingle, zwei muslimischen Gebets- bzw. Dating-Apps, implementiert war und die betreffenden Daten an das Unternehmen sendete.[26]

Eine weitere, letztlich ähnlich gelagerte Kategorie umfasst Websites und die von diesen implementierten Drittparteien. Auch hier ist der Einbezug einer Vielzahl von Drittparteien der Normalfall und kommt letztlich keine Website ohne sie aus,[27] woran nach derzeitigem Erkenntnisstand auch die DSGVO in den ersten Jahren ihrer Anwendbarkeit im Großen und Ganzen nichts geändert hat.[28] Ein Blick auf die publik gewordenen oder wissenschaftlich beleuchteten Fälle zeigt, dass die oben beschriebenen Probleme hinsichtlich Intransparenz und begrenzter Kontrollmöglichkeiten gegenüber diesen Drittparteien hier nicht schwächer, im Zweifel eher stärker präsent sind. Im Februar 2020 berichtete der *Guardian* darüber, dass die Websites zahlreicher Behörden britischer Gemeinden Databroker-Unternehmen und anderen Drittparteien die Erhebung von Nutzerdaten erlaubt hatten, darunter sensible Daten im Zusammenhang mit der Beantragung von Sozialleistungen oder Hilfsangeboten für Drogenmissbrauch.[29] Im August 2019 wurde publik, dass das Bayerische Rote Kreuz auf

---

lations, Wired vom 09.10.2019 (https://www.wired.com/story/amazon-marketplace-apps-privacy/). Zuletzt abgerufen am 14.01.2022.

[26] Siehe *Joseph Cox*, How the U. S. Military Buys Location Data from Ordinary Apps, Motherboard vom 16.11.2020 (https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x): „Location data firm X-Mode […] encourages app developers to incorporate its SDK, essentially a bundle of code, into their own apps. The SDK then collects the app users' location data and sends it to X-Mode." Zuletzt abgerufen am 14.01.2022.

[27] So etwa erst kürzlich das Ergebnis einer Studie des Reuters Institute, das insbesondere auf Nachrichtenseiten eine Fülle an Drittparteien fand. Vgl. *Libert/Nielsen*, Third-Party Web Content on EU News Sites: Potential Challenges and Paths to Privacy Improvement.

[28] Siehe *Sørensen/Kosta*, Before and After GDPR, S. 1599, wonach sich trotz kategoriespezifischer Fluktuation die durchschnittliche Zahl von in Websites einbezogenen Drittparteien nicht signifikant verändert hat.

[29] Siehe *Sarah Marsh*, Councils let firms track visits to webpages on benefits and disability, The Guardian vom 04.02.2020 (https://www.theguardian.com/technology/2020/feb/04/councils-let-firms-track-visits-to-webpages-on-benefits-and-disability). Zuletzt abgerufen am 14.01.2022.

seiner Website einen sog. Tracking-Pixel[30] von Facebook eingebunden hatte, der im Rahmen eines von interessierten Besuchern auszufüllenden Fragebogens zur Evaluierung der Geeignetheit zur Blutspende unter anderem die Antworten auf Fragen zu solch sensiblen Themen wie HIV-Status, Drogenkonsum, Schwangerschaft oder sexueller Orientierung an Facebook übermitteln konnte, weil er vom Roten Kreuz falsch konfiguriert worden war.[31]

Schon diese beispielhaft aufgeführten Fälle verdeutlichen auf den ersten Blick mehrere Dinge: Erstens: Das Angebot digitaler Dienste ist im gleichen Maße wie der digitale Raum insgesamt zunehmend datengetrieben.[32] Zweitens: Die Akteurspluralität bei der Nutzung digitaler Dienste ist zum absoluten Normalfall geworden und bedeutet im Zusammenhang mit der genannten Datengetriebenheit der Dienste, dass die Nutzung eines Dienstes mit vielen Datenverarbeitungen durch zahlreiche Akteure und durch die Unterstützung zahlreicher Akteure einhergeht.[33] Drittens: Die hohe Anzahl publik gewordener Skandale und Datenlecks im Zusammenhang mit aus Nutzerperspektive unbekannten oder unerwarteten Akteuren und Datenempfängern deutet darauf hin, dass diese Akteurspluralität – unabhängig von in Einzelfällen tatsächlich eingetretenen Schädigungen – eine grundlegend gesteigerte Gefährdung für Datenschutz und Privatheit mit sich bringen könnte. Viertens: Die genutzten digitalen Dienste befinden sich weder im luftleeren Raum, noch befinden sich die neben Nutzer und Anbieter zusätzlich involvierten Akteure zufällig und unstrukturiert neben diesen – stattdessen lässt sich die Gemengelage an Akteuren am besten als digitales Ökosystem beschreiben, in welches ein Dienst eingebettet ist und in dem er sich im Gefolge unterschiedlicher Akteure mit ihren jeweils eigenen Rollen und damit eigenen Motivationen, Handlungs- und Gestaltungsmöglichkeiten befindet. Um diese Gemengelage besser zu verstehen, bietet es sich an, die typischen Rollen sowie die Umgebungen, in denen sie sich bewegen, näher zu betrachten.

I. Verarbeitungen auf Plattformen

Wir befinden uns im Zeitalter der Plattformökonomie.[34] Schon im analogen Bereich war in den letzten Jahren ein zunehmender Trend hin zu Produkten und Diensten zu betrachten, die auf oder im Kontext von Plattformen angeboten

---

[30] Zur Erläuterung der Funktionsweise von Pixeln und ähnlichen Tracking-Methodensiehe *Stiemerling/Lachenmann*, ZD 2014, 133 (134 ff.).

[31] Siehe *Matthias Eberl*, Blutspendedienst übermittelte heikle Daten an Facebook, Süddeutsche Zeitung vom 27.08.2019 (https://www.sueddeutsche.de/digital/blutspende-brk-facebook-patientendaten-1.4576563). Zuletzt abgerufen am 14.01.2022.

[32] Siehe erneut *Weichert*, ZD 2014, 605 (607).

[33] Siehe *fouad* u. a., Proceedings on Privacy Enhancing Technologies 2020, 499 (514).

[34] Zu diesem Begriff *Dijck* u. a., The platform society; Vgl. auch *Evans*, Berkeley Tech. L. J. 2012, 1201 (1205): „[…] although multi-sided platforms have existed for thousands of years, they are becoming an increasingly important part of the fabric of the economy."

werden.[35] Nicht anders gestaltet es sich im digitalen Raum – immer häufiger werden digitale Dienste auf digitalen Plattformen angeboten und finden die im Zusammenhang mit den Diensten durchgeführten Datenverarbeitungen daher ebenfalls auf Plattformen statt. Plattformen, respektive ihre Betreiber, sollen dabei verstanden werden als eigenständige Akteure des digitalen Ökosystems. Die konkrete Definition dessen, was sie ausmacht, kann je nach gewählter Perspektive und Fachdisziplin differieren und gestaltet sich insgesamt ausgesprochen schwierig – es scheint, als würde sich der Begriff der digitalen Plattform insbesondere durch seine Dynamik und Konturlosigkeit auszeichnen. Häufig werden einzelne Charakteristika in den Mittelpunkt gestellt, so etwa die Funktion als Intermediär für das Zusammenbringen unterschiedlicher Marktseiten[36] (etwa Kunden, Nutzer oder Empfänger einerseits und gegenüberstehende Anbieter von Diensten, Produkten oder Informationen andererseits).[37] Auch das BKartA versteht unter Plattformen solche Unternehmen, die „als Intermediäre die direkte Interaktion zweier oder mehrerer Nutzerseiten, zwischen denen indirekte Netzwerkeffekte bestehen, ermöglichen."[38] Das Europäische Parlament hingegen gibt unumwunden zu, dass eine einheitliche (juristische) Definition ob der vielen verschiedenen Spielarten und Ausprägungen von Plattformen nicht leistbar ist.[39] Häufig folgt das konkrete Verständnis und folgen die als besonders virulent herausgestellten Merkmale der jeweiligen rechtspolitischen Stoßrichtung. So wundert es nicht, dass aus wettbewerbsrechtlicher Perspektive das Potential für unlautere Marktmacht und Machtmissbrauch und die zu ihnen beitragenden Netzwerkeffekte[40], für die Diskussion um die Verantwortlichkeit der Plattformbetreiber für rechtswidrige Inhalte oder die Aufrechterhaltung bestimmter qualitativer Zielwerte[41] hingegen ihre Rolle als besonders effektiver

---

[35] Siehe etwa die Abhandlungen am Beispiel Intel bei *Gawer/Henderson*, J Economics Management Strategy 2007, 36.

[36] Vgl. die Ausführungen bei *Schweitzer*, in: Körber/Kühling, Regulierung – Wettbewerb – Innovation, S. 269 (270 f.).

[37] So etwa die Definition des französischen Digitalrates *Conseil National du Numérique*, Ambition Numérique. Pour une Politique Française et Européenne de la Transition Numérique, S. 59: „[u]ne plateforme pourrait être définie comme un service occupant une fonction d'intermédiaire dans l'accès aux informations, contenus, services ou biens, le plus souvent édités ou fournis par des tiers."

[38] *Bundeskartellamt*, Arbeitspapier – Marktmacht von Plattformen und Netzwerken, S. 14.

[39] *European Parliament*, Report on online platforms and the digital single market (2016/2276(INI)), S. 6: „[…] that it would be very difficult to arrive at a single, legally relevant and future-proof definition of online platforms at EU level, owing to factors such as the great variety of types of existing online platforms and their area of activity, as well as the fast-changing environment of the digital world."

[40] Siehe hierzu *Bundeskartellamt*, Arbeitspapier – Marktmacht von Plattformen und Netzwerken; *Volmar*, Digitale Marktmacht; *Lynskey*, Regulating ‚Platform Power', S. 1 ff.; *Guggenberger*, Stanford Technology Law Review, 2021, 237 (237 ff.).

[41] Vgl. etwa zum umstrittenen Vielfaltsbegriff im Medienrecht *Paal*, MMR 2018, 567 (567 ff.); *Paal/Heidtke*, ZUM 2020, 230 (230 ff.); *Müller-Terpitz*, AfP 2017, 380 (380 ff.).

Verbreiter und Intermediär[42] im Mittelpunkt steht.[43] Besonders aktuell sind die mit der im Juli 2020 anwendbar gewordenen P2B-Verordnung verbundenen Bestrebungen, die Markt- und Verhandlungsmacht von Plattformen gegenüber den gewerblichen Nutzern ihres Angebots einzuhegen[44] sowie die unter dem Begriff Digital Services Act laufenden Bemühungen, die in die Jahre gekommene eCommerce-RL zu modernisieren und an die für Verbraucher drohenden Gefahren der heutigen Plattformökonomie anzupassen[45]. Die Schwierigkeit, einen übergreifenden und kohärenten Rechtsrahmen für den diffusen Begriff der Plattform und die zahlreichen von ihm tangierten Rechtsbereiche zu schaffen, wird aber auch an diesem Ansatz offenbar, wie *Schneider&Kremer* pointiert ausführen, wenn sie kritisieren, dass es der Verordnung „schlicht an der wissenschaftlichen und empirischen Durchdringung der komplexen Strukturen der Plattformökonomie an den Schnittstellen zwischen Vertrags-, Lauterkeits-, Wettbewerbs- und Datenschutzrecht" fehle.[46] Auch aus wirtschaftswissenschaftlicher Perspektive wurden Plattformen klassischerweise betrachtet als durch Netzwerkeffekte geprägte mehrseitige Märkte, innerhalb derer der Betreiber unterschiedliche Nutzerseiten mit jeweils unterschiedlichen Erwartungen befriedigen und gleichzeitig durch beide Geld verdienen muss.[47] Dabei kann das Geschäftsmodell des Plattformbetreibers mal stärker auf der einen, mal stärker auf der anderen Nutzerseite aufbauen (sodass eine Nutzerseite der sog. *loss leader* und eine der sog. *profit leader* ist), muss aber insgesamt die unterschiedlichen Nutzerinteressen in Einklang bringen, damit sich das Modell für alle Beteiligten lohnt:[48] „An important characteristic of multisided markets is that the demand on each side vanishes if there is no demand on the others,

---

[42] Vgl. *Schulz*, Roles and Responsibilities of Information Intermediaries; *Schulz/Dankert*, Informatik-Spektrum 2017, 351 (351 ff.); *Thompson*, Vand J Ent & Tech L 2016, 783 (783 ff.) Zu den einzelnen regulatorischen Bemühungen im Bereich der Intermediärshaftung siehe zudem ausführlich in Kapitel 3 D. III.

[43] Siehe auch die Definitionsannäherungen bei *Adam/Micklitz*, in: Micklitz/Joost/Reisch/Zander-Hayat, Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt, S. 45 (48 ff.).

[44] Siehe dazu ausführlich *Alexander*, WRP 2020, 945; vgl. auch *Busch*, GRUR 2019, 788; *Schneider/Kremer*, WRP 2020, I; *Voigt/Reuter*, MMR 2019, 783.

[45] Einführend hierzu *Busch* u. a., MMR 2020, 667 (667 f.).

[46] *Schneider/Kremer*, WRP 2020, I.

[47] Siehe hierzu grundlegend *Rochet/Tirole*, Journal of the European Economic Association 2003, 990.

[48] Siehe *Rochet/Tirole*, Journal of the European Economic Association 2003, 990 (991), die das klassische Beispiel einer Videospielplattform erwähnen. Hier basiert das Geschäftsmodell nur sekundär auf den Endkunden, die sich (zwar in regelmäßigen Abständen, aber immer nur einmalig) eine Spielkonsole kaufen, und primär auf den Spieleproduzenten, die Lizenzen für die Entwicklung erwerben und Anteile an den Verkaufseinnahmen abgeben müssen. Das Gegenbeispiel stellen klassische PC-Betriebssysteme dar, die ihr Geld in erster Linie durch die Endnutzer verdienen, während Entwickler nahezu kostenneutral Software entwickeln können. Vgl. auch *Weyl*, American Economic Review 2010, 1642 (1649 ff.).

regardless of what the price is."[49] Das Forschungsinteresse betrifft hier daher in erster Linie die Preisdynamiken und Konkurrenzkämpfe zwischen den einzelnen Plattformen und damit die Frage, durch welche Strategien sich Plattformen wirtschaftliche Vorteile erarbeiten können.[50]

Ergänzt man die wirtschafts- um eine wirtschaftsinformatikwissenschaftliche Perspektive, liegt der Fokus zunehmend auf Plattformbetreibern als wirtschaftliche Akteure, die sich zur Steigerung der Wertschöpfung im Rahmen ihres eigenen Angebots dritter Akteure bedienen, denen sie wiederum die grundlegenden Werkzeuge und Parameter der Wertschöpfung zur Verfügung stellen und die sie mit einem Stamm potenzieller Kunden zusammenbringen.[51] Sie müssen demnach ein eigenes *system of use* anbieten, auf das andere Akteure aufbauen und das sie einfach erweitern können.[52] Technischer gesprochen: Eine Plattform ist eine erweiterbare Codebasis eines softwarebasierten Systems, das die grundlegende Funktionalität sowie die mit ihr verbundenen und interagierenden Module und die Interfaces, durch die sie interagieren, bereitstellt.[53]

Was eine Plattform diesem Verständnis zufolge auszeichnet und für ihren Betreiber wirtschaftlich attraktiv macht, ist demnach das Wertschöpfungs- und Innovationspotential, das durch die Kombination der bereitgestellten (soft- und bzw. oder hardware-seitigen) Infrastrukturen, Werkzeuge und Gestaltungsmöglichkeiten durch die Plattformbetreiber einerseits und die unabhängige Kreativität der davon angezogenen Nutzer andererseits zustande kommt, und das der Plattformbetreiber zu seinen wirtschaftlichen Gunsten nutzen will.[54] Das Forschungsinteresse dieses Zweigs der Wirtschaftsinformatik zielt dementsprechend zunehmend stärker nicht auf die Intermediärsfunktion, also das Zusammenbringen der mehrseitigen Nutzergruppen, sondern auf ein besseres Verständnis der Dynamiken hinter der Generativität und Innovationsfähigkeit

---

[49] *Evans* u. a., Invisible engines: how software platforms drive innovation and transform industries, S. 64.

[50] Vgl. *de Reuver* u. a., Journal of Information Technology 2018, 124 (125 f.).

[51] Vgl. die Ausführungen bei *Beimborn* u. a., WI 2011, 371; siehe auch ausführlich zu Softwareplattformen *Evans* u. a., Invisible engines: how software platforms drive innovation and transform industries.

[52] *Gawer/Cusumano*, MIT Sloan Management Review 2008, 28 (29).

[53] *Tiwana* u. a., Information Systems Research 2010, 675 (676): „The extensible codebase of a software-based system that provides core functionality shared by the modules that interoperate with it and the interfaces through which they interoperate." Gleichzeitig machen es Entwicklungen wie Plattformen auf Plattformen zunehmend schwieriger, eine trennscharfer Abgrenzung dafür herzustellen, welche Akteure im Einzelfall eine Plattform darstellen, und welche nicht. Vgl. *de Reuver* u. a., Journal of Information Technology 2018, 124 (128).

[54] Vgl. *von Hippel/Katz*, Management Science 2002, 821; siehe außerdem *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (175) m. w. N.; teilweise wird auch das Wertschöpfungspotential durch Mitwirkung der Endnutzer betrachtet, vgl. *Skog* u. a., Digital Service Platform Evolution: How Spotify Leveraged Boundary Resources to Become a Global Leader in Music Streaming, S. 4566 ff.

solcher Plattformen und den Möglichkeitsräumen, die sie ihren Nutzern bieten.[55]

Im Rahmen dieser Arbeit soll auf dieses zuletzt genannte Verständnis aufgebaut und sollen unter digitalen Plattformen und ihren Betreibern daher generell solche Akteure verstanden werden, die digitale Räume und die zugrundeliegende technische Infrastruktur sowie die Ressourcen bereitstellen und kontrollieren, auf der und auf deren Basis ggf. sie selbst, aber auch und vor allem dritte unabhängige Akteure Dienste entwickeln und anbieten. Als entscheidendes, aber nicht einziges Kriterium gestaltet sich dabei die technische Ebene – legt ein Anbieter im Rahmen seines abgegrenzten digitalen Raums fest, nach welchen Kriterien und auf welcher Basis Dienste entwickelt werden und über welche Schnittstellen und unter welchen Umständen in diesem Zusammenhang personenbezogene Daten von Endnutzern verarbeitet werden können, so bietet er eine Plattform im Sinne des Verständnisses dieser Arbeit an. Neben der technischen bestehen weitere wichtige, für das hiesige Verständnis aber alleine nicht ausreichende Ebenen wie die vertragliche Kontrollebene, die den Zugang zur Plattform reglementierende Kontrollebene sowie die faktische Kontrollmacht, die mit der Marktmacht, die Plattformen häufig anheimfällt, sowie den Netzwerkeffekten, die Plattformnutzer sich erhoffen, einhergeht.[56] Häufig bedingen sich diese Ebenen gegenseitig bzw. sichern ihre jeweilige Durchsetzung gegenseitig ab. Die in anderen Plattformdefinitionen dominierenden Merkmale (Netzwerkeffekte, Intermediärsfunktion etc.) sind daher auch für den hier gewählten Analyseblick mittelbar von Bedeutung, aber nur in Form bloß einer von mehreren notwendigen und nicht in Form einer hinreichenden Bedingung. Um es mit einem abgewandelten Zitat aus der Wirtschaftsinformatik zu sagen: *„*Platforms that merely mediate between different user groups but offer no extensible codebase should not be considered digital platforms […].*“*[57]

Umfasst sind vom hier gewählten Fokus daneben auch Aktivitäten von Plattformbetreibern abseits der eigenen Plattform im engeren Sinne, also dem kontrollierten digitalen Raum, wenn sie mit der Auslagerung von Plattformbestandteilen oder der mit der Plattform einhergehenden Reichweite zusammenhängen: „[…] platforms are transforming into components being integrated into more

---

[55] Vgl. *de Reuver* u. a., Journal of Information Technology 2018, 124 (126).

[56] Vgl. *Boudreau/Hagiu*, in: Gawer, Platforms, Markets and Innovation, S. 163 (164): „MSPs [multi-sided platforms] regulate access to and interactions around MSPs through nuanced combinations of a long list of legal, technological, informational and other instruments – including price setting.“

[57] *de Reuver* u. a., Journal of Information Technology 2018, 124 (127); in dieselbe Richtung gehend für mobile Plattformen wie Android und iOS *Greene/Shilton*, New Media & Society 2018, 1640 (1675): „Mobile platforms are not just passive intermediaries supporting other technologies.“ Aufgrund der bereits beschriebenen Datengetriebenheit werden solche Plattformökosysteme zuweilen auch Datenökosysteme (data ecosystems) genannt. Siehe etwa *Oliveira/Lóscio*, What is a data ecosystem?, S. 128 ff.

extensive digital infrastructures."[58] Betrachtet wird somit das gesamte Ökosystem einer Plattform, das sich aus der Plattform und all den auf ihr agierten Akteuren und ihren Beziehungen zueinander ergibt.[59]

Die klassischen Akteursrollen auf Plattformen sind mit diesem Verständnis die des *Plattformbetreibers*, des unabhängigen *Diensteanbieters* auf der Plattform und des *(End-)Nutzers*. Hinzu treten in der Realität, wie in den obigen Fällen teilweise angeklungen, zahlreiche *Drittparteien* oder *Drittanbieter*, die durch die auf einer Plattform vertretenen Diensteanbieter mittelbar oder unmittelbar in das Ökosystem einer Plattform einbezogen werden. Bei der Betrachtung der auf Plattformen stattfindenden Datenverarbeitungen erscheint es zunächst sinnvoll, zwischen Verarbeitungen durch Diensteanbieter einerseits und solchen durch den Betreiber der betreffenden Plattform andererseits zu unterscheiden. Darüber hinaus bieten sich als dritte Kategorie Verarbeitungen durch die eben genannten Drittparteien an.

1. Verarbeitungen durch Diensteanbieter

Die klassischste Form der Verarbeitung personenbezogener Daten auf einer Plattform erfolgt durch den einzelnen Anbieter, dessen Dienst der Nutzer wahrnimmt. Das kann etwa eine App auf einem Smartphone, einem Smart-TV oder einem sozialen Netzwerk wie Facebook sein, aber auch ein Add-on in einem Browser oder einem weiteren Dienst. In der Regel ist dem Nutzer dabei bewusst, dass der Diensteanbieter ein eigenständiger Akteur und nicht identisch mit dem Plattformbetreiber ist. Spielt sich eine Datenverarbeitung in diesen Fällen vordergründig bilateral zwischen dem Nutzer eines Dienstes und dem Diensteanbieter ab und entspricht damit vermeintlich der klassischen Dichotomie, die das Datenschutzrecht zwischen dem Betroffenen und dem Verantwortlichen eröffnet,[60] so sollte hier aufgrund des gewählten Fokus' auf Einflussmöglichkeiten und Entscheidungsmacht dennoch auch der Plattformbetreiber als Akteur in den Blick genommen werden. Er bestimmt durch die Ausgestaltung seiner Plattform generell die Art und Weise, nach der Diensteanbieter, aber auch Nutzer auf dieser agieren und sich verhalten können. Für Diensteanbieter bedeutet dies, sich an die Plattformvorgaben unter anderem hinsichtlich Qualitätssicherung und Zertifizierung ihrer Apps anzupassen. Diese Vorauswahl und die generelle thematische bzw. inhaltliche Ausrichtung der Plattform kann sich

---

[58] *de Reuver* u. a., Journal of Information Technology 2018, 124 (130).

[59] Vgl. *Evans* u. a., Invisible engines: how software platforms drive innovation and transform industries, S. vii, die von Ökosystemen im Zusammenhang mit Plattformen als „mutually dependent communities of businesses and consumers that have a symbiotic relationship with the platform" sprechen. Siehe auch *Tiwana* u. a., Information Systems Research 2010, 675 (683 ff.).

[60] Siehe zu den klassischen Akteursrollen des Datenschutzrechts in Abgrenzung zum Verantwortlichen ausführlich *infra* in Kapitel 2 C. II.

teilweise bereits darauf durchschlagen, welche Verarbeitungszwecke und Datenarten überhaupt infragekommen. Dies gilt, obwohl Triebfeder solcher Limitierungen nicht unbedingt zwingend der Datenschutz der Nutzer, sondern häufig ein davon unabhängiger von der Plattform verfolgter Wert ist. Lässt etwa Apple auf seinen Plattformen iOS und MacOS im Rahmen des Distributionskanals des AppStore keine pornografischen Applikationen zu, weil dies dem eigenen Verständnis als familienfreundliche Plattform entgegenstünde,[61] ist ein Nebeneffekt dieser zunächst verarbeitungsneutralen Entscheidung, dass keine damit zusammenhängenden Nutzungsdaten anfallen und verarbeitet werden können. Auf inhaltlicher Eben gilt dies genauso. Stellt Amazon im Rahmen seiner oben beschriebenen Plattform Marketplace klar, dass Entwickler dazu eingeladen sind, Apps für Händler zu entwickeln, dabei aber beachten müssen, dass die Verarbeitung von Kundendaten einzig zum Zwecke der Produktversands und der steuerlichen Abrechnung vorgesehen ist, verengt sich deren Möglichkeitsraum – jedenfalls theoretisch – bereits beträchtlich. Dass die plattformseitig vorgegebenen Limitierungen nicht zwingend mit den Interessen der Diensteanbieter identisch sein müssen, zeigt dieses Beispiel ebenfalls. Gleichzeitig sind derartige Limitierungen auf vertraglicher Ebene oder oberflächliche Kontrollen der von den App-Entwicklern dargelegten Verarbeitungszwecke leicht zu umgehen, was die divergierenden Anbieterinteressen zu einem Problem werden lassen kann, wie das Beispiel um Amazon zeigt. Konsequenzen für vorgabenwidrig handelnde Anbieter drohen daher erst, etwa in Form von einem Ausschluss aus der Plattform, wenn ihre Handlungen publik werden.

Flankiert werden rein vertragliche und vollzugsbedürftige Vorgaben daher durch teils selbstvollziehbare und damit stärker wirkende Limitierungen, die auch auf technischer Ebene die der Verarbeitung zugrundeliegenden Parameter dessen, was wie und unter welchen Umständen möglich ist, regulieren, und bestimmtes Verhalten unter Umständen faktisch verunmöglichen. Dabei kann das Ausmaß stark variieren. Die Vorgaben können bereits auf Ebene der zu verwendenden Programmiersprachen und Codebibliotheken beginnen und setzen sich bei den Schnittstellen zum Datenzugriff fort. Hier kann der Plattformbetreiber je nach Regulierungsgrad der Plattform unterschiedlich detailliert und restriktiv darüber entscheiden, wovon der Zugriff auf welche Datenkategorie in welchen Szenarien abhängt. Grob lässt sich hier unterscheiden zwischen Schnittstellen, die von keinerlei Berechtigung abhängen und von Apps frei genutzt werden können; Schnittstellen, die von der Genehmigung des Plattformbetreibers abhängen, welche wiederum bspw. von einem Glaubhaftmachen der le-

[61] Siehe hierzu Apples AppStore Review Guidelines (https://developer.apple.com/app-store/review/guidelines/), die unter Abschnitt 1.1. unter anderem pornografisches Material verbieten. Zuletzt abgerufen am 14.01.2022. Die Subsumtion konkreter Apps unter diesen Begriff durch die Reviewer sorgt zuweilen für Diskussionen, vgl. *Eaton* u. a., MIS Quarterly 2015, 217 (228).

gitimen und mit der Nutzung der App zusammenhängenden Verwendung der Daten oder von dem Vorlegen geeigneter Garantien der zweckkonformen Verwendung abhängig gemacht werden kann; sowie Schnittstellen, die von der Erteilung einer Einwilligung des jeweiligen App-Nutzers abhängig gemacht werden – wobei auch hier unterschiedliche Gestaltungsmöglichkeiten hinsichtlich der Art und Weise der Nutzerinformation und des Designs der Einwilligungsabfrage infrage kommen oder ggf. beides auf Systemebene von der Plattform selbst übernommen werden kann.

Betrachtet man etwa das obige Beispiel des Cambridge Analytica-Skandals, der sich auf der Plattform des sozialen Netzwerks von Facebook abspielte, zeigt sich eine Form der Ausgestaltung der Verarbeitungsbedingungen, die sich in expliziten Nutzungsvereinbarungen, deren Einhaltung kaum überprüfbar waren, erschöpfte. Facebook hatte die App This is Your Digital Life in sein App Center aufgenommen und die Möglichkeit zur Erhebung von Nutzerdaten unter der Prämisse zugelassen, dass die Daten zu wissenschaftlichen Zwecken oder der Verbesserung der Nutzererfahrung verarbeitet und nicht an Dritte weitergegeben werden würden – Limitierungen, die von den App-Entwicklern nicht eingehalten wurden.[62] Die Plausibilität dieser Verarbeitungszwecke wurde dabei nicht tiefergehend infrage gestellt und deckte sich vordergründig mit den tatsächlichen Funktionen der App – dem Beantworten mehrerer Quizfragen zur Erstellung eines psychologisch fundierten Persönlichkeitsprofils.[63] Zusätzliche Erkenntnis schafft hier ein Blick auf die Entwicklung der relevanten Schnittstelle, die Facebook den Entwicklern unabhängiger Apps für den Zugriff auf Nutzerdaten zur Verfügung stellt: War diese sog. Graph API nach ihrer Einführung 2010 noch nahezu komplett offen und ließ den Zugang zu Nutzerdaten auf Anfrage der App-Entwickler ohne nennenswerte Pflicht zur Darlegung der Gründe zu, wurde sie 2014 – nicht zuletzt begründet durch Bedenken bzgl. Datenschutz und Privatheit der Nutzer – durch eine sehr viel restriktivere Version 2.0 ersetzt,

[62] „What happened here was a breach of the developer's agreement with FB – not some kind of security breach or hacking. GSR did more with the data than the TOS permitted – both in terms of keeping it around and in terms of sharing it with CA. […] This is a story about an ecosystem full of privacy risk, and the inevitable abuse that resulted." Aus dem Interview mit *Daphne Keller* auf Legal Aggregate vom 20.03.2018 (https://law.stanford.edu/2018/03/20/data-analytic-companies-app-developers-facebooks-role-data-misuse/). Siehe außerdem *Carole Cadwalladr & Emma Graham-Harrison*, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian vom 17.03.2018 (https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election): „Facebook's ‚platform policy' allowed only collection of friends' data to improve user experience in the app and barred it being sold on or used for advertising." Beide zuletzt abgerufen am 14.01.2022.

[63] Tiefergehende Hintergründe zu der App und seinen Entwicklern und Geldgebern finden sich bei *Matthew Rosenberg, Nicolas Confessore & Carole Cadwalladr*, How Trump Consultants Exploited the Facebook Data of Millions, The New York Times vom 17.03.2018 (https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html). Zuletzt abgerufen am 14.01.2022.

die den Schutz der Nutzer stärker in den Vordergrund stellen sollte.[64] Die im Cambridge Analytica-Skandal relevanten Nutzerdaten wurden – auch wenn der Skandal selbst erst 2018 publik wurde – bereits 2014, also vor Inkrafttreten der neuen, restriktiveren API, erhoben. Nichtsdestotrotz wurden auch im Nachgang des Skandals zahlreiche weitere Restriktionen, etwa bzgl. der Erhebung von Daten durch sehr lange nicht genutzte Apps und bzgl. der konkreten Daten, die standardmäßig freigegeben werden, eingeführt.[65]

Das Beispiel und die nachfolgenden Reaktionen durch Facebook zeigen auf, wie unterschiedliche Design- und Ausgestaltungsentscheidungen eines Plattformbetreibers die Umstände und Möglichkeiten der Datenverarbeitungen durch Diensteanbieter auf einer Plattform bedingen können. Zwar lässt sich, selbst technisch, kaum beeinflussen, was mit den betreffenden Daten passiert, sobald sie eine Plattform verlassen haben – der eigentliche Skandal im eben beschriebenen Fall lag schließlich in der Weitergabe der Daten an Cambridge Analytica, nicht in der initialen Erhebung durch die Quiz-App –, doch können zumindest der Umfang und die Auswahl der Daten limitiert und auch die Wahrscheinlichkeit abrede- und zweckwidriger Weitergaben und Weiterverwendungen verringert werden, indem etwa strengere Kontrollen durchgeführt, Garantien eingefordert oder Vertragsstrafen eingeführt werden. Teilweise werden auch jetzt schon, allerdings meist nur im Einzelfall und reaktiv mit Blick auf publik gewordenes Fehlverhalten einzelner Dienste, Konsequenzen in Form von bspw. Ausschlüssen aus der jeweiligen Plattform gezogen.[66] Hier gibt die typische Machtverteilung – klassischerweise ist ein einzelner Dienst mit Blick unter anderem auf Netzwerkeffekte stärker von einer Plattform abhängig als die Plattform vom jeweiligen Dienst – Plattformbetreibern daher grundsätzlich einige Möglichkeiten an die Hand. Diese können dabei auch übers Ziel hinaus schießen und ihrerseits negative Folgewirkungen entfalten. So soll etwa im Facebook-Beispiel nicht unerwähnt bleiben, dass die eben erwähnten Res-

---

[64] Eine gute Darstellung der Entwicklung des Graph API findet sich bei *Jonathan Albright*, The Graph API: Key Points in the Facebook and Cambridge Analytica Debacle, Medium vom 21.03.2018 (https://medium.com/tow-center/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747). Zuletzt abgerufen am 14.01.2022.

[65] Siehe die Mitteilung von Facebook vom 04.04.2018 (https://about.fb.com/news/2018/04/restricting-data-access/) sowie den Post von *Mark Zuckerberg* auf Facebook vom 21.03.2018 (https://www.facebook.com/zuck/posts/10104712037900071): „For example, we will remove developers' access to your data if you haven't used their app in 3 months. We will reduce the data you give an app when you sign in – to only your name, profile photo, and email address. We'll require developers to not only get approval but also sign a contract in order to ask anyone for access to their posts or other private data." Beide Links zuletzt abgerufen am 14.01.2022.

[66] So schließt etwa Apple in unregelmäßigen Abständen Apps, die erwiesen schädigendes Verhalten an den Tag gelegt haben, aus dem AppStore aus. Siehe bspw. *Luke Dormehl*, Apple removes Mac apps which are stealing user data, Cult of Mac vom 10.09.2018 (https://www.cultofmac.com/574257/apple-removes-mac-apps-which-are-stealing-user-data). Zuletzt abgerufen am 14.01.2022.

triktionen im Nachgang des Cambridge Analytica-Skandals auch die Möglichkeit der – grundsätzlich vollkommen legitimen – wissenschaftlichen Nutzung (etwa im Bereich der Psychologie oder Soziologie) erheblich einschränkten.[67] Hinzu treten die Auswirkungen, die bestimmte Ausgestaltungsentscheidungen auf die Selbstschutzmöglichkeiten der einzelnen Nutzer haben: Das Opt-out-Modell und die versteckte Platzierung bzgl. des gewährten Zugriffs auf Daten von Nichtnutzern der App, die mit App-Nutzern befreundet waren, legte den Grundstein für das erreichte Ausmaß abgerufener Daten.

Auch in scheinbar simplen Konstellationen der Verarbeitung von Daten eines Nutzers durch den von ihm genutzten Dienst bewegen sich also beide Akteure in vielen Fällen auf einer Plattform und tritt daher der Plattformbetreiber in positiver wie negativer Hinsicht als zusätzlich in den Blick zu nehmender Akteur dazu.

2. Verarbeitungen durch Drittparteien

Von zunehmender Bedeutung sind daneben Verarbeitungen durch Drittparteien, die üblicherweise durch erkennbar auf einer Plattform aktive Diensteanbieter Einzug in die Plattform finden. Der technisch am weitesten verbreitete Weg ist der des Einbezugs fremden Codes über sogenannte SDKs. Dabei stellt die Drittpartei vorgefertigten Code zur Verfügung, den ein Diensteanbieter nur noch in seine App implementieren muss. Wie zu Beginn dieses Kapitels anhand einiger Untersuchungen gezeigt wurde, kommt heutzutage keine Smartphone-App, in der Regel aber auch keine Website, ohne die Nutzung fremden Codes aus. Die Gründe dafür können funktionaler Natur sein, indem etablierte Standards und Funktionen, die der Öffentlichkeit zur Verfügung gestellt werden, genutzt werden sollen, oder indem Nutzungsstatistiken zum Zwecke des Troubleshootings und der Überprüfung des eigenen Dienstes an ein entsprechendes Unternehmen weitergegeben werden. Nicht immer geht damit die Möglichkeit der Drittpartei, Nutzerdaten zu erheben, einher. In den meisten Fällen aber liegt genau darin der Zweck. Besonders prägnant an dieser Art des Einbezugs ist, dass mit ihr regelmäßig dieselbe Zugriffsberechtigung auf Nutzerdaten einhergeht, die dem einbeziehenden Dienst selbst zusteht bzw. vom Plattformbetreiber eingeräumt wurde. Gleichzeitig sind die Möglichkeiten des Diensteanbieters, die von ihm einbezogene Drittpartei hinsichtlich der Wahrnehmung dieser Berechtigungen zu kontrollieren oder solche Handlungen überhaupt wahrzunehmen, sehr be-

[67] Siehe hierzu *Robbie Gonzalez*, Facebook's New Data Restrictions Will Handcuff Even Honest Researchers, Wired vom 22.03.2018 (https://www.wired.com/story/fb-data-restrictions-hobble-researchers/). Zu den eingeschränkten Bedingungen, unter denen der Zugriff zwischenzeitlich erlaubt wurde siehe zudem *Jeffrey Mervis*, Researchers finally get access to data on Facebook's role in political discourse, Science Magazine vom 13.02.2020 (https://www.sciencemag.org/news/2020/02/researchers-finally-get-access-data-facebook-s-role-political-discourse). Beide zuletzt abgerufen am 14.01.2022.

grenzt. Hinzu tritt die Tatsache, dass die Existenz und die einzelnen Identitäten einbezogener Drittparteien für die Nutzer der jeweiligen Dienste regelmäßig kaum bis gar nicht sichtbar sind. Zwar klären Diensteanbieter sie ggf. in ihren Datenschutzerklärungen – teilweise detailliert, in vielen Fällen jedoch nur sehr rudimentär und ohne die einzelnen Drittparteien beim Namen zu nennen – über die Tatsache des Einbezugs auf, doch geht eine solche Information in ohnehin schon sehr unübersichtlichen und ausufernden[68] sowie in den seltensten Fällen gelesenen[69] Datenschutzerklärungen tendenziell eher unter bzw. führt dazu, dass letztlich dutzende Datenschutzerklärungen gelesen werden müssten, um die Verarbeitungsabsichten aller involvierten Drittparteien zu erkennen[70].

Ein sehr symptomatisches Beispiel für eine solche Konstellation ist der oben bereits kurz beschriebene Fall um die unter Apples iOS-Plattform laufende Wetter-App AccuWeather. Ihr Betreiber hatte, wie ein Sicherheitsforscher bei der Analyse der Datenströme herausfand,[71] unter anderem ein SDK des auf Standortdaten spezialisierten Marketing- und Analytics-Unternehmens Reveal Mobile in die App implementiert, um damit bei der Nutzung der App anfallende personenbezogene Daten augenscheinlich bewusst zu Monetarisierungszwecken abrufen zu lassen.[72] Der – jedenfalls nach Maßgabe des Sicherheitsforschers sowie der berichtenden Medien[73] – eigentliche Skandal fußte dabei auf zweierlei Missverhältnissen. Einerseits durfte Reveal Mobile vereinbarungsgemäß nur solche Daten erheben, deren Erhebung auch der App selbst, durch den Nutzer via Einwilligung oder durch Apple via Genehmigung der entsprechenden Schnittstellennutzung, erlaubt war. Nichtsdestotrotz versuchte die Drittpartei, Stand-

---

[68] Vgl. die Untersuchungen bei *McDonald/Cranor*, I/S: A Journal of Law and Policy for the Information Society, 543; erhellend auch die Erkenntnisse bei *Moran* u. a., Literatin, die die Lesbarkeit von Datenschutzerklärungen und anderen Bedingungen mit der von literarischen Texten vergleichen.

[69] Siehe schon *Vila* u. a., in: Camp/Lewis, Economics of information security, S. 143 (143 ff.).

[70] Vgl. die Analyse der erwähnten Drittparteien und ihrer Datenschutzerklärungen im Zusammenhang mit der Plattform eBay *Kurtz* u. a., Design Goals for Consent at Scale in Digital Service Ecosystems, S. 5 ff.

[71] Vgl. *Will Strafach*, Advisory: AccuWeather iOS app sends location information to data monetization firm, Hackernoon vom 22.08.2017 (https://hackernoon.com/advisory-accuweather-ios-app-sends-location-information-to-data-monetization-firm-83327c6a4870). Zuletzt abgerufen am 14.01.2022.

[72] Siehe etwa *Marvin Strathmann*, Beliebte Wetter-App spioniert iPhone-Nutzer aus, SZ vom 25.08.2017 (https://www.sueddeutsche.de/digital/accuweather-beliebte-wetter-app-spioniert-iphone-nutzer-aus-1.3640431) und *Angela Fritz*, A security researcher discovered AccuWeather app tracked, shared your location – even if you ‚opt out', The Washington Post vom 24.08.2017 (https://www.washingtonpost.com/news/capital-weather-gang/wp/2017/08/23/security-researcher-discovered-accuweather-app-tracks-and-shares-your-location-even-if-you-opt-out/). Beide zuletzt abgerufen am 14.01.2022.

[73] Vgl. *Carlos Ribas*, The AccuWeather/Reveal Situation Is Really An iOS Privacy Problem, Medium vom 25.08.2017 (https://medium.com/@carlosribas/the-accuweather-reveal-situation-is-really-an-ios-privacy-problem-78e85a6f8539) Zuletzt abgerufen am 14.01.2022.

ortdaten der App-Nutzer auch dann zu erheben, wenn Nutzer die entsprechende Abfrage der App bzw. des Betriebssystems[74] explizit abgelehnt hatten. Gelingen konnte dies, andererseits, nur deshalb, weil Apple zu diesem Zeitpunkt bei einer durch den Nutzer verweigerten Einwilligung in die Standortdatennutzung zwar den technischen Zugriff auf die Schnittstelle für GPS-Daten verweigerte, gleichzeitig aber die separate Schnittstelle zum Zugriff auf sog. Netzwerkdaten offen und genehmigungsfrei ließ.[75] Über jene Schnittstelle erhob Reveal Mobile die BSSID-Daten[76] der Router, mit denen App-Nutzer verbunden waren.[77] Diese konnten durch Abgleich mit öffentlich im Internet abrufbaren Listen auf konkrete Standorte zurückgeführt werden,[78] sodass die Drittpartei durch geringen Mehraufwand Zugriff auf vergleichbar präzise Standortdaten der Nutzer erlangen konnte.[79] Im Nachgang der medialen Berichterstattung über den Fall zogen sowohl AccuWeather als auch Apple Konsequenzen: erstere dadurch, dass sie die Nutzung des Reveal Mobile SDK beendeten. Zweitere dadurch, dass sie die von der Drittpartei genutzte Schnittstelle zum Zugriff auf Netzwerkdaten vorerst gänzlich schlossen und später großflächig überarbeiteten und gemeinsam mit anderen Datenkategorien unter der CoreLocation API ebenfalls von der Berechtigung der Nutzer abhängig machten.[80] Ähnliche Problematiken wurden auch unter Googles Android-Plattform bereits bekannt.[81]

---

[74] Sowohl unter Android als auch unter iOS wird das Berechtigungsmanagement vom Betriebssystem übernommen, sodass eine Berechtigung für eine bestimmte App global gesteuert und die Ausgestaltung der Abfrage vom Betriebssystem entschieden wird. Siehe hierzu etwa die *Human Interface Guidelines* von Apple für App-Entwickler hinsichtlich Berechtigungsabfragen (https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/). Zuletzt abgerufen am 14.01.2022.

[75] Vgl. *Carlos Ribas*, The AccuWeather/Reveal Situation Is Really An iOS Privacy Problem, Medium vom 25.08.2017 (https://medium.com/@carlosribas/the-accuweather-reveal-situation-is-really-an-ios-privacy-problem-78e85a6f8539). Zuletzt abgerufen am 14.01.2022.

[76] BSSIDs sind einzigartige und eindeutige Ziffernfolgen zur Identifizierung von WLAN-Zugangspunkten wie Routern, Repeatern und Access Points.

[77] Für eine detaillierte technische Rekonstruktion dieser Zugriffe siehe *Schulz* u. a., in: Leenes/Hallinan/Gutwirth/de Hert, Data protection and privacy: data protection and democracy, S. 145 (148, 157 f.).

[78] Siehe, um nur einige beispielhafte Datenbanken zu nennen, das offene Projekt Radiocells (https://www.radiocells.org/) oder https://wigle.net/. Hintergrund solcher – grundsätzlich legitimen – Datenbanken ist etwa das Zusammenstellen von Informationen über öffentliche Netzwerke, das Verbessern der Navigationsgenauigkeit innerhalb von Räumen oder die Ermöglichung von wissenschaftlichen Untersuchungen.

[79] Siehe hierzu einmal mehr die Details in der Beschreibung des ähnlich gelagerten Falls um InMobi, vgl. *Nithan Sannappa & Lorrie Cranor*, Tech@FTC vom 09.08.2016 (https://www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement). Zuletzt abgerufen am 14.01.2022.

[80] Siehe zum heutigen Stand die entsprechenden Entwicklerhinweise von Apple zu der API (https://developer.apple.com/documentation/corelocation/). Zuletzt abgerufen am 14.01.2022.

[81] Siehe etwa *Alepis/Patsakis*, There's Wally! Location Tracking in Android without Permissions, S. 278 ff.; *Achara* u. a., WifiLeaks: underestimated privacy implications of the access_wifi_state android permission, S. 231 ff.

Hier zeigen sich zunächst die begrenzten Einflussmöglichkeiten, die Diensteanbieter, die sich für den Einbezug bestimmter Drittanbieter entschieden haben, bei der Kontrolle dieser Drittanbieter haben. Der vorherrschende Standard, über den Drittparteien – insbesondere bei Smartphone-Apps, in ähnlicher Form aber letztlich bei jeglichen plattformintegrierten Apps – in Dienste einbezogen werden, erhebt diese Drittparteien auf technischer Ebene zu gleichberechtigten Bestandteilen der jeweiligen Apps. Gleichzeitig muss konstatiert werden, dass ein App-Betrieb ohne Drittanbieter faktisch nicht mehr möglich ist, sei es aus funktionalen oder aus Gründen zu breit etablierter Geschäftsmodelle. Wie der Fall aber ebenfalls zeigt, kommen auch hier – wenn auch in begrenztem Ausmaß – die systemweiten Einflussmöglichkeiten zum Tragen, die Plattformbetreibern sowohl präventiv als auch reaktiv zur Verfügung stehen. Zwar stehen diese nicht unmittelbar mit den Drittanbietern in Kontakt und bestehen auch keinerlei vertragliche Verbindungen zwischen den beiden Akteuren, doch wirken sich Gestaltungsentscheidungen hinsichtlich technischer Zugriffsmöglichkeiten naturgemäß auf diese gleichermaßen aus wie auf die eigentlichen Diensteanbieter. Kontrolliert ein Plattformbetreiber einen Diensteanbieter vor dessen Aufnahme auf die Plattform mit Blick auf seine Vereinbarkeit mit den Plattformvorgaben, könnte er diese Kontrolle grundsätzlich in gewissem Ausmaß auch auf die einbezogenen Drittparteien erweitern.

Für Nutzer sind Verarbeitungen dieser Kategorie ungleich schwieriger zu überblicken als solche, die unmittelbar durch Diensteanbieter vorgenommen werden. Mit Blick auf die Anzahl durchschnittlich einbezogener Drittparteien kann die Nutzung eines einzelnen Dienstes, dessen Verarbeitungen erwartet werden, schnell ein Vielfaches an zusätzlichen Verarbeitungen durch Drittanbieter auslösen.

3. Verarbeitungen durch Plattformbetreiber

Als dritte Kategorie können solche Verarbeitungen betrachtet werden, die auf einer Plattform vom Plattformbetreiber selbst vorgenommen werden. Auch hier scheint, ähnlich wie bei der ersten Kategorie, zunächst eine simple Konstellation eines Datenverarbeiters auf der einen Seite und eines betroffenen Nutzers auf der anderen Seite vorzuliegen. Mag dies auch teilweise der Fall sein, kommen doch einige Szenarien in Betracht, in denen auch mehrschichtige Beiträge zur Verarbeitung vorliegen. Insbesondere können Diensteanbieter oder andere Plattformnutzer dazu beitragen, dass Nutzer ein bestimmtes Verhalten an den Tag legen oder einen Dienst des Plattformbetreibers nutzen und damit die infolge des Verhaltens oder der Nutzung angefallenen Datenverarbeitungen mit herbeiführen. Teilweise verschwimmen dabei die Grenzen zwischen Plattformnutzern und Diensteanbietern – der Begriff des *Prosumer* soll dieses Phänomen beschreiben.[82]

[82] Siehe zu dem Begriff *Meller-Hannich* u. a., VuR 2019, 403 (403): „Prosumer befinden

Ein prominentes Beispiel für eine solche Konstellation ist der der EuGH-Entscheidung Wirtschaftsakademie[83] zugrundeliegende Fall, der später noch ausführlich rechtlich beleuchtet werden soll.[84] Dabei ging es um die datenschutzrechtliche Beurteilung von Datenverarbeitungen, die Facebook auf der eigenen Website, aber im Rahmen einer dort eingerichteten Fanpage, vorgenommen hatte. Fanpages sind besondere Arten von Profilen auf der Plattform, die Unternehmen, Vereine, Selbstständige, aber auch Privatpersonen einrichten und nutzen können, um ihre Dienstleistungen, Produkte, Interessen oder anderweitigen Inhalte zu präsentieren und bewerben. Im Unterschied zu herkömmlichen privaten Profilen können sie dann etwa Werbung für ihre Page oder bestimmte Inhalte schalten oder von Facebook zusammengestellte aggregierte Statistiken über die Besucher der Seite einsehen. Die den letztgenannten Besucherstatistiken zugrundeliegenden Datenverarbeitungen waren Gegenstand des EuGH-Urteils. Der Gerichtshof konstatierte, die Betreiber einer Fanpage seien regelmäßig deshalb gemeinsam mit Facebook datenschutzrechtlich verantwortlich für diese Verarbeitungen – die Facebook zusätzlich zu den angefertigten Statistiken auch zu weitergehenden eigenen Zwecken vornahm –, weil sie die Besucher zum Aufrufen ihrer Fanpage animierten und damit den Anlass für die dabei konkret anfallenden Datenverarbeitungen setzten und zudem von den erstellten Statistiken unmittelbar profitierten.[85] Dies gelte in besonderem Ausmaße für Besucher, die selbst keine Mitglieder des sozialen Netzwerks sind und deshalb – ggf. ohne es (rechtzeitig) zu bemerken – von außerhalb auf die Plattform geführt werden. Im Ergebnis stellte der EuGH damit ein Ausmaß an Einflussmöglichkeiten fest, das es seiner Ansicht nach rechtfertigte, den einzelnen Betreiber einer Fanpage in die Verantwortung zu nehmen.

Das Beispiel zeigt, dass auch in Fällen von auf Plattformen stattfindenden Datenverarbeitungen durch die jeweiligen Plattformbetreiber zusätzliche Akteure in den Blick genommen werden können und sollten, die Einfluss auf das Zustandekommen und ggf. das Ausmaß der jeweiligen Verarbeitungen ausüben. Sowohl andere Plattformnutzer als auch Diensteanbieter können das Verhalten betreffender Nutzer so auslösen oder beeinflussen, dass daraus unmittelbare Auswirkungen auf konkrete Verarbeitungsvorgänge eines Plattformbetreibers erwachsen. Man denke etwa an ein mobiles Spiel wie Pokémon Go, das Smartphone-Nutzer zu überdurchschnittlich viel Bewegung und aktivierter GPS-

sich oft auf der Schwelle zwischen privater und gewerblicher Aktivität […].“ Schon vor über 10 Jahren beschrieb *Zittrain*, Harv. L. Rev. 2006, 1974 (1974 ff.) dieses Phänomen und die einhergehenden Gefahren für unter anderem den Schutz der Privatsphäre unter dem Begriff des generativen Internets.

[83] EuGH Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388.

[84] Siehe dazu die Ausführungen in Kapitel 2 C. II.

[85] EuGH Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 35 f.

Funktion animiert und Google oder Apple dadurch ein Vielfaches an individuellen Standortdaten und Bewegungsmustern verschafft.

Zwar ist der diesen Akteuren zukommende Einfluss ungleich geringer als der in den beiden bereits erörterten Kategorien und beschränkt sich häufig, wie im EuGH-Urteil, auf die binäre Frage des Ermöglichens oder Nichtermöglichens einer Verarbeitung, doch kann er in bestimmten Fällen dennoch ein beachtenswertes Ausmaß erreichen – so etwa dann, wenn durch das entsprechende Handeln bisherige Externe neu auf die Plattform gelenkt werden.

II. Verarbeitungen außerhalb von Plattformen

Daneben kommen weitere multipolare Verarbeitungsszenarien in Betracht, die sich außerhalb von Plattformen abspielen. Hier könnte zwar eingeräumt werden, dass sich mit entsprechend weiter Auslegung der Definition jeder Raum, in dem sich ein Dienst befindet, als Plattform verstehen ließe und dementsprechend jede Datenverarbeitung im Rahmen eines digitalen Dienstes auch auf einer Plattform stattfindet. Ein solch weites Verständnis von Plattformen wäre aber wenig zielführend und würde letztlich jeden Versuch einer Systematik zunichtemachen. Bleibt man bei der oben beschriebenen Definition, bedarf es eines kontrollierten digitalen Raumes, in dem sich Diensteanbieter und Nutzer im Rahmen der Nutzung der unter Zuhilfenahme der plattformeigenen Ressourcen entwickelten Dienste treffen und nach den vom Plattformbetreiber aufgestellten und kontrollierten Regeln handeln.[86] Es kommen demnach weiterhin Dienste und Verarbeitungen in Betracht, die außerhalb solcher Plattformen stattfinden. Als wichtigstes Beispiel stellen sich hier klassische Websites dar.[87]

Geht man also von der Prämisse aus, dass in solchen Szenarien der Diensteanbieter selbst, also bspw. der Betreiber einer Website, in der Regel die Entscheidungen und Einflussfaktoren, die auf Plattformen dem Plattformbetreiber obliegen, in sich vereinte, könnten Szenarien, in denen Daten nur durch die Diensteanbieter selbst verarbeitet werden, für den Zweck dieser Untersuchung außer Betracht gelassen werden. Die Komplexität der beteiligten Akteure erschöpfte sich dann tatsächlich in dem klassischen Dualismus aus Verarbeiter und betroffenem Nutzer. Der Normalfall besteht jedoch auch hier in der Realwelt nicht aus solch simplen Konstellationen, sondern, ähnlich wie oben beschrieben auf Plattformen, aus dem Einbezug einer Vielzahl von Drittanbietern. Im Vergleich zu Apps und anderen Diensten auf Plattformen ist hier zudem festzustellen, dass in ähnlichem, wenn nicht gar noch stärkerem Maße grund-

---

[86] Vgl. *Tiwana* u. a., Information Systems Research 2010, 675 (676).

[87] Dass auch diese bei entsprechender Auslegung oder Anpassung der Definition als im Rahmen einer Plattform – etwa einem Browser, Betriebssystem oder gemieteten Server – laufend angesehen werden könnten, bestätigt die eben gemachte These. Richtigerweise erfüllt keines dieser Beispiele die hier gewählte Definition.

legende Funktionen und für den Grundbetrieb einer Website nötige Bestandteile an Dritte ausgelagert werden. Ein Beispiel dafür sind Content-Management-Systeme (CMS) wie Wordpress, die von Websitebetreibern genutzt werden, um die auf der Website anzuzeigenden Inhalte zu erstellen, bearbeiten und organisieren.

Eine Sonderkategorie von Drittanbietern stellen Plattformbetreiber dar, deren plattformeigene Dienste außerhalb der Plattform in andere Dienste einbezogen werden. Ihr Einbezug unterscheidet sich technisch nicht von dem anderer Drittanbieter, es treten aber auf Seite der Motivation der so handelnden Diensteanbieter genuin plattformspezifische Gründe hinzu: Die auf einer Plattform selbst wirkenden Netzwerkeffekte, die Diensteanbietern eine enorme Reichweite und einen immensen Pool potenzieller Nutzer versprechen, kommen in etwas abgewandelter Form auch hier zur Anwendung. Ein gutes Beispiel dafür sind sog. *social login*- oder *single sign-on*-Funktionen, die Anbieter auf ihre Website oder in ihre App einbeziehen und mittels derer Nutzer ihren bestehenden Account bei Facebook, Google oder anderen großen Plattformen nutzen können, um sich anzumelden. Dies verringert die Transaktionskosten für Nutzer immens – sie müssen keinen neuen Account anlegen, dessen Login-Daten sie sich merken müssten – und macht den betreffenden Dienst so attraktiver, gibt ggf. sogar den Ausschlag gegenüber einem Konkurrenzdienst, bei dem ein neuer Account nötig wäre. Gleichzeitig bietet sich Nutzern der Mehrwert, sehr leicht eigene Kontakte wiederzufinden, die den entsprechenden Dienst ebenfalls nutzen, was insbesondere bei Online-Spielen oder anderen speziell auf Nutzerinteraktion ausgerichteten Diensten einen großen Faktor darstellt. Diensteanbieter erhalten zudem regelmäßig[88] die bei der jeweiligen Plattform gespeicherten Profildaten der Nutzer – teilweise solche, die für die Nutzung der Dienste notwendig sind, teilweise aber auch darüberhinausgehende demografische Nutzerdaten. Im Gegenzug erhält die das *social login* bereitstellende Plattform Zugriff auf die bei der Nutzung des Dienstes anfallenden Daten der einzelnen Nutzer.[89]

Ähnlich gestaltet es sich bei sog. *social plugins*, die typischerweise auf Websites eingebunden werden und auf die Werbepräsenz des Anbieters auf der jeweiligen Plattform verweisen. Hier stehen für den Nutzer weniger Funktionalität und Komfort als vielmehr die Möglichkeit, seine Käufe oder genutzten Dienste einfach mit Kontakten auf der jeweiligen Plattform zu teilen. Für den so handelnden Diensteanbieter bedeutet dies eine größere Werbereichweite, für

[88] Bewusst auf Datensparsamkeit ausgelegte Modelle gibt es nur sehr vereinzelt, so etwa das erst kürzlich explizit als Gegenmodell vorgestellte Konzept von Apple. Siehe *Lily Hay Newman*, ‚Sign In With Apple' Protects You in Ways Google and Facebook Don't, Wired vom 06.04.2019 (https://www.wired.com/story/sign-in-with-apple-sso-google-facebook/). Zuletzt abgerufen am 14.01.2022. Gleichwohl bleibt auch hier die Problematik des verstärkten Bindens an einen Plattformbetreiber bestehen.

[89] Einen guten Überblick über Funktionsweise und datenschutzrechtliche Problempunkte am Beispiel des *social login* von Facebook bietet *Moser-Knierim*, ZD 2013, 263 (263 ff.).

die einbezogene Plattform einmal mehr eine zusätzliche Quelle für Besucherdaten, die leicht mit Profilen bestehender oder (noch) nicht existierender Plattformnutzer zusammengeführt werden können. Ein praxisrelevantes Beispiel für ein solches Szenario stellt der dem EuGH-Urteil Fashion ID[90] zugrundeliegende Fall dar. Hier hatte ein Modeunternehmen auf seiner Website das SDK des sog. Gefällt mir-Buttons von Facebook eingebunden. Dieses stellte einen Rahmen auf der Website des Unternehmens bereit, in dem Inhalte der Facebook-Seite des Unternehmens dargestellt wurden und Besucher der Website diese Facebookseite mit „Gefällt mir" markieren konnten. Ebenfalls wurde eine Vorschau von Facebook-Nutzern angezeigt, denen die Seite bereits gefiel, darunter auch Freunde der jeweiligen Websitebesucher, sofern diese die Option aktiviert hatten, in ihrem Browser dauerhaft bei Facebook eingeloggt zu sein.[91] In diesem Fall betonte der EuGH neben der offensichtlichen Einflusssphäre Facebooks zusätzlich den Einfluss, den der Websitebetreiber dadurch ausübe, dass er freiwillig und im Bewusstsein um die damit einhergehenden Folgen das Plugin einbinde und die Verarbeitung der Daten seiner Besucher erst ermögliche. Dieser Einfluss genügte dem EuGH, um neben Facebook auch dem Websitenbetreiber datenschutzrechtliche Verantwortlichkeit für die Verarbeitung der Besucherdaten zuzuschreiben.[92]

Derartige *social plugins* zeichnen sich einerseits dadurch aus, dass sie für den Websitebesucher sichtbar sind, dieser also leicht bemerkt, dass er auf eine von ihm ggf. nicht erwartete dritte Partei trifft. Andererseits übermitteln sie, sofern nicht explizit anders konfiguriert, Besucherdaten bereits von Beginn an und somit unabhängig vom Eintritt des Besucherwissens und ohne dessen Möglichkeit zur Intervention, an den jeweils eingebunden Plattformbetreiber. Technisch geschieht dies über das Setzen eines sog. Cookies als Datei auf dem Endgerät des Websitebesuchers.[93] Ähnlich gestaltet es sich bei der Einbindung von kompletten Inhalten wie Youtube-Videos.[94]

Noch intransparenter stellen sich andere Features dar, die Plattformen Websitebetreibern zur Verfügung stellen und deren Existenz und Funktionalität den Besuchern ohne aktive Aufklärung gar nicht offenbar wird. Der Facebook Pixel, der im oben erwähnten „Datenleck" des Bayerischen Roten Kreuzes aktiv war, ist ein gutes Beispiel. Unternehmen und andere Akteure, die ein Werbe-Konto bei Facebook betreiben, können diesen kleinen Code-Schnipsel auf ihrer Web-

---

[90] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629.

[91] Siehe hierzu die technischen Erläuterungen bei LG Düsseldorf, Urt. v. 09.03.2016, Az. 12 O 151/15, in: MMR 2016, 328 (328).

[92] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 84. Für eine ausführliche Abhandlung des Urteils siehe Kapitel 2 C. II.

[93] Vgl. *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 36 Rn. 131 f.

[94] *Vgl. Conrad/Hausen,* in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 36 Rn. 298 f.

site einbinden, um ihre Besucher und Kunden seiten- und geräteübergreifend zu tracken und damit den Erfolg ihrer Werbekampagnen präziser analysieren zu lassen.[95] So können etwa Verhaltensketten einzelner Kunden lückenlos von dem Ersteindruck einer auf Facebook geschalteten Werbung über den Klick auf diese und damit den Verweis auf die eigene Website bis hin zum tatsächlichen Kaufabschluss nachvollzogen werden.[96] Für Facebook selbst bedeutet dies, dass mit zunehmender Integration auf immer mehr Websites letztlich ein nahezu lückenloses Tracking der Bewegung einzelner Nutzer quer durch das gesamte Internet und über Geräte hinweg möglich ist. Durch den Einbezug ist der Pixel ein (für den Besucher unsichtbarer) Teil der Website und empfängt somit all die Besucherdaten, die bereits rein technisch bedingt jede angesteuerte Website erhält – darunter die IP-Adresse und weitere technische Merkmale des genutzten Endgeräts, aber auch die Identität der Website, die der Besucher zuletzt besucht hatte und die, die er als nächstes von der betreffenden Website aus besucht.[97] Diese Daten – darunter etwa der genutzte Internetbrowser und das Betriebssystem sowie die Bildschirmauflösung – dienen in erster Linie der geräteangepassten und korrekten Darstellung der Websiteinhalte, können aber durch die häufig einzigarte Gesamtkombination aller Merkmale[98] auch zur Identifikation des digitalen Fingerabdrucks (sog. Fingerprinting) des jeweiligen Besuchers genutzt werden.[99] Pixel dieser Art werden nicht nur von Facebook, sondern ebenso auch von anderen Plattformen zur Verfügung gestellt.[100] Solange sie eine große Reichweite haben und im Idealfall ein eigenes Werbenetzwerk anbieten können, besteht in der Regel ausreichend Anreiz für Websitebetreiber, das Angebot zu nutzen.

Ebenfalls im Rahmen dieser Kategorie genannt werden kann Google Analytics, ein Tool, das Google Websitebetreibern zur Analyse des Besucherverhaltens auf Basis von Besucherdaten anbietet und das im größten Teil der weltweiten Websites zu finden ist.[101] Wenngleich hier bei entsprechend umfangreich

---

[95] Vgl. *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 36 Rn. 129 f.

[96] Siehe die instruktive Beschreibung des Vorgangs bei *BayLDA*, ZD-Aktuell 2017, 05805.

[97] Diese Daten dienen in erster Linie der geräteangepassten korrekten Darstellung der Websiteinhalte, können aber durch die häufig einzigarte Gesamtkombination aller Merkmale auch zur Identifikation des jeweiligen Besuchers genutzt werden.

[98] Einer Studie der *Electronic Frontier Foundation* aus 2010 zufolge haben ca. 84 % aller genutzten Webbrowser einen einzigartigen digitalen Fingerabdruck (siehe https://www.eff.org/deeplinks/2010/05/every-browser-unique-results-fom-panopticlick). Zuletzt abgerufen am 14.01.2022).

[99] Siehe die Erläuterungen von *Conrad/Hausen*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 36 Rn. 125 ff. sowie die Studienergebnisse bei *Acar* u. a., The Web Never Forgets, S. 677 ff.

[100] Hier lässt sich beispielhaft der Twitter Pixel (https://business.twitter.com/de/help/campaign-measurement-and-analytics/conversion-tracking-for-websites.html) oder das LinkedIN Insight Tag (https://business.linkedin.com/de-de/marketing-solutions/insight-tag) erwähnen. Links zuletzt abgerufen am 14.01.2022.

[101] Selbst konservative Messungen gehen hier von einer Verbreitung von über 50 % aus.

angepasster Konfigurierung eine größtmögliche Pseudonymisierung und damit ein datenschutzkonformer Einsatz zumindest denkbar ist,[102] werden standardmäßig zahlreiche Nutzerdaten an Google übertragen, um konkrete Nutzer und ihr Verhalten so über Websites hinweg nachzuverfolgen.[103]

Gemein haben all die genannten Beispiele, dass die Erhebung der Nutzerdaten unmittelbar durch die eingebundenen Plattformbetreiber beim Besucher vonstattengeht, der Websitebetreiber also nicht als Mittelsmann zur Weitergabe benötigt wird.

B. Bedeutung und Analyse

I. Der Kontrollverlust der Diensteanbieter und der Kontrollzuwachs von Plattformen

Die beschriebenen Fälle geben einen ersten Aufschluss darüber, in welche Rollen sich die Vielzahl an Akteuren im Bereich digitaler Services bzw. Dienste typischerweise aufteilen lässt. Zudem zeigen sie, welche charakteristischen Verhaltensweisen mit den einzelnen Rollen korrespondieren, aber auch welche Handlungsräume sich diesen Rollen bieten und durch wen diese Handlungsräume geschaffen und ausgestaltet werden.

Eine erste große Erkenntnis ist die, dass mit der Existenz und der Beteiligung einer Vielzahl an Akteuren an einem einzigen Service eine Zerfaserung auf mehreren Ebenen einhergeht. Einerseits eine Zerfaserung von Beiträgen: Jeder, inklusive dem Diensteanbieter selbst, leistet einen mehr oder weniger geringen Teil zum großen Ganzen des angebotenen Dienstes; damit einhergehend aber auch eine Zerfaserung an Souveränität und Kontrolle, denn wenn viele jeweils geringe Beiträge leisten, schwindet unausweichlich das Ausmaß der jeweils eigenen Kontrollmöglichkeiten. Besonders schwer wiegt dies für den Diensteanbieter selbst, der, jedenfalls im klassischen Verhältnis zum Nutzer seines Dienstes, immer noch die zentrale Rolle einnimmt – er bzw. sein Dienst wurde aktiv und bewusst ausgesucht, mit ihm sollte ggf. kontrahiert werden. Vergleicht man diese Erkenntnis mit dem grundlegenden Ansatz der datenschutzrechtlichen Verantwortlichkeit, der bei der Verantwortlichkeitsallokation an die Möglichkeit eines Akteurs zur Kontrolle über Zwecke und Mittel eines Akts oder mehrerer verbundener Akte von Datenverarbeitungen anknüpft, liegt der Schluss

---

Siehe etwa die Ergebnisse von W3Techs (https://w3techs.com/technologies/overview/traffic_analysis). Zuletzt abgerufen am 14.01.2022.

[102] Siehe dazu *Diercks*, DSB 2020, 41 (43); strengere Anforderungen stellend aber *Datenschutzkonferenz (DSK)*, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich.

[103] Vgl. zu den technischen Hintergründen *Mayer/Mitchell*, Third-Party Web Tracking, S. 413 ff.

nahe, dass mit der beschriebenen Zerfaserung von Einfluss- und Kontrollmöglichkeiten auch eine gewisse Diffusion von Verantwortlichkeit einhergeht. Anstelle eines einzelnen Diensteanbieters, der für den Nutzer erkennbar im Rahmen von dessen Benutzung des Dienstes Daten verarbeitet und die Kontrolle darüber vollständig in den Händen hält, diffundiert die Kontrolle und damit auch die potenzielle Verantwortlichkeit nunmehr zwischen mehreren Akteuren. Der Diensteanbieter selbst könnte, so die Befürchtung, die normativ in ihn gesetzten Erwartungen in Sachen Einflussnahme nicht mehr eigenständig erfüllen. Ähnliches könnte für den Endnutzer gelten, der einen Dienst nutzt und dessen ihn betreffenden Daten in diesem Zusammenhang verarbeitet werden. Auch ihm gegenüber löst die Akteurspluralität einen Verlust von Kontrolle und Souveränität aus. Um zu überblicken, welche Datenverarbeitungen mit der Nutzung eines Dienstes einhergehen, kann er dies nicht (mehr) abschließend auf Basis seines Eindrucks vom Diensteanbieter selbst tun, sondern muss idealerweise die – teils für ihn bei der Nutzung sichtbaren, teils unsichtbaren – Drittparteien und ihre Möglichkeiten in seine Beurteilung einbeziehen. Hierfür ist er wiederum auf die Informationen des Diensteanbieters angewiesen, die dieser ihm – idealerweise nach seinem besten Wissen – übermittelt. Sind diese Informationen nun aufgrund des angesprochenen Kontrollverlusts des Diensteanbieters unvollständig bzw. entsprechen schlicht nicht den tatsächlichen Möglichkeiten und Praktiken des Drittanbieters, setzt sich dieser Kontrollverlust kaskadenartig fort und potenziert sich auf der Ebene des Endnutzers.

Der nächste Erkenntnisschritt ist der, dass Plattformbetreiber und die von ihnen betriebenen Plattformen in diesem von Zerfaserung geprägten Ökosystem eine herausragende Bedeutung genießen. Zwar verteilt sich die von den unabhängigen Diensteanbietern abgegebene Souveränität zunächst nicht nur auf die beteiligten Plattformbetreiber, sondern auch auf die zahlreichen beteiligten unabhängigen Drittanbieter. Wo sich aber alle übrigen Rollen durch eine nur auf ihren konkreten Einbezug begrenzte Kontrolle auszeichnen, ist der Einfluss der Plattformbetreiber ungleich größer. Kaum ein Szenario ist vorstellbar, in dem sie nicht in der einen oder anderen Rolle beteiligt sind. In vielen Fällen stellen sie die digitalen Räume bereit, auf denen Dienste angeboten und, damit zusammenhängend, Daten verarbeitet werden. Teils sind sie Betreiber eines solchen Raumes und Datenverarbeiter in einer Person, teils teilen sie die von ihnen in ihrem Raum erhobenen Daten aktiv und bewusst mit Dritten. In anderen Fällen sind sie selbst abseits ihres eigenen digitalen Raums präsent, weil sie in unabhängige Dienste einbezogen wurden und dadurch auch dort eine unmittelbare Verbindung zu ihrem Raum herstellen können – nehmen damit also selbst die Rolle eines Drittanbieters ein. Im Gegensatz zu klassischen Drittanbietern, denen Diensteanbieter im Austausch für Funktionalität, Funktionsanalysen, Nutzerkomfort oder Geld einen Teil ihrer Souveränität über ihren eigenen Raum (in Form der App oder des Dienstes) abgeben, ist der Souverä-

nitätsgewinn von Plattformbetreibern größer und grundlegender. Sie können – wie unabhängige Drittanbieter – datenverarbeitungserhebliche Handlungen über die einzelnen Dienste ausüben, bestimmen aber andersherum auch über die Handlungsoptionen sowohl der Dienste als auch der Drittanbieter. Sie definieren nicht nur die einzelnen Schnittstellen und die Bedingungen, unter denen sie genutzt werden können, sondern letztlich auch die möglichen Geschäftsmodelle und Zwecke, die von Diensteanbietern und Drittparteien verfolgt werden können. Selbst abseits der eigenen Plattform, als eigenständige Drittpartei in einem fremden Dienst, unterscheiden sie sich durch die angesprochenen Phänomene der Marktmacht und der indirekten Netzwerkeffekte von herkömmlichen Drittparteien – weil die sie einbeziehenden Diensteanbieter in der Regel bereits selbst Nutzer der Plattform sind und außerdem wissen, dass insbesondere *social login*-Angebote die Attraktivität des Dienstes für Endnutzer immens steigern. Auch gegenüber Endnutzern nehmen sie, je nach Ausmaß der Integration, eine gesteigerte Rolle ein, die dem unmittelbaren Diensteanbieter Konkurrenz machen kann. Sie informieren über dessen Angebot, machen den Dienst im Rahmen ihres Vertriebskanals überhaupt erst sichtbar und übernehmen die Abwicklung der Zahlung eines etwaigen Kaufpreises sowie ggf. des Managements von Einwilligungen in bestimmte Datenzugriffe durch den Dienst.

Betrachtet man daher die einzelnen Ebenen, auf denen der Kontrollverlust der Diensteanbieter im Dreieck Plattformbetreiber – Diensteanbieter – Drittpartei sich zeitigt, lässt sich grob nach der Nähe der jeweiligen Kontrolle zu konkreten Akten von Datenverarbeitungen unterscheiden. Beim Einbezug von Drittparteien wird diesen die unmittelbare Möglichkeit zur Verarbeitung von Daten eingeräumt, während der Diensteanbieter damit auch die Kontrolle über die tatsächliche Ausübung dieser Möglichkeit aus den Händen gibt. Es besteht daher ein unmittelbarer Zusammenhang zwischen der Kontrollübertragung und der Einflussnahme auf Datenverarbeitungen – auch wenn der Kontrollverlust sich freilich nicht auf datenverarbeitungserhebliche Aspekte beschränkt, sondern auch die generelle Funktionstüchtigkeit eines Dienstes erfassen kann.[104] Anders gestaltet es sich bei den Plattformbetreibern. Indem Diensteanbieter sich auf einer Plattform positionieren und ihren Service dort anbieten, um unter anderem das dort vorherrschende Vermarktungspotential und die große Nutzerbasis ausnutzen zu können, ordnen sie sich bei der Ausgestaltung, teilweise gar schon bei der initialen Ausrichtung ihres Dienstes den Vorgaben des Plattform-

[104] So sorgte erst kürzlich eine serverseitige Veränderung bei Facebook dafür, dass das in zahlreiche der wichtigsten iOS-Apps implementierte *social login*-SDK von Facebook die betroffenen Apps zum Abstürzen brachte – unabhängig davon, ob die Nutzer die Apps mit ihrem Facebook-Account nutzten oder nicht. Siehe *Jay Peters*, Spotify, TikTok, and other popular iOS apps were crashing due to a Facebook issue, The Verge vom 06.05.2020 (https://www.theverge.com/2020/5/6/21250023/Facebook-sdk-login-spotify-tinder-tiktok-ios-iphone-crash). Zuletzt abgerufen am 14.01.2022.

betreibers unter. Ist der Zutritt zu einer Plattform, wie im Falle von Android und iOS für Smartphone-Apps gegeben, unabdingbar für einen Diensteanbieter, so richtet er seine Bemühungen und Ideen bei der Konzeption und Entwicklung nach den dortigen Limitierungen und Voraussetzungen aus. Je nachdem, welche Zugriffskanäle und Schnittstellen für Datenzugriffe eine Plattform kennt und von welchen Bedingungen der Zugriff auf sie abhängig gemacht wird, sind bestimmte Typen von Daten für einen Diensteanbieter erreichbar oder nicht. Der hier angesiedelte Kontrollverlust existiert daher auf einer anderen, etwas vorgelagerten Ebene. Der Bezug zwischen der Kontrolle und konkreten Datenverarbeitungen ist auch hier gegeben, aber ungleich lockerer. Dafür ist die von Plattformen ausgeübte Kontrolle tiefgreifender und breitflächiger, erfasst sie doch über die Handlungsräume der Diensteanbieter mittelbar auch die der von diesen einbezogenen Drittanbieter.

Aufgrund dieser herausgehobenen Stellung von Plattformen und Plattformbetreibern und ihren Kontrollmöglichkeiten soll nun ein vertiefter Blick darauf geworfen werden, auf welche Art und Weise Plattformen ihre Kontrolle ausüben und nach welchen Dynamiken die zugrundeliegenden Regeln zustande kommen und durchgesetzt werden. Schließlich sind sie es, die mit Blick auf die festgestellte Zerfaserung von Kontrolle und die Bedeutung ebenjener Kontrolle für den Datenschutz eine etwaige Diffusion von Verantwortlichkeit durch ihre grundlegenden Kontrollmöglichkeiten kompensieren könnten.

II. Die faktischen Regeln des Zusammenspiels von Akteuren auf Plattformen

Plattformen nehmen also eine grundlegende Bedeutung für die Verarbeitung von Daten im Rahmen der von Akteurspluralität geprägten digitalen Dienstleistungen für sich in Anspruch. Zu fragen ist nun zum besseren Verständnis dieser Bedeutung zweierlei: Nach welchen Logiken und Dynamiken gießen Plattformen ihre Kontrollmöglichkeiten in Regeln, die von Diensteanbietern und Nutzern beachtet werden müssen, und nach welcher Maßgabe entwickeln sich diese Regeln mit der Zeit weiter? Und wie setzen Plattformbetreiber diese Regeln auf ihrer Plattform durch bzw. kontrollieren ihre Einhaltung? Für die erste Frage ist ein Blick auf das Geschäfts- und Anreizmodell von Plattformen nötig, für die zweite Frage eine Betrachtung der verschiedenen Ebenen, auf denen Plattformen ihre Kontrolle ausüben.

1. Das Entstehen und die Entwicklung von Regeln und Kontrolle

Bleibt man bei dem Bild einer Plattform als digitalem Raum, in dem der Plattformbetreiber eigene Dienste für Endnutzer anbietet (die sich in dem Anbieten des Raums und dem Zusammenbringen der dort aufeinandertreffenden Nut-

zer erschöpfen oder darüber hinausgehende eigenständige Dienste beinhalten können), den er aber auch unabhängigen Diensteanbietern zur Verfügung stellt, damit diese mit den Endnutzern zusammengebracht werden und durch ihre mithilfe der vom Plattformanbieter bereitgestellten Ressourcen entwickelten Angebote gleichzeitig die Attraktivität der Plattform steigern, so erscheint logisch, dass in einem solchen Raum Regeln herrschen, die das Verhalten der in ihm aktiven Akteure und insbesondere der Diensteanbieter ordnen: „To manage and motivate these external relations, platforms must have rules that promote healthy participant interactions."[105]

Aus einem wirtschafts- und wirtschaftsinformatikwissenschaftlichen Blickwinkel betrachtet ist diese plattformeigene Governance,[106] also die Genese, Komposition und Wirkung der verschiedenen betreibergenerierten, aber von allen Akteuren mitbeeinflussten Regeln auf einer Plattform,[107] in erster Linie geprägt durch zwei konkurrierende Motivationen.

Einerseits liegt der Anreiz zum Betrieb einer solchen auf externe Beiträge fokussierten digitalen Plattform zu einem Großteil darin, durch Kooperation mit unabhängigen, „dritten"[108] bzw. betreiberfernen Entwicklern ein Mehr an Innovationen und Kreativität zu erreichen, das durch betreiberinterne Entwicklung nicht, nicht so schnell oder nur mit größerem Aufwand zu erreichen wäre. Gerade bei Plattformen, die breite Marktsegmente und Nischen ansprechen, können so externe Wissensressourcen nutzbar gemacht werden, die beim Betreiber selbst nicht ohne weiteres vorliegen würden.[109] Auch kann so schneller auf ge-

---

[105] *Parker/Van Alstyne*, in: Augier/Teece, The Palgrave encyclopedia of strategic management, S. 1290 (1291).

[106] In Abgrenzung zur der Governance von Plattformen, also der staatlichen Einflussnahme darauf, wie Plattformen ihre Macht ausüben. Zu dem Zusammenspiel beider Ebenen siehe *Gorwa*, Information, Communication & Society 2019, 854 (856 ff.); grundlegend hierzu *Dijck* u. a., The platform society, S. 137 ff.; *Helberger* u. a., The Information Society 2018, 1 (1 ff.).

[107] *Tiwana* u. a., Information Systems Research 2010, 675 (679): „We define platform governance as who makes what decisions about a platform." Siehe auch *Nieborg/Poell*, New Media & Society 2018, 4275 (4285): „Such standards are operationalized through platform policies, codified in Terms of Service, Terms of Use, and developer guidelines […]." Die hier in den Blick genommenen Wirkungen solcher Standards und Regeln auf Diensteanbieter und Drittparteien liegen dabei klassischerweise nicht im Fokus der Betrachtungen. Stattdessen beschäftigt sich die Forschung zuvorderst mit den Konsequenzen für Endnutzer und insbesondere deren Kommunikationsverhalten. Vgl. dazu *Klonick*, Harv. L. Rev. 2018, 1599 (1599 ff.); siehe auch *Gillespie*, Social Media + Society 2015, 205630511558047 (2): „Recognizing that social media platforms shape the social dynamics that depend on them allows us to draw connections between the design (technical, economic, and political) of platforms and the contours of the public discourse they host."

[108] Die Forschung spricht hier gerne von Drittparteien bzw. Third Parties, vgl. *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources. Im Kontext dieser Arbeit ist hingegen von Diensteanbietern die Rede, da der Begriff der Drittpartei die von diesen einbezogenen, nicht unmittelbar auf der Plattform aktiven Akteure meint.

[109] Vgl. *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 4; siehe zudem *Yoo* u. a., Information Systems Research 2010, 724

wandelte und neuartige Trends reagiert werden, als dies bei internen Entwicklern der Fall wäre.[110] Je heterogener die angezogenen Entwickler und deren Wissensressourcen, desto generativer und somit konkurrenzfähiger die betreffende Plattform.[111] Um dies zu gewährleisten und kreative und innovationsfördernde Entwickler anzuziehen, werden diesen die grundlegenden Ressourcen und Werkzeuge zur Entwicklung bereitgestellt, wird ihnen aber gleichzeitig auch der Weg zu einem großen, teilweise bereits mit der nötigen Hardware ausgestatteten, Nutzerkreis eröffnet und die Distribution, Bewerbung und Zahlungsabwicklung abgenommen,[112] wird also kurz gesagt dafür gesorgt, dass ihre Transaktionskosten möglichst gering bleiben.[113]

Andererseits hat ein Plattformbetreiber die entgegengesetzte Motivation, ein Mindestmaß an Kontrolle über seine Plattform zu bewahren, die Freiheit der Entwickler also dort einzuschränken, wo es der Gewährleistung seiner generellen Plattformausrichtung, der Wahrung der von ihm verfolgten Ziele, aber auch der Compliance mit rechtlichen Vorgaben dient und drohende Beeinträchtigungen durch konkurrierende Akteure abgewehrt werden müssen. Das Entstehen negativer Externalitäten durch „bösartige" Handlungen von Plattformnutzern soll möglichst verhindert oder zumindest gering gehalten werden.[114]

Die letztendlich auf einer Plattform entstandenen und etablierten Rahmenbedingungen stellen daher notwendigerweise einen – im Idealfall den optimalen – Ausgleich zwischen dem Interesse des Plattformbetreibers an der Wahrung seiner eigenen Vorstellungen hinsichtlich der Ausrichtung seiner Plattform und der Gewährleistung der von ihm verfolgten Werte und Zielrichtungen auf dieser einerseits und den Interessen der Diensteanbieter andererseits dar.[115] Schränkt der Betreiber die Freiheit der Diensteanbieter, insbesondere im Stadium der Entwicklung eines Dienstes, zu sehr ein, beraubt er sich damit der von diesen ausgehenden Kreativität und Innovation, mithin auch ihrer Wertschöpfungspotentiale; zudem läuft er Gefahr, den Diensteanbietern gegenüber an Attraktivität und sie schlimmstenfalls an Konkurrenten zu verlieren (sofern solche vorhanden sind und bessere Bedingungen bzw. größere Freiheit bieten). Hat er einen

(730): „Although it is theoretically possible to pursue such generativity within the closed boundary of a single firm or its existing supplier network, a firm's ability to do so on a practical basis is limited by its economic, structural, cognitive, and institutional constraints."

110 Siehe *Mathiassen/Sørensen*, Journal of Information Technology 2008, 313; vgl. außerdem *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (175) m. w. N.

111 Vgl. *Yoo* u. a., Information Systems Research 2010, 724 (730).

112 Zur Bedeutung und Entwicklung von digitalen Applikationsmarktplätzen, die diese Aufgabe auf Plattformen übernehmen, siehe *Ghazawneh/Henfridsson*, Journal of Information Technology 2015, 198 (199 ff.).

113 Vgl. *Evans*, Berkeley Tech. L. J. 2012, 1201 (1208).

114 Vgl. *Evans*, Berkeley Tech. L. J. 2012, 1201 (1212 ff.).

115 *Tiwana* u. a., Information Systems Research 2010, 675 (676 f.): „[…] governing platforms requires a delicate balance of control by a platform owner and autonomy among independent developers."

erfolgreichen und innovativen Entwickler für sich gewonnen, muss er entscheiden, ob er diesem auch den Weg auf andere Plattformen offenlässt (sog. *multihoming*) oder ihn verpflichtet, exklusiv auf seiner Plattform aktiv zu sein (sog. *single-homing*)[116] – auch hier bringen beide Richtungen ihre jeweiligen Vor- und Nachteile mit sich.[117] Daher priorisieren unterschiedliche Plattformbetreiber die beiden Extreme unterschiedlich stark, legen also mal mehr Wert auf möglichst große Generativität und Innovation, mal mehr auf das Durchsetzen und Beibehalten ihrer klar definierten Vision – sie bewegen sich auf einer Skala zwischen einer eher offenen und eher geschlossenen Plattform.[118]

Ein Modell zur Erforschung dessen, welche Dynamik Plattformbetreiber antreibt, wenn sie versuchen, diesen für sie optimalen Ausgleich bei der initialen Regelsetzung und bei späteren Regeländerungen zu finden, stellt das in der Wirtschaftsinformatik entwickelte Konzept der sog. *boundary resources* dar. Diese, wörtlich übersetzt, Begrenzungsressourcen stellen demnach die Ressourcen dar, die Diensteanbietern den Zutritt auf einer Plattform, die Entwicklung von Angeboten sowie die Ausgestaltung dieser ermöglichen und gleichzeitig begrenzen: „[…] the software tools and regulations that serve as the interface for the arm's-length relationship between the platform owner and the application developer."[119] Das können neben SDKs und APIs[120] bspw. auch Distributionskanäle wie Apples AppStore oder der Prozess der Überprüfung neuer Apps vor der Aufnahme in diesen sein. Der Begriffsteil der „Grenze" ist hier somit doppelt zu verstehen: Die Ressourcen können dem Handeln der Akteure auf der Plattform *Grenzen setzen*, sie können denselben Akteuren aber auch neue Freiheiten zur Auslebung ihrer Kreativität und Geschäftsmodelle geben und damit die *Grenzen* dessen, was das Gesamtangebot der Plattform auszeichnet, *erweitern*.[121]

---

[116] Siehe hierzu *Evans* u. a., Invisible engines: how software platforms drive innovation and transform industries, S. 67 ff.

[117] Der Zwang zur exklusiven Bindung kann Entwickler abschrecken, während das Angebot von Diensten, die auch auf anderen Plattformen zu finden sind, die eigene Einzigartigkeit gegenüber diesen Konkurrenten verschwinden lässt. Vgl. *Parker/Van Alstyne*, in: Augier/Teece, The Palgrave encyclopedia of strategic management, S. 1290 (1293) m. w. N.

[118] So kann etwa ein offener Ansatz gerade für Plattformen sinnvoll sein, die gerade den Markteintritt wagen und darauf angewiesen sind, bestehende Dienste von anderen Plattformen auch für sich zu gewinnen und neuen Entwicklern möglichst viel Freiraum zu lassen, um selbst exklusive und innovative Ergebnisse zu erzielen und so Fuß zu fassen. Vgl. *Parker/Van Alstyne*, in: Augier/Teece, The Palgrave encyclopedia of strategic management, S. 1290 (1293 f.).

[119] *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (174).

[120] Siehe hierzu die ausführlichen technischen Erläuterungen bei *Evans* u. a., Invisible engines: how software platforms drive innovation and transform industries, S. 27 ff.

[121] Neben diesen klassischen, auf das Innere der Plattform gerichteten, Grenzressourcen werden insbesondere im Zusammenhang mit reinen Service-Plattformen ohne Verbindung zu plattformeigenen Geräten auch nach außen gerichtete Ressourcen für die Entwicklung auf externen Geräten und Plattformen diskutiert. Siehe anhand des Beispiels Spotify *Skog* u. a., Digital Service Platform Evolution: How Spotify Leveraged Boundary Resources to Become a Global Leader in Music Streaming, S. 4572 f.

Aus ihrer Gesamtkomposition und Anwendung speist sich die Governance der Plattform durch den Betreiber, und ihre Änderungen auf der Mikroebene haben eine Änderung der Governance auf der Makroebene zur Folge. Die Komposition besteht dabei sowohl aus der Auswahl der verschiedenen Ressourcen als auch aus deren einzelner Gestaltung. Ein gutes Beispiel für die Extreme, zwischen denen eine Plattform sich bei der Auswahl ihrer Ressourcen bewegen kann, kann in den Anfangstagen von iOS als Heimat der Apps für Apples iPhone und später auch iPad gefunden werden. Als grundlegende Ressource für die Entwicklung von Apps bei Einführung des ersten iPhones 2007 wählte Apple den hauseigenen Safari-Browser. Apps mussten somit für den Browser entwickelt werden und auf den eigenen Servern der Entwickler, nicht unmittelbar auf dem Betriebssystem der Geräte, laufen. Grund war ein überwiegendes Interesse daran, so die Gefahr von Viren, Malware und Datenlecks auf den iPhones der Nutzer gering zu halten.[122] Erst nach mehreren Monaten und zahlreicher Kritik von Medien und Entwicklern sowie dem Aufkommen von alternativen, die Limitierungen umgehenden Frameworks in Form von bspw. sog. Jailbreaks für das iPhone schwenkte Apple um und bot ein SDK als neue Ressource zur Entwicklung von nativen iPhone-Apps an, justierte also die Abwägung zwischen Entwicklerfreiheit und Plattformkontrolle um.[123] Ähnliche Nachjustierungen in Richtung einer generellen Öffnung wurden im Laufe der Jahre vorgenommen, indem das SDK mehrfach modernisiert wurde und nach und nach zusätzliche APIs geschaffen wurden, die Apps den Zugriff auf Standortdaten eröffneten oder das Versenden von Push-Benachrichtigungen erlaubten.[124] Gleichzeitig wurde immer wieder auch in Richtung einer stärkeren Kontrolle nachjustiert, indem beispielsweise die von Entwicklern zu akzeptierenden vertraglichen Vereinbarungen angepasst wurden, ein strenger Review-Prozess für die Aufnahme in den AppStore eingeführt wurde,[125] oder der Einbezug von Zwischenplattformen wie Java oder Flash verboten wurde, um einen zu großen Einfluss externer Akteure zu verhindern.[126]

Als gutes Gegenbeispiel für diese Entwicklung dienen Facebook und die auf dieser Plattform laufenden Apps (vormals Widgets). Hier versuchte Facebook von Beginn an, durch eine Strategie weitreichender Freiheit und geringer

---

[122] Vgl. *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 7.

[123] *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (181 ff.).

[124] Siehe hierzu und für eine chronologische Nachzeichnung der Nachjustierungen der Grenzressourcen auf der Plattform bis 2010 *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 179 ff.

[125] Vgl. *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (10 f.).

[126] Diese Entwicklung ging so weit, dass selbst Adobes Entgegenkommen in der Form, Flash-Applikationen automatisiert zu iPhone-Apps konvertieren zu lassen, durch eine weitere Änderung der Entwicklerrichtlinien unterbunden wurde. *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 11 f.

Einstiegshürden Entwicklern und ihren Bedürfnissen entgegenzukommen, um möglichst viele von ihnen anzuziehen und zum Experimentieren zu animieren, während der einzige treibende Faktor eigener Einflussnahme darin bestand, den Entwicklerfokus auf Apps mit möglichst hoher sozialer Interaktion zu legen, um das plattformeigene Geschäftsmodell zu unterstützen.[127]

In generalisierter Form wird daher davon ausgegangen, dass die Governance von digitalen Plattformen durch Plattformbetreiber einem iterativen Prozess mit mehreren Abschnitten folgt, die sich jeweils gegenseitig anstoßen und somit einen fortwährenden Ausgleich zwischen Innovation und Kontrolle darstellen.[128] So folgt auf die Einführung einer neuen oder Veränderung des Designs einer bestehenden *boundary resource* die entsprechend restriktivere (also die Lockerung durch absichernde Kontrolle kompensierende) Änderung der Entwicklerrichtlinien. Auf eine Beobachtung der Auswirkungen auf das Verhalten der Diensteanbieter und die nunmehr verstärkte Innovationskraft und Heterogenität von Wissensressourcen folgt ein weiteres Gegenwirken, um etwaig als übergriffig empfundenen Praktiken, so etwa Versuchen der Integration fremder Ressourcen, entgegenzuwirken. Die Notwendigkeit, neue Ressourcen zu erschaffen oder bestehende zu ändern, kann dabei durch eben solche von außen stammenden Übergriffe auf die verfolgte Integrität der Plattform angestoßen werden,[129] sie kann aber auch Diskussionen, Kritik und Wünschen von Entwicklern oder Medien folgen.[130] Dabei stellen die beteiligten Parteien ein sehr heterogenes Feld dar, kann es also durchaus mächtigere Diensteanbieter und Entwickler geben, die größere Chancen haben, durch ihr Entgegenhalten für Veränderung zu sorgen.[131] Das können etwa andere Plattformbetreiber sein, die ihr Produkt expandieren wollen und ihrerseits eine gewisse Gefolgschaft aufweisen.[132] Maßnahmen der Lockerung und Kontrolle wechseln sich somit ab,

---

[127] Vgl. *Boudreau/Hagiu*, in: Gawer, Platforms, Markets and Innovation, S. 163 (173 f.): „[…] Facebook has adopted a strategy of free access and low barriers to entry for widget developers through various measures, including: open and well-documented application programming interfaces (APIs); support for multible development languages; free tools and test facilities; support for communication among developers within Facebook developer forums and conferences."

[128] Vgl. *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 14: „Using boundary resources as the main mediator, each repeated series of actions involve [sic] both acts for keeping control and for stimulating external contributions."

[129] *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (177).

[130] *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 13; *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (176 f.): „[…] may be anticipated or triggered by feedback from third-party developers."

[131] *Eaton* u. a., MIS Quarterly 2015, 217 (236): „Therefore, a powerful actor who can mobilize technical, financial, and legal resources can sometimes overcome the resistance of an artifact in ways that less powerful actors cannot."

[132] Siehe etwa *Eaton* u. a., MIS Quarterly 2015, 217 (227 f.) zum langjährigen Streit zwischen Apple und Adobe über die Nutzung von Flash unter iOS.

während der Plattformbetreiber, sowohl proaktiv als auch reaktiv, versucht, die für ihn passende Balance zu erreichen und beizubehalten. Das zwischenzeitlich stabilisierte Ergebnis dieses Prozesses ist daher keine unmittelbar und isoliert vom Plattformbetreiber aufgezwungene Regel, sondern weist immer auch ein emergentes Element auf.[133]

Führt man dieses Konzept auf den für diese Arbeit relevanten Fokalpunkt der Verarbeitung personenbezogener Daten und damit auch auf den (End)Nutzer von Plattformen zurück, ist eine interessante Erkenntnis zunächst, dass der Nutzer als Akteur bei dem vom Betreiber vorgenommenen Balanceakt der Governance seiner Plattform nur eine sekundäre Rolle neben dem Diensteanbieter spielt. Gleiches gilt für den Gedanken des Datenschutzes. Dieser kann im Einzelfall mittels des Einfallstors entsprechend ausgerichteter und verfolgter Plattformwerte – so im oben beschriebenen Beispiel um Apple[134] – oder im Rahmen einer generellen (und damit zunächst personenbezugsunabhängigen) Governance des Umgangs mit Daten[135] eine Rolle spielen und so dazu führen, dass im Rahmen des Kontrollgegengewichts auch die Auswirkungen auf Datenschutz und Datensicherheit beachtet und ihnen entgegengewirkt wird. Wenngleich Plattformbetreiber zahlreichen Rechtspflichten unterworfen sind, die sich zumindest auch auf die Governance der Akteure auf ihrer Plattform auswirken,[136] werden solch normative Einflüsse im Rahmen des Konzepts der *boundary resources* bisher nicht dezidiert berücksichtigt.[137]

Nichtsdestotrotz lässt sich schwerlich bestreiten, dass das im Rahmen der Governance der Plattform erfolgte Hin und Her bzgl. Lockerungen und Kon-

---

[133] Vgl. *Eaton* u. a., MIS Quarterly 2015, 217 (236): „[…] the dialectics of resistance and accomodations in the distributed tuning is emergent and situational."

[134] Ein anderes, ebenfalls Apple betreffendes Beispiel ist der zeitweise in den Entwicklerrichtlinien enthaltene Passus, wonach die Nutzung von Standortdaten nur erlaubt war, wenn sie der Funktionsfähigkeit der App und nicht allein standortbasierter Werbung diente. Vgl. *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (183).

[135] Siehe hierzu die ausführliche Literaturanalyse und Fallstudie bei *Lee* u. a., Data Governance Decisions for Platform Ecosystems, S. 6378 ff.

[136] Die aktuellsten und virulentesten Beispiele hierfür sind sicherlich die aus dem NetzDG stammende Pflicht sozialer Netzwerke zur Kontrolle von Nutzerinhalten auf ihre Strafbarkeit sowie die im Zuge der Reform der Urheberrechtsrichtlinie entstandene Pflicht zur präventiven Kontrolle von Nutzerinhalten auf ihre urheberrechtliche Konformität.

[137] Teilweise wird aber jedenfalls der Einfluss von Regulierungsbehörden auf die Evolution von Plattformen konzediert, wenn diese Quasibeiträge in Form von bspw. Genehmigungen leisten. Vgl. *Tiwana* u. a., Information Systems Research 2010, 675 (681). Zudem entstehen in der Literatur teilweise bereits Tendenzen, die ein Zusammenführen (datenschutz-)rechtlicher und wirtschaftsinformatikwissenschaftlicher Perspektiven versuchen und das Konzept der boundary resources um speziell datenschutzrechtliche Elemente erweitern wollen. *Eaton* u. a., MIS Quarterly 2015, 217 (236) berücksichtigen etwa die Möglichkeit von Regulierungsinstanzen, Einfluss auf den Entwicklungsprozess zu nehmen; auch losgelöst vom sehr spezifischen Begriff der boundary resources werden die Möglichkeiten der Ausnutzung plattformspezifischer Dynamiken und Handlungslogiken für den Datenschutz bisweilen zumindest schon gesehen. Vgl. hier etwa *Westerlund/Enkvist*, jipitec 2016, 2 (7 ff.).

trollverschärfungen teilweise unabhängig von entsprechenden Plattformwerten großen Einfluss auf datenverarbeitungsrelevante Handlungen und Handlungsmöglichkeiten der Diensteanbieter hat. Im Lichte zunehmend datengetriebener und datenfinanzierter Dienste ist naheliegend, dass Änderungen und Neueinführungen von *boundary resources* häufig solche Handlungsmöglichkeiten betreffen, die einen engen Bezug zu Datenverarbeitungen aufweisen. Dies gilt mit dem oben Gesagten für beide Treiber hinter der Fortentwicklung von *boundary resources*: Geht diese mit Entwicklerwünschen nach zusätzlichen Möglichkeiten und Freiheiten einher (Ressourcen mit einem Fokus auf das Bereitstellen von Mitteln bzw. die Unterstützung von Diensteanbietern, sog. *resourcing*), wird die Änderung häufig im Zugriff auf neue Datenkategorien oder die Datennutzung zu neuen Zwecken bestehen; stellt die Fortentwicklung hingegen eine Reaktion auf potenziell plattformbeeinträchtigendes Entwicklerhandeln dar (Ressourcen mit einem Fokus auf Steigerung oder Erhalt der eigenen Kontrolle, sog. *securing*), so zeigt die Praxis, dass der schädigende Charakter des infragestehenden Verhaltens jedenfalls in einigen Fällen aus Datenschutzskandalen und anderen datenschutzkritischen Ereignissen bestand. Als Beispiel für die erste Kategorie lassen sich die zahlreichen über die Jahre von Apple eingeführten APIs zum Zugriff auf bspw. die Standortdaten oder Kontaktbücher der Nutzer anführen. Ein gutes Beispiel für die zweite Kategorie stellt Apples Reaktion auf mehrere publik gewordene Skandale (der dazugehörige AccuWeather-Fall wurde oben bereits erörtert[138]) bzgl. des mittelbaren Zugriffs auf Standortdaten über den Umweg der MAC-Adressen verbundener Router dar. Hier justierte Apple in Richtung stärkerer Kontrolle nach und verschloss den entsprechenden Zugriffskanal auf die betreffenden Daten, namentlich die Captive Network API, zeitweise gänzlich.[139] Ähnlich verhält es sich mit den Reaktionen von Facebook auf den Cambridge Analytica-Skandal – auch hier wurden datenschutzrelevante Nachjustierungen an den betreffenden Ressourcen vorgenommen.[140]

Als erste Erkenntnis kann daher festgehalten werden, dass das Ausmaß an Kontrolle, das ein Diensteanbieter, der auf einer Plattform agieren möchte, zugunsten des Plattformbetreibers aufgibt, einem von letzterem stetig vorgenommenen Balanceakt unterliegt, der den zwei großen, widerstreitenden Triebfedern – Sicherung und Erweiterung – folgt. Diensteanbieter genießen auf Plattformen daher grundsätzlich diejenige Freiheit und eigene Kontrolle, die nach Einschätzung des Plattformbetreibers fruchtbar für die Erweiterung, Di-

[138] Später wurde die API durch eine neue, klarer reglementierte ersetzt. Siehe dazu in diesem Kapitel bei A. I. 2. sowie zum heutigen Stand die entsprechenden Entwicklerhinweise von Apple zu der CoreLocation API (https://developer.apple.com/documentation/corelocation/). Zuletzt abgerufen am 14.01.2022.

[139] Siehe *Jeff Butts*, Thanks to Misuse, Apps Can't View MAC Addresses on iOS 11, the Mac Observer vom 22.10.2017 (https://www.macobserver.com/news/product-news/apps-cant-view-mac-addresses-on-ios-11/). Zuletzt abgerufen am 14.01.2022.

[140] Siehe hierzu ausführlich in diesem Kapitel bei A. I. 2.

versifizierung und Vertiefung des Diensteportfolios und damit des Gesamtangebots der Plattform ist. Gleichzeitig genießen sie nur gerade so viel Freiheit, dass es dem Plattformbetreiber noch möglich ist, die volle Souveränität über seine Plattform zu bewahren und seine verfolgte Ausrichtung mitsamt seiner Grundwerte beizubehalten und die Weiterentwicklung der Plattform entsprechend zu steuern. Beteiligt an diesem Prozess sind nicht zuletzt die Diensteanbieter selbst, die durch geäußerte Kritik an der Einführung neuer oder Änderung bestehender Ressourcen, aber auch durch ihr abweichendes Verhalten bei bspw. als überbordend empfundenen Einschränkungen die Evolution der Ressourcen und damit die Governance einer Plattform prägen.[141] Dabei wirken sich sowohl Ressourcen, die die Freiheit der Anbieter erweitern, als auch solche, die die Kontrolle der Plattform steigern bzw. erhalten, oftmals auf den Umgang mit personenbezogenen Daten und somit auf das Schicksal der Nutzer aus, auf die sie sich beziehen.

Die zweite, darauf aufbauende Erkenntnis ist die, dass auch Plattformbetreiber *by design* keine umfassende und unbegrenzte Kontrolle über das Geschehen auf ihren Plattformen und insbesondere die Handlungen und Entwicklungen der einzelnen Diensteanbieter innehaben. Das Überlassen von Freiheiten und Freiräumen ist schließlich ebenso wie das Zurverfügungstellen von Ressourcen und Werkzeugen dem eigenen Geschäftsmodell inhärent und daher gewollt. Im Vergleich zu einem (heutzutage häufig fiktiven) Vor-Plattformmodell eines Plattformbetreibers, in dessen Rahmen er alle Dienste eigenhändig anbot, ist daher ebenso wie bei den einzelnen Diensteanbietern ein gewisses Ausmaß an Kontrollverlust zu konstatieren. Diese Erkenntnis soll das oben gezogene Fazit, wonach Plattformen und ihre Betreiber die zentralen und mächtigsten Akteure innerhalb der Gemengelage der modernen Datenverarbeitungsrealität darstellen, nicht in Zweifel ziehen, sondern mit einem realistischen und detaillierteren Rahmen versehen.

2. Die Art der Durchsetzung von Regeln auf Plattformen

Von Interesse ist deshalb in einem nächsten Schritt, wie und in welcher Effektivität und Effizienz die auf Kontrolle ausgerichteten Ressourcen einer Plattform in der Praxis wirken und durchgesetzt werden. Dabei sollen insbesondere die Ressourcen im Fokus stehen, die einen engen Bezug zu Datenverarbeitungsvorgängen aufweisen. In welchen Bereichen nähern sie sich einer umfassenden Kontrolle an, inwieweit lassen sie sich durch entsprechendes Handeln der Diensteanbieter umgehen? Es geht also um die „formal and informal machan-

[141] *Eaton* u. a., MIS Quarterly 2015, 217 (235 f.) sprechen hier vom Akt des „tunens" von Ressourcen, an dem nicht nur der Plattformbetreiber, sondern auch die anderen, nicht nur auf der Plattform befindlichen Akteure beteiligt sind: „Distributed tuning emerges from ongoing tensions among dispersed heterogeneous actors who deal with a set of technology artifacts in a network of dialectic interrelating […]."

isms implemented by a platform owner to encourage desirable behaviour by module developers".[142]

Hier lässt sich zunächst unterscheiden zwischen einer ersten Ebene in Form einer vertraglichen Kontrollressource, wie sie bspw. Apple und Google bei ihren mobilen Betriebssystemen als Entwicklerrichtlinien definieren, und einer zweiten Ebene in Form von technischen Kontrollressourcen, die die jeweils transportierten Limitierungen gewissermaßen selbst umsetzen, indem das vertraglich eingeschränkte Verhalten auch technisch verunmöglicht oder jedenfalls eingeschränkt wird.

a) Vertragliche Absicherung

Eine bedeutende Kontrollebene stellt die Absicherung durch Verträge und andere Vereinbarungen dar. Diensteanbieter und andere Plattformnutzer unterwerfen sich den Regeln, die Plattformbetreiber in Form von Nutzungsbedingungen, Entwicklerrichtlinien oder anderen Regelsätzen aufstellen, um Zutritt zur Plattform zu erlangen und auf ihr agieren zu dürfen.[143] Die Sicherstellung der Einhaltung dieser vereinbarten und von den Diensteanbietern akzeptierten Regeln wird einerseits bereits durch ihren verbindlichen Charakter als *vertragliche* Vereinbarungen bemüht.[144] Gleichzeitig lebt die Wirksamkeit dieser Kontrollebene davon, dass die verbindlichen Regeln auch auf ihre Einhaltung hin *überprüft* und bei festgestellten Verstößen *durchgesetzt*, also mit entsprechenden Folgen versehen werden.[145] Sie sind daher in großem Maße vollzugsbedürftig.[146]

---

[142] *Tiwana* u. a., Information Systems Research 2010, 675 (680).

[143] *Strahilevitz*, Michigan Law Review 2006, 1838 (1837) unterscheidet hier zwischen vier verschiedenen groben Kategorien des Gebrauchs von Ausschlussregelungen: (1) dem gänzlichen Ausschluss von anderen aus dem eigenen Raum, (2) der selektiven Aufnahme gewollter Akteure und damit dem Ausschluss aller anderen, (3) der Schaffung eines ausschließenden Klimas und Rahmens durch Vermittlung weicher Auswahlkriterien, die für eine homogene Zusammensetzung sorgen sollen, und (4) der Schaffung besonderer exklusiver Vorteile für Akteure, die sich den weichen Vorgaben des Plattformbetreibers anpassen, während alle anderen benachteiligt werden.

[144] Neben diesen verbindlichen Regeln gibt es häufig auch unverbindliche Empfehlungen oder (noch) nicht kontrollierte Ankündigungen späterer Regeländerungen. So kennt Apple etwa das Konzept von veralteten (*deprecated*) APIs und SDKs, die in absehbarer Zeit komplett eingestellt oder ausgetauscht werden. Die Nutzung derart markierter APIs und SDKs wird nicht verboten oder unterbunden, es wird aber von der weiteren Nutzung abgeraten und vor der drohenden Einstellung der Nutzbarkeit gewarnt. Teilweise wird nur die bereits bestehende Nutzung kurzfristig weiter erlaubt, während neu auf die Plattform aufzunehmende Dienste verpflichtet werden, die entsprechenden Schnittstellen nicht zu nutzen. Vgl. *Prassana Aithal*, How to check your application is using any of the deprecated Apple APIs, Mac O' Clock vom 08.05.2020 (https://medium.com/macoclock/how-to-check-your-application-is-using-any-of-the-deprecated-apple-apis-2bf6ea67f47b). Zuletzt abgerufen am 14.01.2022.

[145] Siehe *Evans*, Berkeley Tech. L. J. 2012, 1201 (1206, 1222): „[…] the ability of platforms to enforce rules concerning negative externalities rests on being able to penalize and ultimately exclude members of the community. […] The platform also needs to be able to detect violations for these rules to be meaningful."

Hinsichtlich ihrer Überprüfung kann grob zwischen zwei Zeitpunkten getrennt werden: dem Zeitpunkt der Zulassung zur Plattform und dem nachgelagerten, nach hinten theoretisch unbegrenzten Zeitraum der bereits bestehenden Zulassung auf der Plattform. Sie unterscheiden sich nicht zuletzt darin, wie die vertraglich definierten Regeln kontrolliert und durchgesetzt werden.

Vor der erstmaligen Aufnahme auf die Plattform wird typischerweise die Vereinbarkeit des jeweiligen Dienstes, zum Beispiel einer App, mit den vertraglichen Vereinbarungen überprüft.[147] Die Kontrolldichte kann dabei je nach Strenge des Plattformbetreibers und Offenheit der Plattform[148] unterschiedlich stark ausfallen und von nicht existent über stichprobenartig bis hin zu umfassenden Überprüfungen jedes einzelnen Dienstes reichen.[149] Auch die Bedeutung des Distributionskanals kann variieren: Während etwa der AppStore auf Geräten von Apple die einzige (legale) Möglichkeit ist, als Nutzer Apps zu installieren, lässt Google auf seinem Android-Betriebssystem nicht nur alternative Distributionskanäle zu – einer der bekanntesten dürfte hier der Amazon Appstore oder das auf Transparenz und Datenschutz ausgerichtete F-Droid-Repositorium sein –, sondern erlaubt Nutzern bei Aktivierung der entsprechenden Einstellung auch die manuelle Installation von Apps aus unbekannten Quellen.[150] Nach einer einmal erfolgten Aufnahme auf die Plattform wird, wenn überhaupt, nur in verringertem Maße die andauernde Einhaltung der vereinbarten Regeln überprüft. Eine solche Überprüfung kann etwa bei jedem (ggf. nur jedem größeren) Update des jeweiligen Dienstes, nach fest definierten Zeiträumen oder einmal mehr stichprobenartig ohne bestimmte Regelmäßigkeit erfolgen.

Eine Durchsetzung der Regeln bei festgestelltem Verstoß vollzieht sich dann durch Nichtaufnahme auf die Plattform bzw. nachträgliche Entfernung von die-

---

[146] *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (184) sprechen hier von „control actions that rely on regulative measures."

[147] Vgl. *Tilson* u. a., Change and Control Paradoxes in Mobile Infrastructure Innovation, S. 7 zu den Unterschieden zwischen Android und iOS. Während Apple sehr strenge und klar definierte Entwicklerrichtlinien hat und die Apps für den AppStore beinahe kuratiert, errichtet Google für sein Pendant eher geringe Hürden, was nicht zuletzt an der jeweiligen Anzahl an Apps zu erkennen ist (ca. 3,5 Mio. auf Android und 2,2 Mio. unter iOS nach Stand vom 1. Quartal 2021 (vgl. https://de.statista.com/statistik/daten/studie/208599/umfrage/anzahl-der-apps-in-den-top-app-stores). Zuletzt abgerufen am 14.01.2022.

[148] Siehe *Benlian* u. a., Journal of Information Technology 2015, 209 für den Versuch einer Operationalisierung des Begriffs der Offenheit einer Plattform; für eine Analyse der Bedeutung von Offenheit für das Marktpotential einer Plattform siehe *Ondrus* u. a., Journal of Information Technology 2015, 260 (263 ff.).

[149] Siehe etwa zur Entwicklung dieses Review-Prozesses bei Apples AppStore *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (182 f.); eine generellere Analyse mitsamt Typologie unterschiedlicher Applikationsmarktplätze bieten *Ghazawneh/Henfridsson*, Journal of Information Technology 2015, 198 (201 ff.).

[150] Siehe *Tilson* u. a., Change and Control Paradoxes in Mobile Infrastructure Innovation, S. 6.

ser.[151] Je nach differenzierter Ausgestaltung existieren zudem vorgelagerte mildere Maßnahmen wie Verwarnungen oder Aufforderungen zur Beseitigung des infragestehenden Verstoßes. Flankiert sein kann jede Art von Maßnahme außerdem von weitergehenden Erläuterungen und ggf. Gelegenheiten zur Stellungnahme und Erklärung des regelwidrigen Verhaltens.[152] Fallen, wie bei Android, die Aufnahme in den Distributionskanal und die Aufnahme auf die Plattform nicht zusammen und wird also die Aufnahme auf die Plattform gar nicht oder nur begrenzt kontrolliert, verliert diese Art der Maßnahme an Wirkung, kann aber immer noch merkbare Auswirkungen haben. Ist eine App nicht mehr im offiziellen Distributionskanal und nur noch in alternativen Repositorien (wie dem Amazon AppStore) aufzufinden, die erst installiert werden müssen, verliert sie derart massiv an Wirksamkeit, dass der Effekt dem einer gänzlichen Versagung der Aufnahme auf die Plattform nahe kommt.[153]

Wie oben beschrieben, können sich die vertraglichen Vereinbarungen infolge des stetigen Tunings der jeweiligen Grenzressourcen sehr dynamisch und häufig ändern. Ein bei Aufnahme auf die Plattform mit deren Vereinbarungen konformer Dienst bzw. die von diesem vorgenommenen Datenverarbeitungen kann bzw. können nach einiger Zeit bereits gegen die geänderten Regeln verstoßen. Auch deshalb ist eine einigermaßen effiziente Kontrolle einer Plattform letztlich nur möglich, wenn nicht nur bei Aufnahme, sondern auch nachträglich noch regelmäßig die Einhaltung der Regeln überprüft wird.

Bei der Überprüfung der Einhaltung lässt sich nicht nur hinsichtlich Zeitpunkt, Frequenz und Kontrolldichte, sondern auch hinsichtlich der Art und Weise und, damit zusammenhängend, der Wirksamkeit der Überprüfung differenzieren. Diese hängt zudem davon ab, was genau vertraglich reglementiert wurde. Verbietet etwa Apple in den Richtlinien für den AppStore bestimmte Kategorien von Apps, sind diese im Rahmen einer ersten Sichtung leicht zu identifizieren. Geht es um Inhalte der entsprechenden Dienste, etwa in Form von Nacktheit oder Gewaltdarstellungen, lassen diese sich teilweise mittelbar über die Kategorie und die Funktionalität der Dienste erfassen, müssen aber (insbesondere bei auf nutzergenerierte Inhalte aufbauenden Diensten) in den meisten Fällen genauer untersucht und können häufig erst nach Aufnahme auf die Plattform und tatsächlicher Nutzung durch die Endnutzer ernsthaft kontrolliert werden. Noch schwieriger wird die Überprüfung der Einhaltung bei den hier relevanten Handlungen eines Dienstes mit Datenverarbeitungsbezügen. Prak-

---

[151] Dies entspricht der ersten von *Strahilevitz*, Michigan Law Review 2006, 1838 (1843 ff.) konzipierten Kategorie, dem „*bouncer's right*".

[152] *Evans*, Berkeley Tech. L. J. 2012, 1201 (1222): „And finally, the platform may employ a process in which suspected wrongdoers can plead their cases, or at least convey potentially useful information, and possibly an appeals process."

[153] Diese Ausgestaltungsart entspricht daher der von *Strahilevitz*, Michigan Law Review 2006, 1838 (1858 ff.) beschriebenen vierten Kategorie („*exclusionary amenities*"), die aber der ersten Kategorie („*bouncer's right*") bereits recht nahe kommt.

tisch findet die Überprüfung, insbesondere beim Antrag auf Aufnahme auf eine Plattform, häufig in Form einer Plausibilitätskontrolle statt. Begehrt etwa ein Diensteanbieter für seinen Dienst den Zugang zu bestimmten Kategorien von Nutzerdaten, die den Richtlinien nach nur verfügbar sind, sofern sie primär der Funktionalität einer App dienen, muss er glaubhaft machen können, weshalb diese Daten für den Funktionsumfang seiner App vonnöten sind.[154] Eine weitere, auf einer tieferen Ebene stattfindende Möglichkeit ist die Überprüfung der Code-Basis eines zur Aufnahme eingereichten Dienstes.[155] Hier lässt sich unter anderem bereits ablesen, auf welche Datenflüsse und Verarbeitungen der Dienst zu seiner Funktion angewiesen ist, welche Verarbeitungen vorgenommen werden und welcher Code welcher Drittparteien in den Dienst eingebunden wurde. Eine solche Analyse des Codes kann daher die eben genannte Plausibilitätsprüfung unterstützen, indem sie die von den Diensteanbietern abgegebene Begründung für die geforderte Nutzung begründungspflichtiger Datenkategorien mit den tatsächlichen Funktionalitäten auf Code-Ebene abgleicht und so Fälle von *permission gaps*[156] oder *overprivilege*[157] aufdeckt. Ebenso kann überprüft werden, welche Arten von ggf. ungewollten oder verbotenen Drittparteien in den Dienst eingebunden wurden und an welche Server Nutzerdaten gesendet werden. Werden, wie im Falle von Android und iOS, auch Updates für die Dienste über den jeweiligen Distributionskanal (wie Apples AppStore) verteilt, bietet sich diese Kontrollmethode auch besonders für die kontinuierliche Überprüfung nach erstmaliger Aufnahme des Dienstes an, um zu verhindern, dass nachträglich Änderungen vorgenommen werden, die den Richtlinien widersprechen.

Gleichwohl unterliegt die Überprüfung der Wirksamkeit vertraglicher Kontrollressourcen natürlichen Limitierungen. Wie bereits angeklungen, ist die zukünftige Einhaltung bestimmter Regeln im Vorfeld (also bei ex ante Überprüfung vor Aufnahme in den AppStore oder andere Distributionskanäle) je nach Natur der jeweiligen Regelung nicht ohne weiteres abschätzbar. Zu einem spä-

---

154 Siehe das Beispiel des Apple AppStore bei *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (184).

155 Siehe hierzu etwa Ansätze wie *Singh* u. a., IEEE Access 2019, 6562 (6572 f.); *Nanevski* u. a., Verification of Information Flow and Access Control Policies with Dependent Types, S. 165 ff.; *Li/Zhang*, Towards a Flow- and Path-Sensitive Information Flow Analysis, S. 53 ff.; *Adams* u. a., CLSR 2019, 105337; *Bartel* u. a., Automatically securing permission-based software by reducing the attack surface, S. 274 ff.; *Struse* u. a., in: Paternò/de Ruyter/Markopoulos/Santoro/van Loenen/Luyten, Ambient Intelligence: Proceedings of the Third International Joint Conference, Aml 2012, Pisa, Italy, November 13–15, 2012, S. 65 (65 ff.); *Felt* u. a., Android permissions demystified, S. 627 ff.

156 Mit *Bartel* u. a., Automatically securing permission-based software by reducing the attack surface, S. 274 verstanden als Fälle, in denen eine App mehr Berechtigungen erlangt, als sie tatsächlich benötigt, und so böswilligen Drittanbietern Möglichkeiten für Datenverarbeitungen einräumt.

157 *Felt* u. a., Android permissions demystified, S. 627 verwenden diesen Begriff für dasselbe Phänomen: „Overpriviliged applications expose users to unnecessary permission warnings and increase the impact of a bug or vulnerability."

teren Zeitpunkt wird hingegen – schon allein aus Kapazitätsgründen – meist nur kursorisch geprüft und fallen notwendiger Weise bestimmte Dienste unter den Tisch. Teilweise kann dem durch bewusste Designentscheidungen entgegengewirkt werden, die die generelle Transparenz zwischen den einzelnen Plattformnutzern erhöht und Selbstkorrekturmechanismen aktiviert.[158] Dazu gehört etwa die Möglichkeit für Endnutzer, Diensteanbieter und ihre Dienste zu bewerten, sodass „schwarze Schafe" einerseits leichter identifizierbar und damit von anderen Nutzern aktiv vermieden, andererseits weniger prominent im Distributionskanal beworben und damit seltener gefunden werden.[159] Diese Hoffnungen erfüllen sich freilich nur bei Vorliegen zweier anspruchsvoller Bedingungen: dass die Vorstellungen von Plattformbetreibern und Endnutzern hinsichtlich dessen, was schlechtes bzw. abweichendes Verhalten ausmacht, übereinstimmen; und dass das schlechte Verhalten von Nutzern überhaupt ohne weiteres erkannt werden kann. Benötigt eine App etwa unüblich viele Berechtigungen, die nicht im Zusammenhang mit der Leistung der App stehen – bspw. eine Taschenlampen-App, die Zugriff auf Standortdaten fordert – fällt dies Nutzern zumindest theoretisch schnell auf und schlägt sich in negativen Bewertungen nieder.[160] Der Einbezug vieler Drittparteien, die im Rahmen zunächst nachvollziehbar erscheinender Berechtigungen Daten zu unerwarteten Zwecken (weiter)verarbeiten, ist hingegen kaum erkennbar und beeinflusst somit auch nicht die Bewertungen.

Eine weitere Limitierung betrifft die Reichweite der Wirkung. Speziell hinsichtlich des Umgangs mit Daten kann die oben angesprochene Analyse des Codes eines Dienstes einen wichtigen Einblick bieten, ihre Reichweite endet aber spätestens dort, wo die Daten die Plattforminfrastruktur verlassen. Ob die Vorgaben eines Plattformbetreibers hinsichtlich der von ihm erlaubten Zwecke, zu denen bspw. Standortdaten von Nutzern erhoben werden dürfen, auch eingehalten werden, nachdem diese auf einen Server des Diensteanbieters oder eines von diesem einbezogenen Drittanbieters übermittelt wurden, entzieht sich dessen Kenntnisbereich. Hier zeigt sich: Je grober und breitflächiger eine Limitierung, desto leichter lässt sich auch ihre Befolgung kontrollieren – je ausdifferenzierter und detaillierter, desto schwieriger wird die Kontrolle. Dürfen Diensteanbieter Nutzerdaten nur noch direkt auf dem Endgerät des Nutzers verarbeiten und nicht auf eigene oder dritte Server übertragen werden, ist das rela-

---

158 Vgl. *Evans*, Berkeley Tech. L. J. 2012, 1201 (1226 f.).

159 Die letztgenannten Maßnahmen entsprechen abermals der vierten von *Strahilevitz*, Michigan Law Review 2006, 1838 (1858) beschriebenen Kategorie, den „*exclusionary amenities*", die in Form der erleichterten Auffindbarkeit nur denen zugutekommen, die sich plattformkonform verhalten.

160 Dass dies in der Praxis nicht immer zwingend der Fall ist und häufig keine Korrelation zwischen überdurchschnittlich vielen und besonders sensiblen Berechtigungen einer App und ihrer Bewertung im jeweiligen Distributionskanal besteht, wird in Studien teils gezeigt. Vgl. etwa *Chia* u. a., Is this app safe?, S. 319 f.

tiv einfach festzustellen; ist der Transfer aber grundsätzlich erlaubt, unterliegt jedoch bestimmten Voraussetzungen (etwa bzgl. des Zwecks oder der späteren Weitergabe), kann der Plattformbetreiber letztlich stets nur auf Basis bestimmter, von ihm überprüfbarer Indizien eine Abschätzung vornehmen und so die Wahrscheinlichkeit eines Verstoßes verringern. Ein gewisses Restrisiko und somit auch ein gewisses Vollzugsdefizit bleibt bestehen – insbesondere deshalb, weil Plattformen durch die eingangs beschriebenen widerstreitenden Anreize (Offenheit versus Kontrolle) tendenziell eher zu ausdifferenzierten und detaillierten Limitierungen greifen, um ein übermäßiges Abschneiden des Wertschöpfungspotentials zu verhindern.

b) Technische Absicherung

Eine zusätzliche Ebene der Absicherung, die die vertragliche Ebene komplementiert, kann daher auf technischer Ebene verortet werden. Getreu der Prämisse *code is law*[161] betrifft sie Entscheidungen hinsichtlich der Architektur der Plattform und des Designs der einzelnen Schnittstellen und Zugriffskanäle, die Handlungen der Diensteanbieter technisch verunmöglichen, erschweren oder mit bestimmten Abhängigkeiten versehen und so normative Wirkung entfalten.[162] Im Gegensatz zu Ressourcen vertraglicher Absicherung sind sie daher zu weiten Teilen nicht vollzugsabhängig, sondern zu einem gewissen Grad selbstvollziehend.[163] Verunmöglichen sie bestimmtes Verhalten komplett und sichern damit die Einhaltung ihrer Regeln ab, liegt ein faktischer Totalvollzug dieser Regeln vor – diese Art von handlungsunterbindenden Strukturen ist auch unter dem Begriff der *impossibility structures* bekannt.[164] Insbesondere in Bezug auf datenverarbeitungserhebliche Handlungen wird auf dieser Ebene teils auch das

---

[161] Zurückgehend auf *Lessig*, Code and other laws of cyberspace.

[162] Welche Auswirkungen solche technischen Absicherungen haben können, zeigt das Beispiel des Videospielmarkts, der in den 1980ern infolge einer Überschwemmung der bis dato am weitesten verbreiteten Spielekonsole, der Atari, mit qualitativ minderwertigen Spielen zeitweise brach lag, weil Kunden nicht mehr in der Lage waren, gute von schlechten Spielen zu unterscheiden. Nintendo löste dieses Problem, indem Spiele für die eigene Konsole nur mit einem selbst entwickelten Sicherheitschip spielbar waren, sodass Spiele ohne Genehmigung von Nintendo und damit ohne Qualitätssicherung den Markt faktisch nicht erreichen konnten. Siehe *Boudreau/Hagiu*, in: Gawer, Platforms, Markets and Innovation, S. 163 (163); ausführlich und instruktiv auch die Abhandlung bei *Evans* u. a., Invisible engines: how software platforms drive innovation and transform industries, S. 115 ff.; grundlegend zur regulativen Wirkung von Technologien im Generellen *Leenes*, Legisprudence 2012, 28.

[163] Vgl. *Finck*, Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy, S. 12: „Code is, unlike any other normative systems, self-executing and can govern behaviour easily[…].“ So auch schon *Lessig*, Code and other laws of cyberspace, S. 236 f.; zur normativen Wirkung von Architektur im Generellen; *Murray/Scott*, The Modern Law Review 2002, 491 (503 f.) relativieren diese Aussage, indem sie (zurecht) darauf hinweisen, dass auch Architekturen, einschließlich Code, zunächst von Menschen gestaltet werden müssen, sodass man durchaus auch von vorgelagerter Durchsetzung sprechen könnte.

[164] Siehe hierzu *Rademacher*, JZ 2019, 702 (702 f.).

oben beschriebene Überprüfbarkeitsdefizit auszugleichen versucht. So werden Schwierigkeiten bei der Kontrolle dadurch ausgeglichen, dass bestimmte richtlinienwidrige Verhaltensweisen auf der Plattform technisch schlicht nicht möglich gemacht werden. In diesem Fall sichert die technische Kontrollebene die vertragliche Kontrollebene ab. Beispiele für solche technischen Kontrollressourcen sind insgesamt sehr vielfältig. Da Plattformbetreiber letztlich die gesamte digitale Infrastruktur (sowie teilweise auch die dazugehörige Hardware in Form von Nutzerendgeräten), also die grundlegenden Strukturen, ohne die ein Dienst auf der Plattform weder existieren noch agieren könnte,[165] bereitstellen, hat jede einzelne Ausgestaltungsentscheidung unmittelbar Auswirkungen auf den Möglichkeitsraum der auf der Plattform agierenden Akteure. Selbst einer im Kern freiheitsermöglichenden Ressource, etwa der Schnittstelle zum Abruf bestimmter bisher nicht nutzbarer Sensordaten, liegt meist gleichzeitig auch eine begrenzende Komponente inne. Das betrifft bereits die Ausgestaltung des grundlegenden SDK, das die Entwicklung von Diensten für eine Plattform ermöglicht, ebenso wie die Ausgestaltung eines jeden API. Eine klassische technische Kontrollressource mit nur peripherem Datenverarbeitungsbezug, die vertragliche Regelungen absichert, ist etwa die Verhinderung externer (und damit ohne finanzielle Beteiligung des Plattformbetreibers ablaufender) Käufe und Abonnements für Apps, wenn der Plattformbetreiber selbst einen solchen Dienst mittels seines Distributionskanals anbietet.[166] Ein noch grundlegenderes Beispiel ist die technische Verunmöglichung der Installation externer Apps, wenn die Regel aufgestellt wurde, dass nur überprüfte und in den Distributionskanal aufgenommene Apps auf der Plattform verfügbar sein dürfen – auch hier ist Apples iOS der prägnanteste Fall, während Google auf Android die Möglichkeit nur erschwert, aber explizit zulässt.

Ein Beispiel für eine datenverarbeitungserhebliche Designentscheidung kann demgegenüber etwa darin liegen, dass Plattformbetreiber das Management für Nutzereinwilligungen selbst übernehmen und so die wichtigen Parameter der Ausgestaltung des Einwilligungsprozesses festlegen und den Zugriff auf die betreffenden Daten(-kategorien) ohne erteilte Einwilligung schlicht nicht zulassen, wenn der Zugriff vertraglich von der Nutzereinwilligung abhängig gemacht wird. Mittelbar kann auch das Management von In-App-Käufen und Abonnements datenverarbeitungsrelevante Auswirkungen haben, indem die Diensteanbieter keinen Zugriff auf Konto- und andere Daten der Nutzer erlangen.

---

[165] Frei nach *Tilson* u. a., Change and Control Paradoxes in Mobile Infrastructure Innovation, S. 1: „[…] the constitutive information technologies and organizational structures, along with the related services and facilities necessary for an enterprise or industry to function."

[166] Entsprechende Mechanismen sind sowohl bei iOS als auch bei Android vorhanden. Für einen guten Überblick über die Entwicklungen bei der Kontrolle von Apple über Abonnements, die auch außerhalb der Plattform geschlossen wurden, siehe *Eaton* u. a., MIS Quarterly 2015, 217 (233 ff.).

Denkbar sind im weiteren Sinne aber auch technische Kontrollressourcen, die solche Limitierungen faktisch-implizit zementieren, die nicht bereits explizit in den Entwicklerrichtlinien normiert wurden. Das ist meist dann der Fall, wenn die Limitierungen bereits Teil der freiheitsermöglichenden Ressourcen sind, also letztlich die Grenze einer Erweiterung der Handlungsfreiheit darstellen. Häufig führt das dazu, dass sie eine weniger lange Halbwertszeit haben und eher emergent und ohne bewusste Entscheidungsfindung zustande kommen. Sie stellen daher einen Kontrast zu den vertraglichen Kontrollressourcen dar, die mit dem eingangs dargestellten iterativen Prozess der Genese und Evolution von *boundary resources* meist eine bewusste und gegensteuernde Korrektur auf die ersten Erkenntnisse nach Einführung neuer Freiheiten darstellen.

Weisen technische Kontrollressourcen daher ihrer Art nach eine grundsätzlich bessere Möglichkeit der Durchsetzung als vertragliche Kontrollressourcen auf bzw. helfen häufig dabei, letztgenannte durchzusetzen, so sind auch sie aber nicht frei von Limitierungen.

Zum einen ist jede technische Ressource nur so gut und wirksam wie ihre Entwicklung und die menschlichen Überlegungen, die in ihrem Zusammenhang angestellt wurden. Mit anderen Worten: Eine technische Kontrollressource, die bestimmtes Verhalten oder bestimmte Verhaltensfolgen verunmöglichen oder erschweren soll, bedarf zunächst einer menschlichen Übersetzungsleistung, die die entsprechende Handlung oder die möglichen Folgen möglichst konkret vorhersieht und in Code überträgt. Dabei müssen alle denkbaren Kontexte berücksichtigt und auch abwegige Formen der Nutzung einer Ressource sowie das Zusammenwirken mehrerer Ressourcen mitgedacht werden. Doch nicht jedes Verhalten und jede Folge lässt sich zu hundert Prozent in technische Logiken übersetzen. Und nicht jedes, insbesondere bösartige, Verhalten lässt sich im Vorfeld erahnen und absehen oder überhaupt dauerhaft gänzlich verhindern. Typischer ist daher, entsprechend der eingangs geschilderten Dynamik, die *Nach*justierung von Kontrollressourcen, also eine *nach*trägliche Reaktion auf bereits eingetretenes Handeln, das so nicht vorhergesehen wurde. Schön zu sehen ist das etwa hinsichtlich der oben beschriebenen Kontrolle Apples, nur geprüfte und im AppStore zugelassene Apps auf der Plattform iOS zuzulassen. Hier findet ein regelrechter Wettkampf zwischen Apple und der Nutzercommunity statt, die mittels sog. *Jailbreaks* regelmäßig eine Öffnung des Betriebssystems für einen alternativen AppStore namens Cydia herbeiführt, aus dem auch solche Apps bezogen werden können, die in Apples AppStore nicht zugelassen sind.[167] Hier nutzt die Community Lücken in Apples Betriebssystem, die bei dessen Updates stetig wieder geschlossen werden, um dann früher oder später durch neugefundene Lücken ersetzt zu werden, die wiederum beim darauf-

[167] Vgl. hierzu den aus der Anfangszeit von Cydia stammenden Artikel von *Jenna Wortham*, Unofficial Software Incurs Apple's Wrath, New York Times vom 12.05.2009 (https://www.nytimes.com/2009/05/13/technology/13jailbreak.html). Zuletzt abgerufen am 14.01.2022.

folgenden Update des Betriebssystems geschlossen werden. So ergibt sich ein dauerhaftes Hin und Her – „an ongoing distributed tuning where both parties take turns at asserting their respective goals“[168] – da Apple nicht in der Lage ist, neue *Jailbreaks* dauerhaft zu verhindern. Ein weiteres gutes Beispiel für die limitierte Wirkung einer technischen Kontrollressource ist im oben erläuterten[169] Fall der AccuWeather-App zu betrachten: Weil Apple unter iOS den Zugriff auf Standortdaten für Diensteanbieter nur mit der Zustimmung der Nutzer freigeben wollte, wurde der Zugriff auf alle unmittelbar oder gemeinsam standortbestimmenden Datenquellen (u. a. Wi-Fi, GPS und Bluetooth) gebündelt über eine Schnittstelle (die Core Location API) geregelt und der Zugriff auf die Schnittstelle von der Erteilung der entsprechenden Nutzereinwilligung abhängig gemacht.[170] Dem in die AccuWeather-App integrierten SDK des Unternehmens Reveal Mobile gelang es über einen kleinen Umweg dennoch, an die Standortdaten auch derjenigen Nutzer zu gelangen, die ihre Einwilligung verweigert hatten. Dazu nutzten sie eine andere Schnittstelle (die Captive Network API), die – ohne Berechtigungen zu verlangen – den Zugriff auf Informationen über das mit dem Endgerät verbundene Netzwerk sowie den verwendeten Router erlaubte. Ähnliche Lücken lassen sich auch auf Googles Android-Plattform finden, für die Wissenschaftler zwischenzeitlich belegten, wie fehlende Berechtigungen zum Zugriff auf das Mikrofon eines Nutzergeräts durch die Nutzung des berechtigungsfreien Speech-to-text API (zur Umwandlung der gesprochenen Mikrofoneingaben in Text) umgangen werden konnten.[171]

Hier zeigen sich also zwei Dinge: Die Wirksamkeit der Kontrollkomponente einer Ressource (hier die Core Location API) hängt in starkem Maße davon ab, dass die vom Plattformbetreiber kreierten Kategorien und Kanäle hinsichtlich der verfolgten Kontrollzwecke eine originalgetreue Abbildung der Wirklichkeit darstellen, die denkbaren Handlungen der Diensteanbieter und Nutzer also korrekt ins Technische übertragen; zudem müssen die verschiedenen Ressourcen auch ineinandergreifen und im Zusammenspiel funktionieren, ohne sich zu konterkarieren – die Wirksamkeit einer einzelnen Ressource hängt nicht nur von ihr selbst, sondern auch von ihrer Wirkung im Verhältnis zu den sie umgebenden Ressourcen ab. Geht es also um die Limitierung des Zugriffs auf Daten der Oberkategorie „Standortdaten“, so muss gewährleistet sein, dass dieser Oberkategorie eine hinreichend weite und akkurate Definition davon zugrunde liegt, aus welchen Daten sich Nutzerstandorte entnehmen oder zurückführen lassen. Erfasst eine Kontrollressource (wie hier die *Core Location* API) nicht alle po-

---

168 *Eaton* u. a., MIS Quarterly 2015, 217 (235).

169 Kapitel 1 A. I. 2.

170 Siehe https://developer.apple.com/documentation/corelocation/. Zuletzt abgerufen am 14.01.2022.

171 Vgl. etwa *Alepis/Patsakis*, in: Ali/Danger/Eisenbarth, Security, Privacy, and Applied Cryptography Engineering, S. 53 (61 f.).

tenziellen Standortdaten, so müssen auch die korrespondierenden Ressourcen entsprechend ausgerichtet sein. Zu dieser Erkenntnis kam auch Apple, sodass im Nachgang des AccuWeather-Falls und weiterer problematischer Fälle[172] die Captive Network API zunächst gänzlich verschlossen und später durch eine neue, genauer reglementierte und mit Zugriffsbedingungen versehene CNCopyCurrentNetworkInfo API ersetzt wurde.[173] Eine solche Verteilung der Kontrolle auf verschiedene Ressourcen lässt sich häufig nicht vermeiden, weil Daten unterschiedlichen Nutzungszwecken dienen können, deren Legitimität nicht immer übereinstimmen muss. Der Zugriff auf Daten über das verwendete Netzwerk kann etwa legitimerweise von solchen Apps benötigt werden, die den Status des eigenen WLAN-Netzes diagnostizieren, um weniger benutzte Frequenzen zu empfehlen, oder von solchen, die VPN-Verbindungen zu andere Netzwerken herstellen. Die Nutzung der Daten zur Ermittlung des Nutzerstandorts ist daher nur einer von mehreren denkbaren Nutzungszwecken, sodass die pauschale Eingliederung in den Zugriffskanal der Core Location API dieser Realität nicht hinreichend Rechnung tragen würde. Umso wichtiger ist bei solch differenzierten Kategorisierungen und Quernutzungen, dass die Ausgestaltung der verschiedenen Ressourcen aufeinander abgestimmt ist, da anderenfalls eine Ressource die Wirkung der anderen konterkariert.

Zum anderen ist auch die Wirkung an sich funktionierender, gut übersetzter und in die Gesamtkomposition an Ressourcen eingefügter Kontrollressourcen meist auf das Umfeld der Plattform und ihres Ökosystems begrenzt. Weitergehendes Handeln außerhalb der Plattform entzieht sich daher in der Regel dem Wirkungskreis ihrer Kontrollressourcen. Das zeigt sich sehr anschaulich am Beispiel des Cambridge Analytica-Falls, wo ein großer Teil des Schadens in der zweckwidrigen Weitergabe der erhobenen Nutzerdaten an das Analytics-Unternehmen und dessen Weiterverarbeitung zu Zwecken abseits der offiziell vorgesehenen Forschung lag.

Eine technische Methode, diese plattformexterne Weiterverwendung zu unterbinden, gibt es schlicht nicht.[174] Kontrollressourcen können hier also höchs-

[172] Vgl. etwa den InMobi-Fall. *Nithan Sannappa & Lorrie Cranor*, Tech@FTC vom 09.08.2016 (https://www.ftc.gov/news-events/blogs/techftc/2016/08/deep-dive-mobile-app-location-privacy-following-inmobi-settlement). Zuletzt abgerufen am 14.01.2022.

[173] Siehe https://developer.apple.com/documentation/systemconfiguration/1614126-cncopycurrentnetworkinfo. Voraussetzung für den Zugriff ist nun die erteilte Zustimmung des jeweiligen Nutzers zur Nutzung der Core Location API oder einer der zwei anderen abschließend enumerativ aufgezählten legitimen, die Funktionalität der jeweiligen App betreffenden Zwecke. Link zuletzt abgerufen am 14.01.2022.

[174] Derartige Bemühungen werden etwa im Urheberrecht bei der Kontrolle von Nutzungslizenzen bereits seit längerem angestellt. Mittels Digitalem Rechtemanagement (DRM) soll die Nutzung und Verbreitung von Werken auch noch im Herrschaftsbereich der Nutzer kontrolliert und eingeschränkt werden. Noch älter sind Kopierschutzmechanismen für physische Verkörperungen urheberrechtlich geschützter Werke wie CDs oder DVDs. Auch in diesen Fällen gibt es freilich seit jeher Möglichkeiten der Umgehung. Siehe die Case Study bei *Leenes*,

tens dort anknüpfen, wo sich das jeweilige Handeln noch auf der Plattform abspielt, um bereits hier das Risiko eines späteren Missbrauchs zu verringern.

c) Die Verzahnung der beiden Ebenen

Wie oben bereits angeklungen, bedingen sich die beiden Ebenen in ihren Entwicklungen und Wirkungen gegenseitig. Wird die Handlungsfreiheit der Diensteanbieter auf technischer und faktischer Ebene vergrößert, folgt darauf in vielen Fällen eine Verschärfung der Regeln auf Ebene der vertraglichen Absicherung. Das bedeutet auch, dass die technische Ebene häufig die vertragliche Ebene unterstützt und absichert, indem etwa bestimmte vertraglich verbotene Handlungen technisch schon gar nicht oder nur unter erschwerten Bedingungen möglich gemacht werden; gleichzeitig kann davon ausgegangen werden, dass in den seltensten Fällen eine völlige Kongruenz zwischen den beiden Ebenen besteht, also nicht alles, was vertraglich verboten ist, auch technisch erschwert oder unmöglich gemacht wird. Das liegt zum einen daran, dass nicht alle Handlungen überhaupt der technischen Regulierung offenstehen – man denke hier etwa an vertragliche Regeln zur Weiterverwendung von Daten außerhalb der Plattform –, zum anderen aber insbesondere daran, dass die Nuancen des Erlaubten im Rahmen der Weiterentwicklung einer Plattform eben stetig nachjustiert werden, wobei mit dem oben Beschriebenen das technisch Mögliche dem vertraglich Erlaubten meist einen Schritt voraus ist. Mit anderen Worten: Es ist dem auf Innovation und Wertschöpfung gerichteten Geschäftsmodell digitaler Plattformen gerade inhärent, immer wieder neue Handlungsfreiräume zu schaffen, deren Ausfüllung zunächst ungewiss ist, sodass auch etwaige negative Auswirkungen (für die generelle Souveränität des Plattformbetreibers, aber auch für Endnutzer) nicht im Voraus erahnt werden (können). Zudem drohen, wie oben erwähnt, gerade auch bei übermäßig restriktiver Plattformoffenheit negative Auswirkungen für die Plattform, wenn – wie im Falle des fehlenden SDK zu Anfangszeiten des iPhones – Diensteanbieter und externe Plattformbetreiber die wahrgenommenen Limitierungen durch eigene, in die Plattform eingebrachte Ressourcen zu kompensieren versuchen.[175]

Legisprudence 2012, 28 (161 ff.) Ein vergleichbarer Ansatz scheidet für den Datenschutz mangels eigentumsähnlicher Konzeption sowie aufgrund weitaus komplexerer Abwägungsfragen aus. Grundlegend zum Einsatz technicher Durchsetzungsmechanismen im Urheberrecht *Helberger*, in: Dommering/Asscher, Coding regulation: essays on the normative role of information technology, S. 219; zukünftig wären zudem Ansätze im Bereich der Blockchain ein denkbarer Weg, um über verschiedene Datenverarbeiter und Datentransfers hinweg die Befolgung aufgestellter Limitierungen nachzeichnen und überprüfen zu können.

[175] So etwa zu sehen am Beispiel von Adobes Programmierplattform Flash. Apps, die auf dieser Basis geschrieben waren, waren unter iOS lange Zeit nicht unterstützt, was Adobe dazu brachte, ein Tool zur Konvertierung in iPhone-Apps anzubieten („While Flash applications still would not run on the iPhone, the CS5 simply turned Flash applications into iPhone applications automatically"). Dieses Unterfangen war jedoch nur von kurzem Erfolg gekrönt,

Während somit eine Erkenntnis darin besteht, dass vertragliche Kontrollressourcen häufig technische Kontrollressourcen zur eigenen Absicherung und Durchsetzung brauchen, haben vertragliche Kontrollressourcen in anderen Aspekten ihre eigenen Vorteile. So gilt die oben beschriebene Wirkungslimitierung auf die Plattform selbst für sie nur begrenzt – ein vertraglich vereinbartes Verbot etwa, durch eine App erhobene Daten nur zu Forschungszwecken zu verwenden, hat auch noch Bestand, wenn die infragestehenden Daten sich im Machtbereich des Diensteanbieters oder bereits eines Dritten befinden, und kann prozessual auch durchgesetzt werden. Eine faktische Limitierung bleibt gleichwohl bestehen – vertragswidrige Datenverwendungen müssen zunächst einmal festgestellt werden, was sich außerhalb der Plattform grundsätzlich schwierig gestaltet.

Abschließend lässt sich daher festhalten, dass beide Arten von Kontrollressourcen ihre jeweils eigenen Vor- und Nachteile mit sich bringen und für ihre Wirksamkeit gegenseitig aufeinander angewiesen sind. Limitierungen ergeben sich aus faktischen Schwierigkeiten bei der Durchsetzung, aus den betriebswirtschaftlichen Handlungsdynamiken des Plattformbetriebs, die eine komplette Kontrolle meist nicht erstrebenswert machen, sowie aus der Herausforderung der Übersetzung menschlichen Handelns in technische Parameter.

C. Ergebnis

Die zunehmende Akteurspluralität im digitalen Raum sorgt somit für ein zunehmendes Diffundieren von Arbeitsbeiträgen und Einflusssphären. Klassische Akteursrollen wie die des Diensteanbieters und des Nutzers bleiben in vielen Bereichen bestehen, erfahren aber teils immense Kontroll-, Transparenz- und Souveränitätsverluste, die sich häufig gegenseitig bedingen.[176] Da digitale Dienste in rapide anwachsender Form hinsichtlich ihrer Features wie auch Geschäftsmodelle datengetrieben und somit auf personenbezogene Daten angewiesen sind, erwachsen aus diesen Entwicklungen auch Auswirkungen auf Privatsphäre und Datenschutz der Nutzer.[177] Dass diese Konsequenzen derzeit vielmals negativer Art sind, zeigt die große Anzahl beispielhafter Skandale und publik gewordener Problemfälle.[178]

---

da Apple seine Entwicklerrichtlinien kurz darauf anpasste und auch konvertierte Apps verbot. *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 11 f.

[176] Siehe dazu die Ausführungen *supra* bei B. I.

[177] Siehe hierzu etwa die Ergebnisse der explorativen Umfrage von Facebook-Nutzern zu Apps auf Facebooks Plattform bei *King* u. a., Privacy: is there an app for that?, S. 10, die durch alle Nutzertypen hindurch Wissens- und Verständnislücken hinsichtlich der Befugnisse und Verarbeitungszwecke von App-Anbietern aufzeigen.

[178] Siehe die beispielhafte Auflistung *supra* bei A.

Wie dieses Kapitel gezeigt hat, bilden sich, getrieben durch betriebswirtschaftliche und innovationfördernde Entwicklungen, neue Modi, nach denen sich die Gemengelage an Akteuren im Umfeld digitaler Dienste sortiert und ordnet. Ein zentraler Modus ist der der digitalen Plattform und des sie umgebenden Ökosystems. Die auf solche Plattformen gerichteten Überlegungen zeigen, dass Plattformbetreiber im Rahmen des Ökosystems ihrer Plattform, teils aber auch außerhalb dieses Rahmens, eine herausgehobene Stellung einnehmen und die Kontrollverluste der ihr Ökosystem bevölkernden Akteure in ihrer Person teilweise zu kompensieren vermögen (A.). Die von ihnen etablierten und durchgesetzten Regeln und Sanktionen nähern sich innerhalb ihres Einflussbereichs bzgl. ihrer Wirkmacht teilweise gar staatlichen Regeln an.[179] Gleichzeitig erleben auch sie – nicht anders als staatliche Akteure – Limitierungen bei der Ausübung ihrer Einflussmöglichkeit und sehen sich einem stetigen und komplexen Prozess des Austarierens zwischen den beiden großen Polen der Kontrolle und der Freiheit ausgesetzt, der von externen und internen Faktoren getrieben ist (B.).

Aufbauend auf diesen beiden Erkenntnissen sollen über die nächsten Kapitel zwei Aspekte tiefergehend untersucht werden. Erstens: Was bedeutet die festgestellte Akteurspluralität mit ihren Auswirkungen für den Datenschutz und insbesondere sein eng mit dem Gedanken der individuellen Kontrolle und Einflussmöglichkeit verbundenes Konzept der Verantwortlichkeit (Kapitel 2)? Erhärtet sich der durch die untersuchten Cases aufgekommene Verdacht, das bestehende Datenschutzrecht könnte durch die zunehmende Komplexität und Zerfaserung der Akteurskonstellationen unter Druck geraten? Und zweitens: Spiegelt das bisherige Konzept des Datenschutzes die identifizierte Sonderstellung der Plattformbetreiber gebührend wider? Und wenn nicht, bietet sich hier ein möglicher Ansatzpunkt für eine Modernisierung des Datenschutzrechts in Zeiten zunehmend komplexer Akteurskonstellationen (Kapitel 3)?

[179] Vgl. *Evans*, Berkeley Tech. L. J. 2012, 1201 (1204): „In some cases, the rules and penalties imposed by the platform are similar to, and in some cases close substitues for, rules and penalties adopted by a public regulator." Ähnlich auch *Boudreau/Hagiu*, in: Gawer, Platforms, Markets and Innovation, S. 163 (169 f.).

Kapitel 2

Die datenschutzrechtliche Verantwortlichkeit

In diesem Kapitel soll zunächst die datenschutzrechtliche Verantwortlichkeit in Form ihrer sekundärrechtlichen Ausgestaltung in der DSGVO (und, in Grundzügen, der ihr vorangegangen DSRL) beleuchtet werden. Dabei soll der Blick auf die Rolle des Verantwortlichen innerhalb des Datenschutzes, die mit ihr verbundenen Pflichten und die für ihre Zuschreibung bestehenden Voraussetzungen geschärft werden, indem zunächst einige Überlegungen zum Datenschutz an sich angestellt werden: einerseits zu der Frage, welcher Regelungszweck damit eigentlich verfolgt, welches Schutzgut geschützt werden soll (A.). Andererseits, darauf aufbauend, zu der Frage, was für ein Regelungskonzept sich hinter der vom EU-Gesetzgeber gewählten Art der Verantwortlichkeitszuschreibung verbirgt und auf welchen Prämissen dieses aufbaut (B.). Zuletzt sollen mit diesem geschärften Blick dann die verschiedenen datenschutzrechtlichen Akteursrollen in ihrer Entwicklung über die Jahre skizziert und insbesondere der Wandel und die Konturierung der Voraussetzungen ihrer Qualifizierung im Laufe dieser Zeit analysiert werden (C.).

A. Regelungszweck und Schutzgut des Datenschutzrechts

Die untrennbar miteinander verwobenen Fragen nach Regelungszweck und Schutzgut des Datenschutzrechts sind so alt wie die Antworten auf sie vielseitig und ausufernd. Gewiss scheint einzig die Tatsache, dass jedenfalls nicht Daten das Schutzgut und somit der Schutz von Daten der Regelungszweck ist, sodass grundlegende Einigkeit zumindest hinsichtlich der untauglichen Bezeichnung des Rechtsgebiets besteht.[1] Datenschutz schützt also nicht Daten, sondern – dieser Konsens ist wohl erreicht – (natürliche)[2] Personen bei der Verarbeitung der sie betreffenden Daten.[3]

---

[1] Vgl. *von Lewinski*, Die Matrix des Datenschutzes, S. 4 f.; siehe außerdem statt vieler *Pötters*, in: Gola, DSGVO, Art. 1 Rn. 8; vgl. außerdem *Simitis*, NJW 1971, 673 (676); prägnant auch *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 11 (23).

[2] So bereits der Wortlaut von Art. 1 Abs. 1 DSGVO und vorher Art. 1 Abs. 1 DSRL, der einen Schutz personenbezogener Daten bei juristischen Personen ausschließt. Dass diese Einschränkung nicht zwingend ist, zeigt etwa das Schweizer Bundesgesetz über den Datenschutz,

I. Die Frage des grundrechtlichen Schutzguts

Art. 1 Abs. 2 DSGVO konkretisiert weiter: Geschützt werden „die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten". Diese Formulierung lässt viel Spielraum für Interpretationen bei der Suche nach dem konkreten Schutzgut. Sind es nun *alle* Grundrechte und Grundfreiheiten, die vor bei Datenverarbeitungen entstehenden Gefahren geschützt werden sollen?[4] Oder bloß einzelne, vielleicht sogar nur das am Ende der Formulierung explizit herausgestellte – und wiederum mit ganz eigenen Konturproblemen hinsichtlich seines Schutzguts behaftete – Recht auf Schutz personenbezogener Daten? Der Wortlaut, der dem herausgestellten Recht ein *insbesondere* voranstellt, spricht für die erste, weite Auslegung. Ein solch weites Verständnis aber führt freilich schnell zu Konkurrenzproblemen[5] und vielerorts zu Kritik, der Datenschutz werde zu einer überfrachteten Rechtsmaterie erhoben und mit Aufgaben belegt, die er kaum zufriedenstellend erbringen kann.[6] Datenschutz würde nach diesem Verständnis zu einem „unerfüllbaren Vollkaskorecht"[7] werden, das, frei nach dem Prinzip des *law of the horse*[8] und mit dem Ergebnis einer *uberprotection*[9], undifferenziert alle Rechtsfragen, die sich aus der Verarbeitung personenbezogener Daten ergeben, dem Datenschutzrecht überantwortet.[10]

Um eine Annäherung an die Auflösung dieser Unklarheit hinsichtlich der Grenzen des Schutzguts und der von ihm insgesamt umfassten Grundrechte

---

das ausweislich seines Art. 2 für das „Bearbeiten von Daten natürlicher und juristischer Personen" gilt.

[3] Vgl. *Albers*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 213 (222).

[4] In diese Richtung gehend etwa *Buchner*, in: Kühling/Buchner, DSGVO/BDSG, Art. 1 DSGVO Rn. 13 f. *Buchholtz/Stentzel*, in: Gierschmann u. a., DSGVO, Art. 1 Rn. 28.

[5] Insbesondere zum Verbraucherrecht und zum Wettbewerbsrecht. Siehe dazu etwa die andauernde Diskussion um die Frage, ob Datenschutzverstöße durch Mitbewerber nach Maßgabe des UWG abgemahnt werden dürfen oder die DSGVO diesbezüglich eine Sperrwirkung entfaltet, vgl. *Diercks*, CR 2019, 95. Zur Frage des Verhältnisses zwischen Datenschutz- und Kartellrecht siehe *Zanfir-Fortuna/Ianc*, Data Protection and Competition Law.

[6] Siehe etwa *Bull*, Sinn und Unsinn des Datenschutzes; *Giesen*, NVwZ 2019, 1711 (1711 ff.).

[7] *Veil*, Die Schutzgutmisere des Datenschutzrechts – Teil II; in dieselbe Richtung gehend *Giesen*, NVwZ 2019, 1711 (1714 ff.), der von einer „totalitäre[n] Tendenz" spricht.

[8] Ein durch den US-amerikanischen Richter Frank H. Easterbrook bekannt gewordenes Theorem, wonach die Erschaffung eines eigenständigen und weitreichenden Rechtsgebiets des „Cyberlaw" für alle Sachverhalte mit Internetbezug ebenso wenig zu sachgerechten und differenzierten Lösungen führen würde, wie es ein pauschales „Pferderecht" für unterschiedlichste Sachverhalte (Kauf, Haftung, Lizenzen, Pflege) im Zusammenhang mit Pferden täte. Eine gute Übersicht der Rechtsgebiete, die das Datenschutzrecht als Querschnittsmaterie tangiert, liefert *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (26).

[9] *Zanfir-Fortuna/Ianc*, Data Protection and Competition Law, S. 10 ff.

[10] Siehe hierzu auch *Purtova*, Law, Innovation and Technology 2018, 40.

und -freiheiten zu wagen, soll der Fokus hier auf die in Art. 1 DSGVO *explizit* genannten Schutzgüter – namentlich das Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DSGVO) sowie der freie Verkehr dieser Daten (Art. 1 Abs. 3 DSGVO) – gelegt werden, in der Hoffnung, aus ihrer Analyse bereits ein weitergehendes Verständnis hin zu einer Konturierung des gesamten Schutzguts zu gewinnen.

1. Schutz personenbezogener Daten

a) Das europäische Datenschutzgrundrecht

Unmittelbar abzustellen ist im Anwendungsbereich der DSGVO, mit Blick auf Art. 51 Abs. 1 GRCh, auf die in der GRCh normierten Unionsgrundrechte. Spricht Art. 1 Abs. 2 DSGVO diesbezüglich vom Recht auf Schutz personenbezogener Daten, sind hier zwei Grundrechte in den Blick zu nehmen: die Rechte auf Achtung des Privat- und Familienlebens in Art. 7 sowie auf Schutz personenbezogener Daten in Art. 8 GRCh.[11] Mit dem Privatleben[12] schützt Art. 7 GRCh in Form der Entwicklung und Entfaltung der individuellen Persönlichkeit[13] und insbesondere dem Recht auf Selbstbewahrung und Selbstdarstellung einen dem deutschen allgemeinen Persönlichkeitsrecht sehr ähnlichen Lebensbereich. Die Norm entspricht in ihrem Wortlaut und, ausweislich der Charta-Erläuterungen, auch inhaltlich dem in Art. 8 EMRK garantierten Recht,[14] sodass dieses gem. Art. 52 Abs. 3 S. 1 GRCh als Rechtserkenntnisquelle „gleicher Bedeutung und Tragweite" herangezogen und somit auch die zu ihm ergangene Rechtsprechung des EGMR berücksichtigt werden muss.[15] Da die EMRK kein dem Art. 8 GRCh vergleichbares Äquivalent eines eigenständigen Datenschutzgrundrechts kennt, wurde dieser dort stets als Ausprägung des Privatlebens-

[11] Mit Blick auf das weitere primäre Unionsrecht ließe sich auch der mit Art. 8 I GRCh wortlautgleiche Art. 16 Abs. 1 AEUV heranziehen, was jedoch aufgrund dessen fehlender Schrankenbestimmung erhebliche Konkurrenzprobleme nach sich ziehen würde. Die Norm wird daher – auch mit Blick auf ihre historische Bedeutung als symbolische primärrechtliche Verankerung des bis dato nur sekundärrechtlich (in Form der DSRL) und durch die Grundrechtsprechung des EuGH etablierten Datenschutzrechts – überzeugender Weise als „objektivrechtliche Querschnittsverpflichtung" und somit nicht als Grundrecht verstanden, vgl. *M. Schröder*, in: Streinz, EUV/AEUV, Art. 16 Rn. 6. A. A. statt vieler *Frenz*, Handbuch Europarecht Band 4, Rn. 1357.

[12] Als einen der geschützten Teilbereiche neben Familienleben, Wohnung und Kommunikation.

[13] *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, Art. 7 GRCh Rn. 3–6; *Jarass*, in: Jarass, Grundrechtecharta, Art. 7 Rn. 3.

[14] Siehe die über die Jahre leicht veränderten Erläuterungen zur Charta der Grundrechte der Europäischen Union (die nach Art. 6 Abs. 1 Uabs. 3 EUV gebührend bei der Auslegung der Charta-Grundrechte berücksichtigt werden sollen) in ABl. C-303 vom 14.12.2007, Erläuterungen zu Art. 7, S. 20.

[15] Vgl. *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, Art. 52 GRCh Rn. 21 ff.

schutzes von Art. 8 EMRK mit umfasst.[16] Gekoppelt war der Schutz dabei an einen – allerdings sehr weit verstandenen[17] – Privatlebensbezug der verarbeiteten Daten, sodass, anders als nach BVerfG-Konzeption, nicht jedes personenbezogene Datum in den Schutzbereich fiel.[18]

Die Existenz von Art. 8 GRCh als explizit normiertes Recht einer jeden Person auf Schutz personenbezogener Daten (Abs. 1) verkompliziert diese Lage und wirft die Frage nach dem Verhältnis der beiden Normen und der Reichweite der Eigenständigkeit von Art. 8 GRCh auf. So prüft der EuGH die beiden Normen in seinen Entscheidungen regelmäßig gemeinsam[19], geht also von einem naturgemäß engen Zusammenhang der beiden Grundrechte aus und spricht gar von der „in Art. 7 und 8 der Charta anerkannte[n] Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten“[20] und dem Grundrecht „betreffend den Schutz personenbezogener Daten und damit des Privatlebens“[21], was die Vermutung nahe legt, es handele sich hier um ein einheitliches (Kombinations-)Grundrecht.[22] Gleichzeitig deuten jüngere Ausführungen, etwa in der Entscheidung zur Vorratsdatenspeicherung, darauf hin, dass Art. 8 GRCh isoliert gerade in Verarbeitungsfällen ohne Privatsphärenbezug zum Tragen kommen soll.[23] Weitergehende explizite systematische Ausführungen oder gar eine Klarstellung zum Verhältnis der beiden Grundrechte lässt der EuGH jedoch vermissen.[24]

---

[16] Siehe die EGMR-Urteile Nr. 9248/81 (Leander/Schweden), ECLI:CE:ECHR:1987:0326JUD000924881 Rn. 48 und Nr. 22798/95 (Amann/Schweiz), ECLI:CE:ECHR:2000:0216JUD002779895 Rn. 65 sowie *Frenz*, Handbuch Europarecht Band 4, Rn. 1183.

[17] So wurde der Schutzbereich etwa auch auf Daten über berufliche Einkünfte erstreckt und die Betroffenheit der Privatsphäre u. a. mit dem Ausmaß und der Systematik der Sammlung und Aufbewahrung der betroffenen Daten sowie mit ihrem Bezug zu lange vergangenen Geschehnissen begründet, vgl. EGMR Nr. 28341/95 (Rotaru/Rumänien), ECLI:CE:ECHR:2000:0504JUD002834195 Rn. 43 f. und Nr. 22798/95 (Amann/Schweiz), ECLI:CE:ECHR:2000:0216JUD002779895 Rn. 65. Siehe auch die Ausführungen bei *Gellert/Gutwirth*, CLSR 2013, 522 (526).

[18] Vgl. *Meyer-Ladewig/Nettesheim*, in: Meyer-Ladewig u. a., EMRK, Art. 8 Rn. 32, die von privaten und öffentlichen Daten sprechen.

[19] Siehe als Beispiel für viele: EuGH, Rs. C-92/09 (Schecke), Slg. 2010, I-11063 Rn. 47 oder in der jüngeren Vergangenheit EuGH, verb. Rs. C-293/12 und C-594/12 (Digital Rights Ireland Ltd.), ECLI:EU:C:2014:238 Rn. 31.

[20] EuGH, Rs. C-92/09 (Schecke), Slg. 2010, I-11063 Rn. 52.

[21] EuGH, Rs. C-275/06 (Promusicae), ECLI:EU:C:2008:54 Rn. 63.

[22] So auch *Eichenhofer*, Der Staat 2016, 41 (62); so auch das Fazit der umfassenden Rechtsprechungsanalyse bei *Lynskey*, ICLQ 2014, 569 (574 ff.).

[23] Vgl. EuGH, verb. Rs. C-293/12 und C-594/12 (Digital Rights Ireland Ltd.), ECLI:EU:C:2014:238 Rn. 29 f.

[24] Siehe *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Hoffmann-Riem, Grundlagen des Verwaltungsrechts Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, S. 107, § 22 Rn. 44, die davon spricht, es fehle an einem „inhaltlich gesicherten Fundament und an dogmatischer Stabilität.“ Ähnlich *Kranenborg*, in: Peers u. a., The EU Charter of Fundamental Rights, Art. 8 Rn. 08.28: „Read together, this case law does not reveal a clear approach on the matter.“ Ebenfalls kritisch *González Fuster*, Birkbeck Law Review 2014, 263

Einem (reinen) Kombinationsverständnis entgegen steht aber nicht nur die Normierung von Art. 8 als eigenständiges – und eben nicht in einem zusätzlichen Absatz des Art. 7 verankertes – Grundrecht innerhalb der GRCh, sondern auch der Wortlaut von Art. 1 Abs. 2 DSGVO, der insofern eindeutig vom „Recht auf Schutz personenbezogener Daten" spricht und das Privatleben nicht explizit erwähnt. Ein Blick auf die Erläuterungen[25] zur GRCh zeigt zudem, dass sich Art. 8 GRCh neben Art. 8 EMRK unter anderem auch auf das Übereinkommen Nr. 108, einen völkerrechtlichen Vertrag aus der Feder des Europarates zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten, stützt, und mit dem expliziten Ziel erschaffen wurde, proaktiven und strukturellen Schutz[26] vor den Gefahren im Zusammenhang mit jeglichen Datenverarbeitungen, unabhängig von ihrem Schutz über Art. 7 GRCh, zu bieten. Ein weiteres starkes Indiz liegt darin begründet, dass ausweislich der Erläuterungen[27] auch die bei Erlass der GRCh bereits bestehende DSRL als Vorbild für das Recht auf Schutz personenbezogener Daten Pate stand. Zwar darf dies nicht zum Anlass genommen werden, einzelne sekundärrechtliche Normen und Datenschutzprinzipien auf Grundrechtsebene zu heben bzw. diese grundlegende vertikale Ebenentrennung aufzulösen, als Abgrenzung zum Privatlebensschutz nach Art. 7 GRCh kann es aber durchaus dienen.[28]

Demzufolge scheint es unstrittig, Art. 8 GRCh auch einen, wie auch immer gearteten, eigenen Wert und Schutzgehalt über die Kombination mit dem Privatleben hinaus zuzubilligen.[29] Wie dieser konkret aussieht, ist jedoch umstritten.

aa) Der bisherige Meinungsstand

So wird – teils in Ablehnung der EuGH-Linie, teils ohne Bewusstsein um den Widerspruch mit dieser – vertreten, Art. 8 GRCh nehme eine *lex specialis*-Stellung gegenüber Art. 7 GRCh ein und verdränge diesen damit dort, wo das Tatbestandsmerkmal der Verarbeitung personenbezogener Daten erfüllt ist.[30]

(263 ff.); prägnant außerdem *Brkan*, German Law Journal 2019, 864 (883): „[…] the numerous meanders of the CJEU's reasoning that sometimes comes across as a true maze[…]."

[25] Vgl. ABl. 303, Erläuterungen zu Art. 8, S. 20.

[26] *Hustinx*, EU-Datenschutzrecht: Die Überprüfung der Richtlinie 95/46/EG und die vorgeschlagene Datenschutz-Grundverordnung, S. 20.

[27] Vgl. ABl. C-303 vom 14.12.2007, Erläuterungen zu Art. 7, S. 20.

[28] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, S. 61, der von einer „Stärkung des horizontalen Selbststands" gegenüber Art. 7 GRCh spricht.

[29] So letztlich auch den EuGH interpretierend *Reinhardt*, AöR 2017, 528 (532): „[…] misst ihm aber auch eine eigenständige Bedeutung zu, ohne dass die konstruktive Eigenständigkeit des Datenschutzgrundrechts immer deutlich würde […]." Siehe auch *Kranenborg*, in: Peers u. a., The EU Charter of Fundamental Rights, Art. 8 Rn. 08.27: „The right to privacy and the right to data protection are closely linked, but should not be seen as one and the same right."

[30] Vgl. *Guckelberger*, EuZW 2011, 126 (127); Vgl. *Kingreen*, in: Calliess/Ruffert, EUV/

Andere stellen die beiden Rechte als separate Kreise mit (weitem) Überlappungsbereich dar – die Differenzierung hinge dann nicht vom Merkmal der Datenverarbeitung ab, sondern davon, ob das verarbeitete Datum qualitativ einen engen Bezug zum Privatleben aufweise oder einen „bloßen", nicht privatsphärenrelevanten[31] Personenbezug.[32] Teilweise wird dies mit divergierenden Schutzzwecken begründet, die im Rahmen von Art. 7 GRCh in der Vertraulichkeit privater Lebensumstände, insbesondere der Privatheit der Kommunikation,[33] bei Art. 8 GRCh hingegen in der Verhinderung von Machtasymmetrien liegen sollen.[34] Andere sehen den Datenschutz deshalb als genuin eigenständig an, weil er das grundlegend individualbezogene Konzept der Privatsphäre für einen überindividuellen Horizont öffne und damit gerade auch vor gesellschaftlichen Implikationen und Gefahren durch Datenverarbeitungen schütze.[35] Ebenfalls wird vertreten, das Datenschutzgrundrecht habe allein instrumentellen Charakter und diene damit der Absicherung des Privatsphärenschutzes (und anderer Grundrechte) hinsichtlich der Gefahren durch Datenverarbeitungen.[36] Gleichzeitig sind Stimmen zu vernehmen, die den Zweck der Norm in der bloßen primärrechtlichen Legitimierung der damaligen DSRL (und damit auch der heutigen DSGVO) sowie der Absicherung und Garantie des Bestandes eines EU-Sekundärdatenschutzrechts insgesamt sehen.[37] Auch könnte in der Schaf-

---

AEUV, Art. 8 GRCh Rn. 2; Vgl. *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, S. 349; in diese Richtung gehend auch *Tzanou*, IDPL 2013, 88 (90 ff.).

[31] Fraglich ist dann freilich, welche Daten einen Bezug zum Privatleben aufweisen und welche nicht. *Roßnagel*, NJW 2019, 1 (2) will hier auf die Bestimmung der betroffenen Person darüber abstellen, was sie als ihre Privatheit versteht.

[32] Vgl. *Jarass*, in: Jarass, Grundrechtecharta, Art. 8 Rn. 4 sowie Generalanwalt *Cruz Villalón*, Schlussanträge zu verb. Rs. C-293/12 und C-594/12 (Digital Rights Ireland Ltd.), ECLI:EU:C:2014:238 Rn. 62 f. mit ausführlicher Begründung; vgl. auch *Bock/Engeler*, DVBl 2016, 593 (596); sowie *Kokott/Sobotta*, International Data Privacy Law 2013, 222 (225); in eine ähnliche Richtung gehend *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Hoffmann-Riem, Grundlagen des Verwaltungsrechts Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, S. 107, § 22 Rn. 43; *Gellert/Gutwirth*, CLSR 2013, 522 (526); in diese Richtung gehend auch BGH, Urt. v. 28.05.2020, Az. I ZR 7/16 Rn. 61 bzgl. der Unterscheidung der Schutzzwecke von DSGVO und ePrivacy-RL; siehe ebenfalls *Roßnagel*, NJW 2019, 1 (2).

[33] Vgl. *Kühling/Raab*, in: Kühling/Buchner, DSGVO/BDSG, Einführung DSGVO Rn. 26.

[34] *Bock/Engeler*, DVBl 2016, 593 (595 f.), die dieses Schutzgut als informationelle Unversehrtheit betiteln. Ähnlich auch, mit Blick auf staatliche Datenverarbeitungen, *Rouvroy/Poullet*, in: Gutwirth/Poullet/de Hert/de Terwangne/Nouwt, Reinventing data protection?, S. 45 (70): „[…] in order to prevent disproportionate informational power relationships to be developed or perpetuated between public and private data controllers and citizens." In die gleiche Richtung gehend *Lynskey*, ICLQ 2014, 569 (28 ff.).

[35] Vgl. *Bygrave*, UNSW Law Journal 2001, 277 (282): „Finally, the view that data protection is essentially privacy protection runs the risk of obscuring the fact that data protection laws benefit not only individuals qua individuals but society as a whole."

[36] *Rouvroy/Poullet*, in: Gutwirth/Poullet/de Hert/de Terwangne/Nouwt, Reinventing data protection?, S. 45 (69 f.); *Lynskey*, ICLQ 2014, 569.

[37] Vgl. *de Hert/Gutwirth*, in: Gutwirth/Poullet/de Hert/de Terwangne/Nouwt, Reinventing data protection?, S. 3 (8 ff., 42): „The incorporation of data protection in Constitutions is prob-

fung von Art. 8 GRCh der Versuch gesehen werden, den Datenschutz über den begrenzten Anwendungsbereich der damaligen DSRL hinaus auch für sämtliche restlichen Bereiche von Datenverarbeitungen auszuweiten.[38]

Insgesamt lässt sich festhalten, dass keine der beschriebenen Herangehensweisen die mit der durch die GRCh geschaffenen und durch den EuGH offen belassenen Unklarheit einhergehenden Probleme gänzlich zu lösen vermag, sich der Großteil von ihnen vielmehr in plausiblen Ansätzen übt, die zwar negativ die Abgrenzung erleichtern, aber darüber hinaus keine positive Aussage zum eigenständigen Wert des Datenschutzgrundrechts leisten und damit letztlich Stückwerk bleiben. Anstatt hier eine ausführlichere einzelne Betrachtung der verschiedenen Ansichten mit punktueller Kritik vorzunehmen, sollen diese inzident im folgenden Abschnitt beleuchtet und teils entkräftet, teils in ihrer begrenzten Perspektive aufgezeigt und eingeordnet werden.

bb) Die Rekonstruierung nach Marsch

Einen den zuletzt beschriebenen Überschneidungstheorien ähnlichen, aber noch weit differenzierter ausgestalteten und in seiner Konsequenz radikaleren Ansatz, der, wie im Folgenden zu erläutern sein wird, im Ergebnis dennoch stärker als die bisher beschriebenen Ansätze zu überzeugen vermag, beschreitet *Marsch*.[39] Bei seiner Rekonstruierung des europäischen Datenschutzgrundrechts teilt er dieses in mehrere in einem Subsidiaritätsverhältnis zueinander stehende Dimensionen auf, von denen insbesondere drei für die hier im Mittelpunkt stehende Problemstellung von Bedeutung sind:[40] zunächst eine aus Art. 8 GRCh allein folgende *Ausgestaltungsdimension* in Form einer an den Gesetzgeber gerichteten, aber auch vom Einzelnen durchsetzbaren, Pflicht zur grundrechtsadäquaten Ausgestaltung des Datenschutzsekundärrechts,[41] sowie eine aus Art. 8 i. V. m. Art. 7 und anderen Grundrechten der GRCh stammende *abwehrrechtliche* Dimension mit einer instrumentellen und einer freiheitsakzessorischen Schutzebene.[42] Hinzu tritt eine für den hiesigen Fall von Datenverarbeitungen durch Private besonders elementare *Schutzpflichten- und Drittwirkungsdimension*.[43]

---

ably a good political statement but it is far too early to evaluate its legal effects." Kritisch dazu *Lynskey*, ICLQ 2014, 569 (571): „[…] it seems unsatisfactory to accept that a new right has been recognised in the EU legal order to provide ex-post legitimacy to existing legislation."

[38] Vgl. *Cannataci/Mifsud-Bonnici*, Information & Communications Technology Law 2005, 5 (12); siehe ebenfalls *Rouvroy/Poullet*, in: Gutwirth/Poullet/de Hert/de Terwangne/Nouwt, Reinventing data protection?, S. 45 (71), die diesen Ansatz jedoch direkt pointiert widerlegen.

[39] *Marsch*, Das europäische Datenschutzgrundrecht.

[40] Marsch ergänzt die hier aufgeführten um eine *organisatorische* und um eine *Leistungsdimension*, die für den Fokus dieser Arbeit aber beide außer Betracht bleiben sollen.

[41] *Marsch*, Das europäische Datenschutzgrundrecht, S. 139.

[42] *Marsch*, Das europäische Datenschutzgrundrecht, S. 203.

[43] *Marsch*, Das europäische Datenschutzgrundrecht, S. 247.

(1) Die Ausgestaltungsdimension aus Art. 8 GRCh

Unmittelbar Art. 8 GRCh zu entnehmen ist diesem Verständnis zufolge „nur" eine Pflicht des EU-Gesetzgebers, den Umgang mit personenbezogenen Daten grundrechtsadäquat und in schutzeffektivierender Weise zu regeln.[44] Dabei soll ihm ein weiter, durch die Prinzipien in Art. 8 Abs. 2 S. 1 GRCh konturierter, Ausgestaltungsspielraum zukommen.[45] Gleichwohl soll mit dieser Ausgestaltungspflicht auch ein subjektiv einklagbares *Recht* korrespondieren, die Dimension also trotz fehlender abwehrrechtlicher Komponente eine subjektive Prägung aufweisen.[46]

Diese Dimension deckt sich mit den Ansichten, die die Einführung von Art. 8 GRCh darin begründet sahen, die Grundrechtsbezogenheit des einfachgesetzlichen Datenschutzes zu stärken, welche zu Zeiten der DSRL aufgrund deren primärer Legitimation durch Art. 114 Abs. 1 2 AEUV und damit des Binnenmarktfokus nur begrenzt vorhanden war.[47]

(2) Die abwehrrechtliche Dimension

Hinzu tritt eine abwehrrechtliche Dimension mit zwei separaten Schutzebenen, die sich nicht isoliert aus Art. 8 GRCh, sondern erst aus dessen Kombination mit anderen Grundrechten ergibt.

Dabei stellt die Kombination mit der Achtung des Privatlebens nach Art. 7 GRCh auf einer *instrumentellen* Schutzebene die erste Schutzebene dar: Ohne das isolierte Schutzgut des Art. 7 GRCh inhaltlich zu erweitern, soll dessen Schutzbereich um einen *Vorfeldschutz* erweitert werden. Das Kombinationsgrundrecht soll also immer dann[48] einschlägig sein, wenn die *Gefahr* einer Verletzung der Privatheit in Form der inneren Entfaltungsfreiheit besteht, ohne dass bereits eine solche Verletzung eingetreten ist.[49] Im Ergebnis entspricht diese kombinationsgrundrechtliche Komponente nach *Marschs* Verständnis dem, was der EuGH als Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten prüft, wenn er Art. 7 und 8 GRCh in seinen Entscheidungen kombiniert.[50] Gleichzeitig steht es in der Tradition der Rechtsprechungslinie des EGMR zu Art. 8 EMRK und setzt somit die Kohärenzvorgabe

---

[44] *Marsch*, Das europäische Datenschutzgrundrecht, S. 130 f.

[45] *Marsch*, Das europäische Datenschutzgrundrecht, S. 137 ff.

[46] *Marsch*, Das europäische Datenschutzgrundrecht, S. 130 f.; Dieses Recht kann sich naturgemäß aber nicht auf konkrete Normen beziehen, sondern nur auf den „unabdingbare[n] Mindeststandard, wie ihn Art. 8 EGRC vorgibt […]." Siehe auch *Frenz*, Handbuch Europarecht Band 4, S. 429 Rn. 1390.

[47] Vgl. Ausführungen und Kritik bei *Lynskey*, ICLQ 2014, 569 (671 f.).

[48] Und zwar, als gegenüber Art. 7 GRCh subsidiäres Recht, *nur* dann.

[49] *Marsch*, Das europäische Datenschutzgrundrecht, S. 205 f.

[50] So etwa in EuGH, verb. Rs. C-293/12 und C-592/12 (Digital Rights Ireland Ltd.), ECLI:EU:C:2014:238.

des Art. 52 Abs. 3 GRCh um. In Abgrenzung zum deutschen, eindeutig als Abwehrrecht ausgestalteten Recht auf informationelle Selbstbestimmung, sowie zu vielen Stimmen, die ebenjenes Verständnis auch auf das europäische Datenschutzgrundrecht schlicht übertragen sehen wollen,[51] soll hier jedoch nicht *jede* Verarbeitung personenbezogener Daten den kombinationsrechtlichen Vorfeldschutz aktivieren; stattdessen soll der Schutzbereich[52] erst bei Verarbeitungen mit erheblichem Gefährdungspotential eröffnet sein,[53] welches sich insbesondere aus den verarbeiteten Daten selbst oder aus der Verarbeitungsweise ergeben soll.[54] Diese Dimension deckt sich mit anderen Ansichten, die die eigenständige Bedeutung des Datenschutzgrundrechts primär oder zumindest auch in seinem instrumentellen Wert sehen.[55]

Eine zweite Schutzebene des Datenschutzrechts in seiner abwehrrechtlichen Dimension soll dort zur Geltung kommen, wo Art. 8 GRCh *freiheitsakzessorisch* andere Freiheitsrechte verstärkt, die in ihrem jeweils eigenen Schutzbereich betroffen[56] sind.[57] Auch hier hat die Kombination mit Art. 7 GRCh eine herausgehobene Stellung und kommt immer dort in Betracht, wo die Verarbeitung personenbezogener Daten bereits die Schwelle von der bloßen Gefahr hin zur tatsächlich eingetretenen Beschränkung etwa der inneren Entfaltungsfreiheit überschritten hat.[58] Denkbar sind aber auch Verstärkungen anderer durch Da-

---

[51] So spricht auch *Kühling*, in: Kühling/Buchner, DSGVO/BDSG, Art. 1 Rn. 9 DSGVO, dem Recht in Art. 8 GRCh eine Rolle als Abwehrrecht zu.

[52] Für eine ähnlich gelagerte Einschränkung auf Eingriffsebene für das Recht auf informationelle Selbstbestimmung, siehe *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft: Symposium des Centre for Security and Society, S. 167 (182 ff.).

[53] *Marsch*, Das europäische Datenschutzgrundrecht, S. 213.

[54] *Marsch*, Das europäische Datenschutzgrundrecht, S. 212 ff.; kritisch gegenüber der Operationalisierbarkeit solcher Kriterien hingegen *Volkmann*, JURA 2014, (824 f.). Ein umstrittenes Beispiel für Daten mit Privatsphärenbezug sind nach Verständnis des BGH in Auslegung von Art. 5 Abs. 3 ePrivacy-RL mittels Cookies auf Nutzerendgeräten gespeicherte Daten. Vgl. BGH, Urt. v. 28.05.2020, Az. I ZR 7/16 Rn. 61.

[55] Vgl. *Rouvroy/Poullet*, in: Gutwirth/Poullet/de Hert/de Terwangne/Nouwt, Reinventing data protection?, S. 45 (69 f.): „In this regard, data protection directives are among the tools through which the individual exercises his right to privacy. […] Yet, data protection is also a tool for protecting other rights than the right to privacy." *Reinhardt*, AöR 2017, 528 (538).

[56] Siehe auch hier *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft: Symposium des Centre for Security and Society, S. 167 (178 f.), der im Endeffekt jedoch insgesamt von einem instrumentellen Gefährdungsschutz vor Beeinträchtigung der anderen (Freiheits-)Grundrechte ausgeht.

[57] Weshalb die Freiheitsrechte in diesen Fällen auch nur durch das Datenschutzgrundrecht – und insbesondere dessen Prinzipien in Art. 8 Abs. 2 GRCh – verstärkt werden, es aber insbesondere im Rahmen der Verhältnismäßigkeitsprüfung nur auf ihre eigenen Schutzgüter ankommt, vgl. *Marsch*, Das europäische Datenschutzgrundrecht, S. 203 ff.

[58] Als Beispiel für ein solches schutzbereichsverstärkendes Hinzutreten von Art. 8 GRCh nennt *Marsch*, Das europäische Datenschutzgrundrecht, S. 203 f. das Urteil des EuGH, verb. Rs. C-293/12 und C-592/12 (Digital Rights Ireland Ltd.), ECLI:EU:C:2014:238 zur Vorratsdatenspeicherungsrichtline.

tenverarbeitungen typischerweise tangierter Freiheitsrechte, wie etwa den in Art. 10, 11 und 12 GRCh verankerten Rechten auf Gewissens- und Religionsfreiheit, auf Meinungsfreiheit und auf Versammlungs- und Vereinigungsfreiheit. Der hinzutretende Art. 8 GRCh mit seinen eigenständigen Prinzipien und Anforderungen, etwa in seinem Abs. 2, soll den Schutz des jeweils einschlägigen Freiheitsrechts dann dergestalt effektuieren, dass er *nach* Bestimmung und Gewichtung der Eingriffsschwere anhand des dortigen Schutzbereichs darauf bezogene Vorgaben hinsichtlich angemessener konkreter Schutzmaßnahmen für den festgestellten abstrakten Schutzbedarf bereitstellen kann.[59] Auch dies deckt mit sich existierenden Ansichten, die in Art. 8 GRCh eine Konkretisierung bestehender Grundrechte und ihrer Schutzgehalte durch datenverarbeitungsspezifische Bedingungen sehen.[60]

(3) Die Schutzpflichten-, Drittwirkungs- und private Ausgestaltungsdimension

Während die eben beschriebenen Dimensionen des Datenschutzgrundrechts sich zunächst – wie alle Unionsgrundrechte gem. Art. 51 Abs. 1 AEUV nur EU-Institutionen und Mitgliedstaaten verpflichten – nur auf *staatliche* Datenverarbeitungsvorgänge beziehen[61], stellt sich für die hier relevanten Verarbeitungen durch *Private* die Frage, welche Dimension hinsichtlich gesetzgeberischer Schutzpflichten und mittelbarer Drittwirkung[62] besteht. Relevant ist dies vor allem deshalb, weil Datenverarbeitungen durch Private – anders als solche Verarbeitungen durch staatliche Akteure – ihrerseits Grundrechtsausübungen dar-

---

[59] *Marsch*, Das europäische Datenschutzgrundrecht, S. 204 f.; das könnten etwa Maßnahmen der Datensicherheit oder Mechanismen der Kontrolle als „elementare Anforderung an die Verhältnismäßigkeit des Umgangs mit personenbezogenen Daten" sein, wie *Reinhardt*, AöR 2017, 528 (541) mit Blick auf EuGH, verb. Rs. C-293/12 und C592/12 (Digital Rights Ireland Ltd.), ECLI:EU:C:2014:238 Rn. 54 und 66 f. konstatiert.

[60] Vgl. *Rodotà*, in: Gutwirth/Poullet/de Hert/de Terwangne/Nouwt, Reinventing data protection?, S. 77 (80): „Accordingly, restrictions or limitations are only admissible if certain specific conditions are fulfilled, rather than merely on the basis of the balancing of interests."

[61] Zwar kennt das Unionsrecht infolge gewachsener EuGH-Rechtsprechung entgegen der deutschen Tradition bereits (allerdings bisher stets Gleichbehandlungs- und Nichtdiskriminierungs-) Fälle der unmittelbaren Drittwirkung von (allerdings stets Grundrechten bzw. -freiheiten, siehe etwa EuGH, Rs. 43/75 [Defrenne II], ECLI:EU:C:1976:56, EuGH, Rs. C-555/07 [Kücükdeveci], ECLI:EU:C:2010:21, EuGH, Rs. 36/74 [Walrave und Koch], Slg. 1974, 1405 und EuGH, Rs. C-415/93 [Bosman], ECLI:EU:C:1974:140. Für das Datenschutzrecht ist eine solche Wirkung jedoch nicht anerkannt und werden als in diese Richtung gehend interpretierte Äußerungen des EuGH, etwa in der Rs. C-131/12 [Google Spain], ECLI:EU:C:2014:317, teilweise scharf kritisiert, siehe bspw. *Wolff*, Bayerische Verwaltungsblätter 2015, 9 [15]; ausführlicher zu Fällen der unmittelbaren Drittwirkung *de Sousa*, Cambridge Journal of International and Comparative Law 2013, 479.

[62] Zur mittelbaren Drittwirkung der Unionsgrundrechte instruktiv *Jarass*, ZEuP 2017, 310 (331); für eine unmittelbare Drittwirkung des Datenschutzgrundrechts argumentierend *Hijmans*, The European Union as Guardian of Internet Privacy, S. 36 ff. Ähnlich *Streinz/Michl*, EuZW 2011, 384 (385).

stellen, deren Regulierung durch staatliche Akte rechtfertigungsbedürftige Eingriffe darstellen (können).[63]

Hinsichtlich der Herleitung einer gesetzgeberischen Schutzpflicht ist zunächst auf das eben beschriebene Schutzebenenverständnis *Marschs* zu rekurrieren: Da nach diesem Art. 8 GRCh isoliert nur einen Ausgestaltungsauftrag beinhaltet und auch in Kombination mit Art. 7 GRCh nur einen *instrumentell* zu verstehenden Vorfeldschutz vor Gefährdungen der Privatheit bietet, mangelt es dem Datenschutzgrundrecht an einem genuin eigenständigen Rechts- bzw. Schutzgut. Nur ein solches kann aber tauglicher Bezugspunkt für eine verfassungsrechtliche Pflicht zum Schutz vor Gefährdungen durch Dritte sein[64], sodass es also nur konsequent ist, wenn *Marsch* Schutzpflichten hinsichtlich der Verarbeitung personenbezogener Daten nur aus anderen Grundrechten ableitet.[65] Aufgrund des engen Bezugs ist das in erster Linie Art. 7 GRCh.[66] In Betracht kommen zudem Schutzpflichten hinsichtlich anderer spezifischer Freiheitsrechte im Rahmen der oben aufgezeigten *freiheitsakzessorischen* Dimension von Art. 8 GRCh, sofern ihr jeweiliger Schutzbereich eröffnet ist.[67]

Dabei soll *Marsch* zufolge für den Regulierungsbereich des allgemeinen privaten Datenschutzrechts, wie er in der DSGVO insbesondere durch das Verbotsprinzip mit Erlaubnisvorbehalt etabliert ist, aber aufgrund der starken Verlagerung ins Vorfeld möglicher Schutzgutverletzungen und der geringen Konkretisierung denkbarer handfester Gefährdungen[68] eine nur sehr begrenzte Determinierung durch Schutzpflichten in Betracht kommen.[69] Dies führt einerseits dazu, dass der Gesetzgeber einen sehr großen „Korridor möglicher Konfliktlösungen“[70] bei der Wahl seiner gesetzlichen Ausgestaltung hat. Gleichzeitig ergeben sich Zweifel hinsichtlich der Tragfähigkeit einer über

---

[63] Vgl. *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 58 ff. für eine kurze Abhandlung der typischerweise tangierten Grundrechte von Datenverarbeitern.

[64] So definiert *Canaris*, Grundrechte und Privatrecht, S. 75, die Schutzgebotsfunktion der Grundrechte als Schutz „grundrechtlicher Güter vor tatsächlichen Beeinträchtigungen durch andere Privatrechtssubjekte“.

[65] So im Kern auch *Reinhardt*, AöR 2017, 528 (538 f.), ohne dass dieser dieselbe Erkenntnis für die Schutzpflichtendimension herausstellt: „[…] bedarf es sowohl zur Beurteilung der Schwere eines Eingriffs als auch zur Strukturierung der Abwägung der betroffenen Grundrechte eines Rückgriffs auf substantielle Maßstäbe.“

[66] *Marsch*, Das europäische Datenschutzgrundrecht, S. 261 f.

[67] In eine ähnliche Richtung lässt sich auch das BVerfG verstehen, wenn es in seinem Beschluss v. 06.11.2019, 1 BvR 16/13, Rn. 89 zum Verhältnis zwischen informationeller Selbstbestimmung und allg. Persönlichkeitsrecht ausführt: „Dementsprechend enthält es keinen gesamthaften Schutzanspruch hinsichtlich jederlei Umgangs mit Informationen, der die übrigen Schutzdimensionen des Grundrechts allgemein übergreifen und zusammenführen würde, sondern lässt deren Wertungen und Abwägungsregeln unberührt.“

[68] Vgl. *Bäcker*, Der Staat 2012, 91 (105 f.), der diesbezüglich eine konkrete Schutzpflicht erst bei erheblichen Gefährdungen der Entfaltungsfreiheit aktiviert sehen will.

[69] *Marsch*, Das europäische Datenschutzgrundrecht, S. 263 f.

[70] *Bäcker*, Der Staat 2012, 91 (109).

eine solch gering verdichtete Schutzpflicht vermittelten Legitimation zum Eingriff in Grundrechte von Daten verarbeitenden privaten Akteuren.[71] *Marsch* greift daher zusätzlich auf die bereits erwähnte Ausgestaltungsdimension des Art. 8 Abs. 1 GRCh zurück und schreibt dieser zwar – anders als im Bereich öffentlicher Datenverarbeitungen – ebenfalls keine die gesetzgeberische Ausgestaltungsfreiheit einschränkende Pflicht, jedenfalls aber eine sog. eingriffsrechtfertigende Strukturermächtigung zu:[72] Dem subsidiären Rang von Art. 8 Abs. 1 GRCh innerhalb der mehrdimensionalen Schutzdimensionen des Datenschutzgrundrechts nach *Marschs* Verständnis entsprechend soll diese den Gesetzgeber dort, wo sich (noch) keine Schutzpflicht aus einem bereits konkret gefährdeten Freiheitsgrundrecht ableiten lässt, zumindest zur gesetzlichen Strukturierung und Begrenzung privater Datenverarbeitungen durch generalisierende Regelungen zur Abwehr noch abstrakter und nicht verdichteter Gefahren sowie – noch früher ansetzend – zur Vorsorge vor Risiken[73] ermächtigen und die damit einhergehenden Grundrechtsbeschränkungen der betroffenen Datenverarbeiter rechtfertigen. Dass in konkreten Fällen eine Verdichtung zu einer konkreten Gefahr für ein Freiheitsgrundrecht wie bspw. Art. 7 GRCh eintritt, ist dadurch nicht ausgeschlossen, aber aus Perspektive des Gesetzgebers auch nicht schädlich: Gerade durch die generalisierende Regelung aller privaten Datenverarbeitungen verbleiben zahlreiche abstrakte Regelungen mit unbestimmten Rechtsbegriffen, deren Auslegung im Wege gerichtlicher Überprüfung unter Rückgriff auf grundrechtliche Wertungen zu erfolgen hat.

b) Das Recht auf informationelle Selbstbestimmung deutschen Vorbilds

Im Rahmen der mitgliedstaatlichen Anwendung der DSGVO ist daneben unter Umständen auch das deutsche Verfassungsrecht von Relevanz.[74]

So war noch zu Zeiten der DSRL das zentrale datenschutzrechtliche Grundrecht lange das vom BVerfG im Volkszählungs-Urteil[75] aus dem allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG[76] fortentwickelte

---

[71] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, S. 264 ff.

[72] *Marsch*, Das europäische Datenschutzgrundrecht, S. 268 f.

[73] Dabei soll hier, mit *Heun*, RW 2011, 376 (380), ein weiter Risikobegriff zugrunde gelegt werden, der „erstens eine Ungewissheit über die Zukunft voraus[setzt] und zweitens die Möglichkeit eines irgendwie gearteten Schadenseintritts auf der einen Seite sowie auch meistens – wenn nicht immer – die Möglichkeit eines Gewinns oder anderer positiver Entwicklungen auf der anderen Seite". Siehe zudem die Begriffserläuterungen *supra* bei Einleitung E.

[74] Zur Bedeutung des Grundgesetzes für die Implementation der Unionsgrundrechte siehe *Bäcker*, EuR 2015, 389 (389 ff.).

[75] BVerfGE 65, 1.

[76] Seinerseits einst vom BVerfG als eigenes Grundrecht hergeleitet, siehe etwa BVerfGE 34, 238. Auch hier war bereits anerkannt, dass der Schutzbereich die Geheimhaltung persönlicher Lebenssachverhalte umfasst, vgl. BVerfGE 56, 37 (41 ff.).

Recht auf informationelle Selbstbestimmung.[77] Diesem zufolge hat der Einzelne grundsätzlich die Entscheidungsbefugnis darüber, wem er wann, zu welchen Verwendungszwecken und in welchem Ausmaß persönliche Lebenssachverhalte preisgibt.[78] Im Interesse der ungestörten Persönlichkeitsentwicklung und -ausübung soll es dem Einzelnen nicht zugemutet werden, im völlig Ungewissen darüber zu verbleiben, welche Informationen sein Umfeld über ihn hat. Geschützt werden sollte somit insbesondere die ungehemmte Persönlichkeitsentwicklung in Zeiten infolge rapider technischer Entwicklungen zunehmend ubiquitärer Datensammlungen und -verarbeitungen sowie zunehmender Möglichkeiten, Daten auch noch nachträglich miteinander zu verknüpfen und so über unerwartete Verwendungsmöglichkeiten unvorhergesehene Rückschlüsse über den Einzelnen ziehen zu können.[79] Das daraus folgende Credo, dass es unter den Bedingungen moderner und automatischer Datenverarbeitung kein wirklich belangloses Datum mehr gibt[80], verdeutlicht den Unterschied zum „klassischen" allgemeinen Persönlichkeitsrecht, bei dem nach Maßgabe der Sphärentheorie noch ein abgestuftes Modell der Schutzwürdigkeit je nach (etwa räumlicher) Nähe des betroffenen Sachverhalts zur Privatsphäre des betroffenen gilt.[81] Gleichzeitig betonte das BVerfG bereits zu diesem Zeitpunkt, gewissermaßen im gleichen Atemzug, dass dieses Recht dem Einzelnen nicht schrankenlos zusteht, sondern im Kontext seiner Stellung innerhalb der sozialen Gemeinschaft zu verstehen ist. Einschränkungen sollten daher im überwiegenden Allgemeininteresse hinzunehmen sein.[82]

Wurde die „Erschaffung" des Grundrechts in der deutschen und auch europäischen Literatur grundsätzlich wohlwollend aufgenommen und teilweise gar als (auf wissenschaftliche Vorarbeiten aufbauender) Meilenstein der datenschutzrechtlichen Entwicklung weit über den konkret entschiedenen Fall hinaus tituliert,[83] mangelt es gleichzeitig nach wie vor nicht an breiter Kritik an dem konkreten Grundrechtskonzept.[84] Im Fokus dieser steht nach wie vor

---

[77] BVerfGE 65, 1 (41 ff.). Flankiert durch die spezielleren Grundrechte wie das auf Schutz der Vertraulichkeit der Kommunikation (Art. 10 GG) und das ebenfalls aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitete Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Vgl. BVerfGE 120, 274 (313).

[78] BVerfGE 65, 1 (43); 118, 168 (184); 120, 274 (312).

[79] BVerfGE 65, 1 (45).

[80] BVerfGE 65, 1 (45).

[81] Vgl. *Grimm*, JZ 2013, 585 (586).

[82] BVerfGE 65, 1 (43 ff.).

[83] Die Programmatik des Urteils generalisierend weiterdenkend etwa *Bäumler*, JR 1984, 361 (361 ff.); *Simitis*, NJW 1984, 398 (398 ff.).

[84] Eher kritische Stimmen aus der Zeit des Urteils finden sich etwa bei *Hufen*, JZ 1984, 1072 (1072 ff.). Vgl. auch *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung; *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?; für die jüngere Vergangenheit siehe exemplarisch *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, S. 123 f.; ein guter Überblick über die verschiedenen

in erster Linie der leicht als herrschaftsrechtlich zu deutende und Eigentumsanalogien hervorrufende Ansatz der Befugnis des Individuums über „seine" Daten.[85] Da Daten zunächst bloße auf Datenträgern verewigte Zeichen seien, die erst durch Interpretation und Kontextanreicherung anderer Personen zu Informationen mit eigenständigem Sinngehalt gemacht würden,[86] sei eine auch nur annähernd verfügungsbefugnisbezogene Konzeption von vornherein zum Scheitern verurteilt, würde sie doch wahlweise etwas Unmögliches (in Form einer Verfügungsbefugnis über Informationen und damit etwas, das sich erst im Gedanken- und Beobachtungsprozess anderer Personen bildet und damit schlicht nicht beherrschbar ist) oder normativ nicht Erforderliches (in Form einer Verfügungsbefugnis über Daten, die gerade noch nicht mit Kontext und Sinn angereichert wurden und daher noch keine Beeinträchtigung nach sich zögen) gewähren.[87] Ähnliche Kritik entzündet sich an dem damit eng verbundenen klassisch abwehrrechtlichen Kern des Grundrechts, der als für die Komplexität des Schutzguts ungeeignet und insbesondere, aber nicht ausschließlich, für den zunehmend relevanter werdenden Umgang mit Daten zwischen Privaten mit jeweils eigenen Grundrechtspositionen, „übergestülpt" abgetan wird.[88] Ein Großteil dieser Kritik fokussiert sich darauf, dass in der Konsequenz die soziale Dimension von Datenverarbeitungen und nachgelagerten Informationsverarbeitungen und -nutzungen nicht schon im Schutzbereich, sondern erst

---

Literaturverständnisse findet sich zudem bei *Drackert*, Die Risiken der Verarbeitung personenbezogener Daten, S. 239 ff.

[85] Vgl. statt vieler: *Albers*, Informationelle Selbstbestimmung, S. 151 ff.; *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft: ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, S. 561 (566 ff.); aus dieser Kritik heraus will *von Lewinski*, Die Matrix des Datenschutzes, S. 40 ff. das Selbstbestimmungskonzept durch eines der „informationellen Fremdbeschränkung" ersetzen. Siehe auch *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft: Symposium des Centre for Security and Society, S. 167 (178 ff.), der ein Verständnis des Recht auf informationelle Selbstbestimmung als Schutz vor Grundrechtsgefährdungen verfolgt. Vgl. ebenfalls *Reinhardt*, AöR 2017, 528 (536): „Werden einige Formulierungen des Gerichts isoliert, lässt sich das Grundrecht im Sinn einer umfassenden Verfügungsbefugnis über persönliche Daten verstehen […]."

[86] Hierzu grundlegendend *Albers*, Informationelle Selbstbestimmung, S. 280 ff.; ausführlicher dazu *infra* bei II. 1. b.

[87] *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft: ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, S. 561 (567 f.).

[88] Vgl. allgemein zu komplexen Geflechten widerstreitender Grundrechte *Hoffmann-Riem*, EuGRZ 2006, 492 (493): „Die Aufgabe der Freiheitssicherung in mehrpoligen Rechtsbeziehungen und damit möglichst unter Bewältigung von (tri- oder sonstigen multipolaren) Konflikten muss sich von der Konzentration auf die abwehrrechtliche Dimension der Freiheitsrechte lösen." Diese Kritik beschränkt sich nicht auf das BVerfG und die deutsche Grundrechtskonzeption, sondern wird zuweilen auch am EuGH und seinem Verständnis der GRCh geübt, vgl. *Reinhardt*, AöR 2017, 528 (562): „Aufgrund der Struktur der Abwägung, die schlicht dem Schema der Rechtfertigung von staatlichen Eingriffen in grundrechtliche Freiheitssphären folgt, kann das Spektrum an widerstreitenden Grundrechtspositionen nicht mehr angemessen in den Blick kommen." Vgl. auch *Franzius*, ZJS 2015, 259 (261).

auf Rechtfertigungsebene berücksichtigt wird.[89] Richtigerweise ist das Recht auf informationelle Selbstbestimmung daher neben diesem unumstritten vorhandenen und relevanten abwehrrechtlichen Kern auch im Lichte seiner objektiv-rechtlichen Funktion zu verstehen: Die Freiheit, das eigene Leben und den sozialen und gesellschaftlichen Umgang mit der Umgebung trotz zunehmend ubiquitären Umgangs mit personenbezogenen Daten, sich rapide entwickelnden Möglichkeiten der umfangreichen Speicherung, Verkettung und Kombination von Daten, der daraus folgenden Generierung von Informationen, Erkenntnissen und Rückschlüssen, sowie der häufigen Konzentration dieser Daten und Informationen bei wenigen großen und mächtigen Akteuren, selbstbestimmt zu führen, stellt heutzutage keinen Naturzustand mehr dar. Es genügt daher nicht, im Sinne der abwehrrechtlichen Funktion allein staatliche Eingriffe in diese Freiheit unter den Vorbehalt der Verfassungsmäßigkeit zu stellen, sondern bedarf zusätzlich staatlicher Strukturierung und Absicherung, um diese Freiheit überhaupt zu ermöglichen.[90] Dies gilt umso mehr für den Bereich des privaten Datenschutzrechts, in dem die (zumindest dem Wortlaut nach) herrschaftliche Konzeption des Grundrechts leicht dazu verleitet, die Verarbeitung durch andere, ihrerseits Grundrechte tragende und ausübende, Private unmittelbar als Eingriff zu sehen, den es zu rechtfertigen gilt.[91] Dieses Verständnis wird nicht zuletzt dadurch bedingt, dass die Ausgestaltung des einfachen Datenschutzrechts als grundsätzliches Verbot mit Erlaubnisvorbehalt leicht für Verwechslungen bzw. falsche Gleichsetzungen sorgt, wie noch zu zeigen sein wird. Der einfachgesetzliche Erlaubnisvorbehalt sollte jedoch nicht mit der grundrechtlichen Rechtfertigungsbedürftigkeit verwechselt werden, die einfachgesetzlich grundsätzlich verbotene Datenverarbeitung nicht mit einem grundrechtlichen Eingriff.[92] Richtigerweise fordert das Recht auf informationelle Selbstbestimmung nach diesem Verständnis im privaten Bereich also vielmehr eine Schutzkonzeption, die die durch Datenverarbeitungen entstehenden Risiken in ihrer Komplexität und insbesondere ihrer gesamtheitlichen und gesellschaftsbezogenen Bedeutung[93] erkennt und begrenzt und gleichzeitig die aufeinander-

[89] Vgl. *Franzius*, ZJS 2015, 259 (263).

[90] Vgl. *Albers*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 213 (216 f.) zu diesem überkommenen streng abwehrrechtlichen Verständnis von Grundrechten: „Consequently, fundamental rights are directed solely toward the protection of freedoms that already exist. The social preconditions of individual freedom or, expressed more radically and more precisely, the social foundation and embeddedness of individual freedom are not given consideration."

[91] So explizit *Roßnagel*, NJW 2019, 1 (5): „Jede Verarbeitung personenbezogener Daten ist ein Eingriff in die Grundrechte auf Privatleben nach Art. 7 GRCh, auf Datenschutz nach Art. 8 GRCh und auf informationelle Selbstbestimmung nach Art. 2 i. V. m. Art. 1 I GG."

[92] So aber *Roßnagel*, NJW 2019, 1 (5).

[93] Vgl. *Albers*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 213 (227): „[…] data protection does not encompass a uniform legally protected good. On the contrary, there are complex and manifold interests that are to be protected."

treffenden multipolaren Grundrechte miteinander in Einklang bringt.[94] Davon umfasst sind daher nicht isoliert die einzelne Datenverarbeitung und ihre Begrenzung, sondern nicht zuletzt auch die daraus potenziell zu gewinnenden Informationen, die möglichen Verwendungskontexte, die auf ihrer Basis ggf. zu treffenden Entscheidungen sowie die Verhaltensweisen, die dadurch bei allen Beteiligten ermöglicht, verunmöglicht, erleichtert, erschwert oder abgeschreckt werden. Trotz dieses erweiterten Fokus auf die eigentlichen Gefahrenpotentiale durch Informationen und nicht Daten, behält die Strukturierung des Umgangs mit Daten mit Blick auf die Vorfeldschutzfunktion des Datenschutzes ihre Notwendigkeit:

„Datenschutz schützt schon dann, wenn es noch nicht wehtut. Das irritiert – ist aber die Pointe des Datenschutzes. Wenn wir warten, bis sich die gespeicherten Daten unmittelbar in Maßnahmen niederschlagen, brauchen wir eigentlich keinen Datenschutz, sondern nur Schutz gegen die Maßnahmen."[95]

Klar ist bei alledem, dass spätestens mit Geltung der DSGVO[96] eine nahezu vollständige europarechtliche Determinierung des Datenschutzrechts, jedenfalls im nicht-öffentlichen Bereich,[97] eingetreten ist.[98] sodass das Recht auf informationelle Selbstbestimmung nach deutscher Grundrechtstradition in seiner unmittelbaren Bedeutung stark abgenommen hat und weiter abnehmen wird.[99]

---

[94] So auch *Franzius*, ZJS 2015, 259 (261): „Daraus folgt jedoch kein strikter Gesetzesvorbehalt für private Datenverarbeitungsvorgänge, sondern im Grunde nur, dass ein rechtlicher Rahmen zur tatsächlichen Sicherung des informationellen Selbstschutzes bereitgestellt wird."

[95] *Masing*, in: Nettesheim u. a., VVDStRL 70, S. 86.

[96] Und mit Blick auf den vollharmonisierenden Charakter der DSRL genau genommen auch schon mit dieser, vgl. *Brühann*, EuZW 2009, 639 (642 ff.). Siehe auch BVerfG, Beschluss v. 06.11.2019, 1 BvR 276/16, Rn. 39 m. w. N. zur diesbezüglichen ständigen Rechtsprechung des EuGH.

[97] Zum Anwendungsbereich nationalen Datenschutzrechts im öffentlichen Bereich siehe *Klement*, JZ 2017, 161 (165 f.).

[98] Mitgliedstaatliche Grundrechte kommen innerhalb der DSGVO einzig noch bei der Nutzung der durch Öffnungsklauseln wie Art. 8 Abs. 1 S. 3 oder Art. 85 DSGVO, teils als expliziter Auftrag, teils fakultativ, gewährten Regelungs- und Umsetzungsspielräume unmittelbar zur Geltung, vgl. *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 234. Die eigene Prüfungskompetenz am Maßstab nationaler Grundrechte erst kürzlich betonend BVerfG 1 BvR 16/13 (Recht auf Vergessen I), Beschluss v. 29.11.2019, Rn. 39ff; für einen Überblick über die verbleibenden nationalen Regelungsbereiche in der DSGVO siehe *Dammann*, ZD 2016, 307 (310 ff.); ausführlich und instruktiv zudem *Kühling* u. a., Die Datenschutz-Grundverordnung und das nationale Recht: Erste Überlegungen zum innerstaatlichen Regelungsbedarf, S. 2 ff.; die Schwierigkeiten bei der Beurteilung der Reichweite mitgliedstaatlicher Regelungsbefugnisse betonend *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (328 f.); einen guten Überblick liefert zudem *Laue*, ZD 2016, 463 (463 ff.).

[99] *Franzius*, ZJS 2015, 259 (270): „Das Recht auf informationelle Selbstbestimmung wird dadurch nicht verdrängt, in seiner Bedeutung für die Anleitung des Gesetzesrechts aber relativiert. Ob es ratsam ist, auf einen Export dieser dogmatischen Figur zu setzen, erscheint zweifelhaft." Als bedeutsam zu erwähnen ist hier zudem, dass jüngst auch das BVerfG dazu überging, im Falle unionsrechtlich vollständig vereinheitlichter Regelungen staatliches Handeln

Mittelbare Bedeutung kommt ihm jedoch über Art. 52 Abs. 4 GRCh, nach welchem Charta-Grundrechte im Einklang mit mitgliedstaatlichen Verfassungsüberlieferungen ausgelegt werden sollen, sowie über Art. 6 Abs. 3 EUV, wonach nationale Grundrechte als allgemeine Rechtsgrundsätze und damit Grundrechtsschicht fortleben,[100] weiter zu.[101] Eine starke inhaltliche Prägung der Charta-Grundrechte durch die Grunddogmatik einer informationellen Selbstbestimmung *herrschaftsrechtlichen* Verständnisses ist dennoch, nicht nur aufgrund der geschilderten umfangreichen Kritik in der deutschen Literatur, nicht zu erwarten; ein solches Verständnis bzw. die explizite Aufnahme eines „right to informational self-determination" wurde im EU-Grundrechtekonvent ausführlich diskutiert und letztlich ausdrücklich abgelehnt.[102] Versteht man das Grundrecht, insbesondere im privaten Bereich, hingegen primär als Strukturvorgabe (mit subjektivrechtlichen Einschlägen)[103] für einen bereits auf Ebene der Risikosteuerung ansetzenden Schutz vor den durch Datenverarbeitungen drohenden Gefahren (inklusive darauf basierender möglicher Informationsgewinnung und -verwendung, Entscheidungsfindung, Wissensgenerierung, Kontextänderungen etc.), das gleichzeitig in adäquater Weise die widerstreitenden Grundrechte und Interessen der Datenverarbeiter und des gesamten kommunikativen Umfelds berücksichtigt,[104] so ist ohnehin keine größere Diskrepanz mit dem eingangs beschrieben Verständnis des europäischen Datenschutzgrundrechts festzustellen.[105] Das soll keine völlige Kongruenz, insbesondere mit der oben wieder-

deutscher Stellen am Maßstab der Unionsgrundrechte zu kontrollieren, vgl. BVerfG 1 BvR 276/17 (Recht auf Vergessen II), Beschluss v. 06.11.2019, Rn. 50 ff.

100 Vgl. EuGH, Rs. C-555/07 (Kücükdeveci), ECLI:EU:C:2010:21 Rn. 21 f.

101 Wobei diese Bedeutung hinter der der EMRK zurückbleibt. Zur Einschätzung mitgliedstaatlichen Verfassungsrechts als auslegungsrelevante Inspirationsquelle siehe *Marsch*, Das europäische Datenschutzgrundrecht, S. 51 f.; dieser wurde bei dieser Einschätzung wiederrum stark geprägt von *Klement*, Wettbewerbsfreiheit, S. 20 ff. und seinem Konzept der „lernenden Grundrechtstheorie".

102 Vgl. *Hustinx*, EU-Datenschutzrecht: Die Überprüfung der Richtlinie 95/46/EG und die vorgeschlagene Datenschutz-Grundverordnung, S. 20. Dies hält jedoch einige Stimmen nicht davon ab, ein ähnlich herrschaftsrechtliches Verständnis in Fortführung des (so verstandenen) Gedankens informationeller Selbstbestimmung auch auf die europäische Debatte zu übertragen, vgl. etwa *Hijmans*, The European Union as Guardian of Internet Privacy, S. 54 f. In diese Richtung gehend auch *Klement*, JZ 2017, 161 (169); *Roßnagel*, NJW 2019, 1 (2); siehe ausführlicher zu dem Verhältnis *Kranenborg*, in: Peers u. a., The EU Charter of Fundamental Rights, Art. 8 Rn. 08.25 ff.; den Entwicklungsprozess von Art. 8 GRCh gut nachzeichnend auch *Cannataci/Mifsud-Bonnici*, Information & Communications Technology Law 2005, 5 (9 f.).

103 *Franzius*, ZJS 2015, 259 (265).

104 Nach *Trute*, in: Roßnagel, Handbuch Datenschutzrecht: die neuen Grundlagen für Wirtschaft und Verwaltung, S. 43 Rn. 6, sei Ziel dieser Vorgabe ein „mehrdimensionales Konzept, das sein Gravitationszentrum in der kommunikativen Selbstbestimmung der Persönlichkeit hat und deren Leitbild nicht das Datengeheimnis, sondern die Wahrung von Selbstbestimmung in einer Datenverkehrsordnung ist."

105 So auch *Kühling/Raab*, in: Kühling/Buchner, DSGVO/BDSG, Einführung DSGVO Rn. 26.; ebenso *Peuker*, Verfassungswandel durch Digitalisierung, S. 321: „[…] sind Parallelen in der wissenschaftlichen Deutung […] unverkennbar."

gegebenen komplexen Auffächerung des europäischen Datenschutzgrundrechts nach *Marsch*, insinuieren. Doch sind die Parallelen teils größer als auf den ersten Blick anzunehmen,[106] und auch mit Blick auf das bisherige einfachgesetzliche nationale Regelungskonzept in Form des BDSG näher an dem – noch zu erörternden – Regelungskonzept der DSGVO, als dies bei vielen anderen Mitgliedstaaten der Fall war.

2. Freier Datenverkehr

Neben dem Schutz natürlicher Personen enthält Art. 1 Abs. 1 DSGVO auch den freien Verkehr personenbezogener Daten als Bezugspunkt für die in der Verordnung enthaltenen Vorschriften. Art. 1 Abs. 3 DSGVO führt weiter aus, dass der Schutz natürlicher Personen nicht dazu führen darf, dass der Verkehr personenbezogener Daten eingeschränkt oder verboten wird. Doch ergibt sich daraus eine normative Entscheidung zugunsten eines dem Schutz natürlicher Personen ebenbürtigen und mit diesem auszutarierenden Schutzguts? Gegen ein solches Verständnis spricht nicht zuletzt die Tatsache, dass das Ideal eines *freien*, also von den Hürden unterschiedlicher nationaler Datenschutzgesetze befreiten, Datenverkehrs bereits die automatische Kehrseite eines einheitlichen datenschutzrechtlichen Regelungswerks innerhalb der Union darstellt und somit in jedem Fall erreicht wird[107] – durch die DSGVO als unmittelbar geltende Verordnung in noch stärkerem Maße als zuvor durch die DSRL[108] und ihre mitgliedstaatlichen Umsetzungen.[109] Einem darüber hinaus gehenden Verständnis des freien Verkehrs im Sinne einer Abwesenheit eines zu hohen Schutzniveaus und somit einer Verringerung desselbigen erteilte auch der EuGH in seinen Entscheidungen mehrfach eine Absage und betonte im Gegenzug das Ideal eines hohen Schutzniveaus in der Gemeinschaft.[110] Hinzu kommt, dass die DSGVO – anders als noch die DSRL zum Zeitpunkt ihres Erlasses – auf Grundlage von

---

[106] So wird auch hinsichtlich der informationellen Selbstbestimmung eine Neukonzeption auf Basis eines instrumentellen Verständnisses als dienendes Recht zur Sicherung anderer Freiheitsgrundrechte erwogen, vgl. *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft: ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, S. 561 (566 ff.). Kritisch dazu *Franzius*, ZJS 2015, 259 (265) m. w. N.

[107] Vgl. *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Art. 1 DSGVO Rn. 35: „Dies ist aber nichts anderes als das dem Grundkonzept der EU stets innewohnende Anliegen des einheitlichen Binnenmarktes, wie es in Art. 26 EUV statuiert wird. Datenschutz und Binnenmarktanliegen befinden sich insoweit für die DSGVO grundsätzlich im Gleichlauf: Beide wünschen eine einheitliche Umsetzung der bestehenden Vorschriften […]."

[108] Die den freien Datenverkehr in ihrem Art. 1 Abs. 2 ebenso als Ziel formulierte.

[109] Wenn auch die effektive Harmonisierung aufgrund der zahlreichen Öffnungsklauseln der DSGVO bisweilen angezweifelt wird, vgl. etwa *Buchner*, in: Kühling/Buchner, DSGVO/BDSG, Art. 1 DSGVO Rn. 20. Zur Bedeutung der Wahl einer Verordnung für ein solch breites Feld wie dem Datenschutz siehe *de Hert/Papakonstantinou*, CLSR 2016, 179 (182 f.).

[110] Siehe etwa EuGH, Rs. C-101/01 (Lindqvist), ECLI:EU:C:2003:596 Rn. 95 und EuGH, verb. Rs. C-468/10 und C-469/10 (ASNEF./.FECEMD), ECLI:EU:C:2011:777 Rn. 28.

Art. 16 Abs. 2 AEUV und damit explizit zum Zweck des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten erlassen wurde.[111]

Einer „Hochzonung" zu einer Zielsetzung mit eigenständigem normativen Wert bedarf es daher nicht.[112] Der freie Datenverkehr bleibt insofern für die Bestimmung des Regelungszwecks der DSGVO außer Betracht.

3. Zwischenergebnis: Konsequenzen für das private Datenschutzrecht

Zusammenfassend lässt sich festhalten, dass die DSGVO den Schutz personenbezogener Daten als ihr primäres Schutzziel formuliert und zusätzlich die Tür für einen Einbezug anderer Grundrechte öffnet. Unter den verschiedenen Ansätzen zu einer Strukturierung und Differenzierung der dogmatischen Grundlagen des europäischen Datenschutzgrundrechts gelingt es dem von *Marsch* gewählten am besten, die vom EuGH nur stiefmütterlich behandelte Frage zum Verhältnis zwischen Art. 7 und 8 GRCh auf allen Ebenen und nicht nur punktuell zielführend aufzulösen. Die von ihm propagierte Verankerung des materiellen Schutzguts im Privatleben und damit in Art. 7 GRCh ist nicht neu[113] und setzt fort, was in der jüngsten EuGH-Rechtsprechung bereits anklang, ohne dort explizit benannt worden zu sein. Neu und überzeugend ist die Auflösung der Konkurrenz zwischen den verschiedenen Schutzdimensionen im Wege der Subsidiarität. Zudem erlaubt insbesondere die, ebenfalls in Einzelheiten bereits so interpretierte, *freiheitsakzessorische* Dimension und ihre Verknüpfung von Art. 8 GRCh mit einschlägigen anderen Freiheitsgrundrechten die (teilweise) Auflösung der eingangs angesprochenen Problematik der vermeintlich zu offenen Formulierung in Art. 1 Abs. 2 DSGVO: Versteht man einen Teilaspekt des Datenschutzgrundrechts darin, andere in ihrem Schutzbereich betroffene Freiheitsgrundrechte hinsichtlich der spezifisch durch die Verarbeitung personenbezogener Daten resultierenden Beschränkungen zu ergänzen, so erklärt dies das weit gefasste Schutzziel (potenziell) *aller* Grundrechte und Grundfreiheiten und begrenzt die Auswirkungen eines solchen Schutzverständnisses gleichzeitig, da der Verweis nur über den Transmissionsriemen des Art. 8 GRCh und die spezifischen mit Datenverarbeitungen einhergehenden Gefahren eröffnet wird.

Für die umfassende Regelung privater Datenverarbeitungen durch die DSGVO und das in ihr normierte Konzept der Verantwortlichkeit bedeutet die-

---

[111] Vgl. *van der Sloot*, in: Leenes/van Brakel/Gutwirth/de Hert, Data Protection and Privacy: (In)visibilities and Infrastructures, S. 3 (10 f.); so auch *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Art. 1 DSGVO Rn. 33.

[112] So auch *Schantz*, in: BeckOK Datenschutzrecht, Art. 1 DSGVO Rn. 3; in die gleiche Richtung gehend *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Art. 1 DSGVO Rn. 21 mit zusätzlichem Verweis auf die Stärkung des freien Binnenmarktes durch Sanktionierung von unlauteren Wettbewerbsvorteilen in Form von Datenschutzrechtsverstößen; a. A. aber *Plath*, in: Plath, DSGVO/BDSG, Art. 1 DSGVO Rn. 6.

[113] Siehe etwa *Buchholtz/Stendel*, in: Gierschmann u. a., DSGVO, Art. 1 Rn. 32 ff.

ses Schutzgut mit Blick auf eine fehlende unmittelbare Drittwirkung des Datenschutzgrundrechts Folgendes: In ihr realisiert sich in erster Linie der Ausgestaltungsauftrag des Art. 8 GRCh, von dem der EU-Gesetzgeber Gebrauch gemacht hat und der ihn in Form einer eingriffsrechtfertigenden Strukturierungsermächtigung[114] zu dem damit einhergehenden Eingriff in die Grundrechte datenverarbeitender Privater legitimiert. Zu einer Pflicht zu einer *konkreten* Art der Ausgestaltung – insbesondere bzgl. der in Art. 8 Abs. 2 GRCh normierten Strukturprinzipien – verdichtet sich dabei aufgrund der zunächst sehr abstrakten Gefährlichkeit privater Datenverarbeitungsvorgänge[115] weder der Auftrag aus Art. 8 GRCh, noch materialisiert sich eine Schutzpflicht aus Art. 7 GRCh oder einem anderen Freiheitsgrundrecht.[116] Anders formuliert: Die nahezu umfassende Regulierung aller privaten Datenverarbeitungen[117] und insbesondere der Gleichlauf zwischen den Regeln für private und öffentliche Datenverarbeitungen war unionsgrundrechtlich zwar nicht geboten[118], aber auch nicht verboten, stellt also ein legitimes, aber nicht das einzig denkbare[119] Ergebnis der gesetzgeberischen Ausgestaltungsfreiheit im Spannungsfeld der von der Verarbeitung personenbezogener Daten (und ihren Folgen) tangierten Grundrechte dar.[120] Gleichzeitig lässt sich dadurch noch keine Aussage darüber treffen, ob nicht einzelne Teilregelungen spezifischer Verarbeitungsumstände innerhalb der DSGVO ihrerseits Sachverhalte regeln, innerhalb derer sich die mit der Verarbeitung einhergehenden Gefahren dergestalt konkretisiert haben, dass eine grundrechtliche Schutzpflicht aktiviert und der gesetzgeberische Gestaltungsspielraum infolgedessen eingeschränkt[121] war. Auch lässt sich im Umkehrschluss nicht pauschal beantworten, ob nicht in bestimmten, beson-

[114] *Marsch*, Das europäische Datenschutzgrundrecht, S. 268 f.

[115] So auch *Grimm*, JZ 2013, 585 (586), der von personenbezogenen Daten als (bloße) Gefahrenquelle spricht.

[116] So auch *Klement*, JZ 2017, 161 (162), demzufolge auch „der kühnste Interpret" nicht zum Ergebnis einer derartig ausgerichteten Schutzpflicht kommen könne.

[117] Von einigen wenigen Ausnahmen wie der Haushaltsausnahme in Art. 2 Abs. 2 lit. c und dem, von der Ausübung durch die Mitgliedstaaten abhängigen, sog. Medienprivileg in Art. 85 DSGVO einmal abgesehen.

[118] So auch schon zum Recht auf informationelle Selbstbestimmung *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 54.

[119] Kritisch zur Wahl einer einheitlichen Regelung des öffentlichen und privaten Datenschutzrechts etwa *Marsch*, Das europäische Datenschutzgrundrecht, S. 259 f.; gegen das unter Erlaubnisvorbehalt stehende grundsätzliche Generalverbot von Datenverarbeitungen argumentierend *Veil*, NVwZ 2018, 686 (688 f.).

[120] Ähnlich hinsichtlich einer bloßen rechtspolitischen Entscheidung für die konkrete Ausgestaltung des privaten Datenschutzrechts auch *Grimm*, JZ 2013, 585 (587 f.); zu diesem Ergebnis kommt auch *Reinhardt*, AöR 2017, 528 (556): „Dass sich das Sekundärrecht durch eine weitgehende Parallelisierung der Datenverarbeitung öffentlicher und nicht-öffentlicher Stellen auszeichnet, ist zunächst Ausdruck einer gesetzgeberischen Entscheidung." Ähnlich auch bereits zum Recht auf informationelle Selbstbestimmung *Albers*, Informationelle Selbstbestimmung, S. 583.

[121] Vgl. BVerfGE 77, 170 (214) und 88, 203 (262).

ders grundrechtssensiblen, Bereichen das die im Rahmen einer Schutzpflicht bestehenden Grenzen der Ausgestaltungsfreiheit kennzeichnende Untermaßverbot[122] verletzt wurde;[123] der in seinem Anwendungsbereich (zumindest seinem Wortlaut nach) auf *ausschließlich* auf automatisierten Verarbeitungen beruhende Entscheidungen begrenzte[124] Art. 22 DSGVO wäre mit Blick auf das Gefährdungspotential[125] auch *solcher* menschlicher Entscheidungen, die durch algorithmische Entscheidungen oder Tendenzen auf Basis personenbezogener Daten *vorgeprägt* wurden, ein solcher Kandidat.

II. Die konkreten Gefahren für Individuum und Gesellschaft

Unabhängig von ihrer grundrechtsdogmatischen Anbindung und der Frage der etwaigen Aktivierung einer staatlichen Schutzpflicht, lohnt ein Blick auf die konkreten faktischen Gefahren, die im Zusammenhang mit (privaten) Datenverarbeitungen und damit als Erwartungshaltung an zeitgemäße Datenschutzgesetzgebung diskutiert werden. Hier zeigt sich, dass trotz teilweise stark divergierender Grundrechtskonstruktionen im nationalen (1. a)) und internationalen (1. b)) Vergleich grundsätzlich ähnliche Topoi individueller Gefahren gebildet werden. Auch Erwägungen hinsichtlich überindividueller Gefahren (2.) finden sich länderübergreifend. Im Anschluss soll ein kurzer Abgleich mit der DSGVO (3.) aufzeigen, wie sich das Ziel der Abwehr dieser Gefahren in einzelnen Bestimmungen wiederfindet.

1. Individuelle Gefahren

a) In der deutschen Literatur

aa) Gefahren durch Informationsverwendung in neuen Kontexten

Ein erstes Fundament der Systematisierung dessen, welche konkreten Gefahren durch (private) Datenverarbeitungen drohen können, kann in Bezug auf das Recht auf informationelle Selbstbestimmung *Albers* zugeschrieben werden. Ihr Ansatz, zunächst streng zwischen den bloßen zu verarbeitenden *Daten* und den daraus später (mittels Anreicherung mit Kontext und Interpretation – kurz ge-

---

[122] Vgl. *Canaris*, AcP 1984, 201 (227 ff.); *ders*., Grundrechte und Privatrecht, S. 83 ff.

[123] Wie später (bei B. III.) noch ausführlicher zu begründen sein wird, wird hier mangels hinreichend gefestigter unionsgrundrechtlicher Schutzpflichtendogmatik die deutsche Grundrechtsdogmatik bemüht. Für einen der wenigen Ansätze zur Konturierung einer unionsgrundrechtlichen Dogmatik siehe die dort genannten Quellen sowie stellvertretend *Suerbaum*, EuR 2003, 390 (408 ff.).

[124] So auch die gängige Interpretation in der Literatur. Stellvertretend für viele etwa *von Lewinski*, in: BeckOK Datenschutzrecht, Art. 22 Rn. 21.

[125] Ausführlich dazu *Bayamlioglu*, EDPL 2018, 433 (435 f.); mögliche Limitierungen der Norm betonend auch *Dreyer/Schulz*, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?

sagt: Sinngehalt – durch die jeweiligen Rezipienten) entstehenden *Informationen* zu unterscheiden und konkrete Gefahren für das Individuum in erster Linie in den Handlungen bzw. Entschlüssen zu diesen zu sehen, die auf Basis des aus den Informationen gewonnen Wissens ausgeführt bzw. gefasst werden, erleichtert die Betrachtung. Daten bilden demnach die Grundlage von Informationen und können, je nach Kontext und Vorwissen des Rezipienten, zu unterschiedlichen Informationen führen.[126] Ebenso haben Daten isoliert keine Bedeutung, sind stattdessen die bloße Darstellung und Abfolge von Zeichen[127] und benötigen daher die Erbringung einer zusätzlichen (Interpretations-)Leistung durch den Empfänger, um mit Bedeutung angereichert zu werden.[128] Daten sind damit notwendige, aber nicht hinreichende Bedingung für Informationen. Dass dabei dennoch auch schon vorher, also im Stadium des Erhebens, Übermittelns und Zusammenführens von Daten die abstrakte Gefährdung als Vorstufe dieser späteren konkreten Verwendungsgefahren durchscheint und damit eine grundlegende rechtliche Rahmung rechtfertigt, begründet *Albers* mit der Ubiquität und Kontextentkoppelung solcher Verarbeitungsvorgänge.[129] Ursprünglich erlangte Informationen können wiederum in Datenform festgehalten und in neuen Verwendungskontexten und Handlungszusammenhängen abgerufen und weiter verwertet werden.[130] Entscheidend ist dabei, dass die Unterscheidung der beiden Begriffe dazu beitragen kann, die drohenden Gefahren klarer zu umschreiben und damit im nächsten Schritt die rechtliche Instrumente besser auf ihre Wirksamkeit hin zu überprüfen. Geht es also etwa um Gefahren daraus, dass Dritte bestimmte Kenntnisse erlangen oder als Basis für eigenes Handeln und eigene Entscheidungsfindungen nutzen, betrifft dies vor allem die Informationsebene.[131] Dem folgend wäre eine konkrete Gefahr dann diejenige der Einschränkung der persönlichen Handlungsfreiheit infolge (negativ) veränderter Rahmenbedingungen durch das gewonnene Wissen eines Dritten infolge einer Datenerhebung und eines Informationsgewinns. Die Handlungsfreiheit könnte dann aktiv eingeschränkt werden, indem der betreffende Dritte sich unmittelbar nachteilig gegenüber dem Individuum verhält oder mittelbar eine ihm sonst zuteilwerdende Behandlung vorenthält. Daneben kommt die Möglichkeit einer passiven Handlungsfreiheitseinschränkung in Form selbstgewählten Verzichts bzw. selbstgewählter Verhaltensanpassung im Wissen um das neu gewonnene

---

126 Vgl. *Albers*, Rechtstheorie 2002, 61 (69).

127 Vgl. *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Hoffmann-Riem, Grundlagen des Verwaltungsrechts Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, S. 107 (115).

128 *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Hoffmann-Riem, Grundlagen des Verwaltungsrechts Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, S. 107 (116).

129 Vgl. *Albers*, Rechtstheorie 2002, 61 (62 f.).

130 *Albers*, Rechtstheorie 2002, 61 (75).

131 *Albers*, Rechtstheorie 2002, 61 (85).

Wissen des Dritten (oder aber auch die latente Ungewissheit um das genaue Ausmaß des damit einhergehenden Kenntnisgewinns) hinzu. Der Fokus liegt hier also primär auf der Gefahr durch den konkreten Verwendungskontext der gewonnenen Information in Kombination mit den einhergehenden nachteiligen Folgen.

bb) Gefahren durch Datenubiquität und Profiling

Ein anderer denkbarer Anknüpfungspunkt kann in der schieren Menge im Alltag systematisch erhobener und verarbeiteter Daten,[132] dem damit einhergehenden und potenziell unbegrenzten Pool an Informationen und daraus folgend einer (noch mehr Unsicherheit verursachenden) Informationsasymmetrie zwischen betroffenem Individuum und Informationsgewinner gesehen werden. Der Überbegriff *Big Data* wird genutzt, um die Umstände, die dieses Phänomen ubiquitärer und oft automatisierter Datenerhebung, -verarbeitung, -aggregierung und -analyse ermöglichen, sowie die daraus erwachsenden Möglichkeiten zu beschreiben. Zur Definition dieses Phänomens wird auf das sog. 3-V-Modell zurückgegriffen, das für dessen drei zentralen Aspekte steht: die Zugriffsmöglichkeit auf eine riesige und weiter steigende Menge verfügbarer Daten (*volume*), die in allen Lebensbereichen und Kontexten und über unterschiedlichste Endgeräte erhoben werden; die dadurch bedingt immense Vielfalt der Daten (*variety*), die aus unterschiedlichsten Quellen und Kontexten stammen und so die Grundlage für Informationen bieten, die ein breites Bild der betroffenen Person zeichnen können; sowie die immense Verarbeitungsgeschwindigkeit (*velocity*) infolge immer leistungsfähigerer Hard- wie auch Software in Form von bspw. Algorithmen, die es ermöglicht, diesen tiefen Pool an Daten zu aussagekräftigen Informationen zu transformieren, aus welchen sich dann entscheidungsrelevante Korrelationen und Rückschlüsse ziehen lassen, die erst im Prozess offenbar werden.[133]

Eng damit verknüpft ist die Gefahr, die aus der häufig als Nebenprodukt solcher systematischen Informationsgewinne auftretenden Intransparenz entsteht, persönliche Einflussnahme und Korrekturmöglichkeit verhindert und damit Ungewissheit und Unsicherheit weiter steigert.[134] Dass ein Individuum nie vollständig kontrollieren kann und konnte, auf welcher Informationsbasis Andere im seinem sozialen Umfeld sich ein Bild von ihm machen und machten, und

[132] Eine gute Systematik und technische Erläuterung der typischerweise beim Nutzen von Webdiensten hinterlassener Datenspuren findet sich bei *Grimm*, DuD 2012, 88 (88 ff.). Siehe auch *Kühling*, Die Verwaltung 2007, 153.

[133] Vgl. *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 34 ff.; siehe auch *Hoffmann-Riem*, AöR 2017, 1 (6 ff.).

[134] Vgl. *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 11 (27); *Paterson/McDonagh*, Monash University Law Review 2018, 1 (7); *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 107.

dass ein Individuum erst Recht nie die jeweilige Interpretation dieser Informationen durch ein Gegenüber auch nur ansatzweise vollständig beeinflussen kann und konnte, steht außer Frage. Dennoch potenzieren die Möglichkeiten digitaler Verarbeitung in Verbindung mit der Ubiquität der eigenen Datengenerierung[135] und deren über quasi jegliche Alltagshandlungen und jegliche Kanäle hinweg erfolgende Sammlung und Aggregierung durch einzelne große Akteure all die schon immer im sozialen Miteinander angelegten Ungewissheiten auf verschiedensten Ebenen. Ohne rechtliche Einrahmung fehlt auf der elementarsten Ebene eine „relative Erwartungs- und Orientierungssicherheit der Individuen im Hinblick auf ihre soziale Umwelt, die die Möglichkeiten eines Vertrauens beispielsweise darauf umfasst, dass gewisse Sichtbarkeitsschranken zwischen verschiedenen Kontexten und Rollen bestehen, dass nicht überall fehlerhafte Datensätze und entsprechend verzerrte Bilder zur eigenen Person kursieren oder dass man nicht in jeder Situation ohne eine Chance des Vergessens mit einer längst überholten Vergangenheit belastet wird.“[136] Wo im „Vorinformationszeitalter“ Ungewissheit größtenteils auf einzelne Personen, abgrenzbare Informationsherkünfte und Verwendungskontexte begrenzt war, droht heute eine auf allen (sich wechselseitig beeinflussenden) Ebenen virulente Unbegrenztheit: unbegrenzte Daten und darauf folgend Informationen, nicht abschätzbare heutige und zukünftige Verwendungskontexte und Verknüpfungen mit bereits bestehenden oder zukünftigen Daten und Informationspools, daraus folgend unvorstellbare Informationsgewinne und -erkenntnisse sowie das für das Internet charakteristische nahezu unbegrenzte Ausmaß an potenziellen Rezipienten und Weiterverwendern. Aus dieser Unsicherheit und Ungewissheit können nicht bloß handfeste Nachteile durch Entscheidungen des informationell überlegenen Gegenübers entstehen, sondern kann sich auch ein generelles Gefühl der Ohnmacht und damit ein fundamentales Defizit der eigenen Souveränität und Selbstbestimmtheit ergeben:[137] Wer nicht weiß, warum ihm etwas Positives verwehrt oder etwas Negatives zugefügt wurde, sieht sich außerstande, sein Verhalten entsprechend anzupassen; Eine gewisse Vorhersehbarkeit der Folgen des eigenen Handelns ist für das Führen eines selbstbestimmten Lebens aber elementar. Indem darüber hinaus Prognosen für die Zukunft auf Basis von Informationen über die Vergangenheit (bisheriges Verhalten, bisherige Wohnorte

---

[135] Häufig auch unter dem Begriff „Ubiquitous Computing“ bereits seit den 00er-Jahren diskutiert, siehe *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 166 f.; vgl. auch *Kühling*, Die Verwaltung 2007, 153; *Roßnagel* u. a., Datenschutzrecht 2016 – „Smart“ genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts; *Matzner*, JICES 2014, 93.

[136] *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 11 (28).

[137] Vgl. *Hoffmann-Riem*, AöR 2017, 1 (24); siehe auch bereits *Donos*, Datenschutz – Prinzipien und Ziele: unter besonderer Berücksichtigung der Entwicklung der Kommunikations- und Systemtheorie, S. 110.

etc.) gemacht werden, wird Entscheidungen letztlich ein Bild des Individuums als zur Veränderung unfähig zugrunde gelegt.

Ein häufig bemühtes Beispiel für die konkrete Anwendung von *Big Data*-Technologien ist das Anlegen von Persönlichkeitsprofilen, die ein umfassendes Bild über die betroffene Person und ihre Interessen, Verhaltensweisen und Präferenzen, aber auch ihre Makel und Laster erzeugen und im weitgehendsten Fall die Persönlichkeit einer Person teilweise bis vollständig abbilden können.[138] Die für derartige Profile[139] nötigen Daten werden typischerweise durch hartnäckiges und umfangreiches Tracking der betroffenen Personen erhoben: klassischerweise hinsichtlich seines Verhaltens im Internet,[140] zunehmend aber auch in Bezug auf „echte" Handlungen im analogen Bereich.[141] Durch diese Allgegenwärtigkeit haben sie das Potential, bei Betroffenen ein diffuses Gefühl des Beobachtetseins und Verfolgtwerdens auszulösen, das sie im schlimmsten Fall davon abhält, bestimmte Handlungen an den Tag zu legen, etwa Websites von psychologischen Hilfsangeboten aufzurufen oder über bestimmte Dinge zu reden.[142] Dieses diffuse Gefühl wird meist dadurch ausgelöst bzw. verstärkt, dass häufig bruchstückhafte Manifestierungen des Trackings sichtbar werden – etwa, wenn Werbung für Dinge angezeigt wird, nach denen erst gestern gesucht oder über die sich mit Freunden oder Familienmitgliedern am Telefon oder im Wohnzimmer unterhalten wurde –, die das Ausmaß erahnen lassen, ohne je Sicherheit darüber zu geben, wer genau welche konkreten Daten erhebt und welches Wissen über einen besitzt.[143]

Nutzerprofile können zudem leicht genutzt werden, um betroffene Personen in ihrem Handeln zu manipulieren. Durch das Identifizieren von Schwachstellen oder für die jeweilige Person besonders bedeutsame Themen, können diese gezielt und auf eine für sie präzise angepasste Art und Weise kontaktiert werden und so zu einem bestimmtes Verhalten (etwa den Kauf einer bestimmten Ware)

---

[138] Siehe hierzu etwa *Hladjk*, Online-Profiling und Datenschutz; *Wenhold*, Nutzerprofilbildung durch Webtracking; *Härting*, CR 2014, 528; *Hoffmann-Riem*, AöR 2017, 1 (12 ff.).

[139] Zu Definitionsansätzen für den Begriff der Profilbildung siehe *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 44 ff.; siehe zudem *Hladjk*, Online-Profiling und Datenschutz; *Lorentz*, Profiling – Persönlichkeitsschutz durch Datenschutz?

[140] Für eine grundlegende Erläuterung der technischen Hintergründe des Webtrackings siehe *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 48 ff.

[141] Dies etwa mittels von Smartphones erhobenen Standortdaten, mittels RFID-Trackings in Supermärkten oder durch die Sensoren von smarten Haushaltsgegenständen und anderen Geräten im eigenen Zuhause, siehe umfassend *Christl*, Kommerzielle digitale Überwachung im Alltag: Studie im Auftrag der Bundesarbeitskammer Wien. Einen nicht unerheblichen Beitrag dazu leistet die zunehmende Konvergenz der digitalen und analogen Welten. *Hildebrandt*, Smart technologies and the end(s) of law, S. 41 ff. nennt diese Hybridwelt *Onlife* (eine Kombination aus Online und Offline) World; zu RFID-Tracking siehe *Nissenbaum*, Privacy in context, S. 31 ff.

[142] Vgl. BVerfGE 100, 313 und 125, 212 zu allerding staatlichen Überwachungsmaßnahmen.

[143] Vgl. *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 106.

bewegt werden (sog. *nudging*[144]*)*, ohne dass die betroffene Person zwingend um den Wissensvorsprung des Gegenüber weiß.[145] Zusätzliche Gefahrenpotentiale offenbaren sich in besonders sensiblen Entscheidungsbereichen, so etwa bei Wahlen, sowie dann, wenn die Beeinflussung mithilfe bewusst falscher Tatsachen erfolgt.[146]

Neben diesen, die Verhaltensfreiheit und generelle Selbstbestimmtheit des Individuums betreffenden, Szenarien besteht die Gefahr, dass Entscheidungen, die auf Basis der gewonnenen Daten und gebildeten Informationen und dem resultierenden Wissen getroffen werden, handfeste negative Auswirkungen zeitigen. Ein plastischer Anwendungsbereich ist dabei häufig der der Einschätzung individueller Kreditwürdigkeit, wie in Deutschland durch die Schufa und generell durch sog. Auskunfteien betrieben. Die oben beschriebene Gefahr fehlender Transparenz, Nachvollziehbarkeit und Einflussnahme kann sich hier auf mehreren Ebenen konkretisieren. Zum einen werden Daten des Einzelnen gezwungenermaßen, unabhängig von seinem Willen, bei nahezu jeder (größeren) Transaktion einem Unternehmen wie der Schufa mitgeteilt und für die zukünftige Einschätzung seiner Kreditwürdigkeit miteinbezogen; der Prozess der Bewertung findet somit am Betroffenen vorbei, losgelöst von seinem aktiven Zutun statt.[147] Zum anderen werden zur Auswertung der gesammelten Daten in zunehmendem Maße Algorithmen eingesetzt, die am Ende ihrer Analyse im Wege statistischer Auswertung Aussagen über die Wahrscheinlichkeit etwa einer Kreditrückzahlung machen.[148] Wie dieser „Score" letztlich genau zustande kommt, welches individuelle Verhalten also bspw. den Ausschlag für oder gegen die Gewährung eines Kredits gegeben hat und welche Verhaltensanpassung dies verhindert hätte oder für die Zukunft verhindern könnte, ist dabei häufig kaum noch zu rekonstruieren[149] und ist auch nicht an vorderster Front im Interesse von Schufa und ähnlichen Unternehmen, denen es primär auf die (vermeintliche) Richtigkeit des Ergebnisses ankommt. Dem Einzelnen wird somit verwehrt, Einfluss darauf zu nehmen, welche Daten das Unternehmen zur Basis seiner Bewertung macht,[150] und zu kontrollieren, ob diese korrekt sind und das

144 Zurückgehend auf *Thaler/Sunstein*, Nudge.

145 Vgl. *Hildebrandt*, Smart technologies and the end(s) of law, S. 263.

146 Vgl. *Hoffmann-Riem*, AöR 2017, 1 (14 ff.) m. w. N.

147 *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 119 f.; vgl. auch *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 11 (28 f.).

148 Vgl. *Ernst*, JZ 2017, 1026.

149 Die Schwierigkeiten hinsichtlich Nachvollziehbarkeit und Erklärbarkeit nehmen mit der zunehmenden Entwicklung von klassischen, deterministischen Algorithmen hin zu (selbst) lernenden Algorithmen exponentiell zu, vgl. *Burrell*, Big Data & Society 2016, 1. Siehe außerdem grundlegend *Pasquale*, The black box society.

150 Genau genommen könnte er Einfluss darauf nehmen, müsste dafür aber auf eine Vielzahl an (teilweise alltäglichen und lebenswichtigen) Transaktionen verzichten. Die Unzumutbarkeit der Einflussnahme kann daher der Unmöglichkeit der Einflussnahme gleichgestellt werden.

aus ihnen entstandene Bild der eigenen Kreditwürdigkeit der Realität bzw. eigenen Wahrnehmung entspricht. Hinsichtlich der ihn negativ betreffenden Entscheidung gegen einen Kredit besteht hier eine Gefahr der Diskriminierung, die sich einerseits aus der bereits angesprochenen Verwendung von die Vergangenheit betreffenden Informationen, andererseits aus der inhärenten Intransparenz der Entscheidungsfindung speist.[151] Auch eine unvollständige bzw. lückenhafte Datenbasis kann zu diskriminierenden Entscheidungen führen, wenn etwa Minderheiten und Individuen mit untypischen Kombinationen an für die Entscheidung relevanten Merkmalen im Gesamtpool von entscheidungserheblichen Daten unterrepräsentiert sind, sodass das entsprechende System bzw. der eingesetzte Algorithmus keine eindeutige Prognose abgeben kann und so aus „Vorsicht" eine negative Entscheidung trifft – sog. *uncertainty bias*.[152]

cc) Gefahren durch Verarbeitung besonders sensibler Daten

Die eben im Zusammenhang mit Diskriminierungen genannten geschützten Merkmale stehen auch im Mittelpunkt eines weiteren Beispiels konkreter moderner Gefährdungsszenarien: die Verarbeitung von besonders sensiblen Daten, wie sie bspw. die DSGVO in Art. 9 durch Bindung an besonders strenge Verarbeitungsvoraussetzungen schützt. Hier besteht grundsätzlich eine erhöhte Gefahr schädigender Auswirkungen durch Handlungen, die auf Basis des gewonnenen Wissens durchgeführt werden – so zum Beispiel diskriminierende Entscheidungen, aber auch Schädigungen der körperlichen Unversehrtheit, wenn etwa die sexuelle Orientierung oder die Religiosität einer Person in den falschen Kontexten gegenüber den falschen Rezipienten veröffentlicht werden.[153] Diese besondere Gefährdung ergibt sich, so das Konzept hinter dem besonderen Schutz dieser Datenkategorien,[154] einerseits aus dem Inhalt der Daten, andererseits aus den typischen Verwendungszusammenhängen, die bei ihrer Nutzung erwartet bzw. befürchtet werden muss.[155]

Ein besonders heikler Punkt, der die Limitierungen des Konzepts einer abschließenden Liste besonders sensibler Daten á la Art. 9 DSGVO aufzeigt, sind Standortdaten und andere Daten, denen die Möglichkeit des Rückschlusses auf weitere Gegebenheiten (sei es unmittelbar oder durch Kombination mit öffentlich verfügbaren weiteren Daten) bereits inhärent ist. So können etwa (grund-

---

[151] So besteht bspw. die Gefahr, dass für die Entscheidung mittelbar oder unmittelbar an diskriminierende Kriterien angeknüpft wird, ohne dass dies ohne weiteres erkennbar ist, vgl. *Martini*, JZ 2017, 1017 (1018). Siehe auch *Edwards/Veale*, Duke Law & Technology Review 2017, 18 (29 f.); genereller zum Thema Preisdiskriminierung im Internet auf Basis von Kundenprofilen *Odlyzko*, in: Camp/Lewis, Economics of information security, S. 187.

[152] Vgl. *Goodman/Flaxman*, AIMag 2017, 50 (52 f.).

[153] Vgl. *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 9 DSGVO Rn. 6.

[154] Generell kritisch zum Konzept der Einteilung in sensible und weniger sensible Daten *Schneider*, ZD 2017, 303.

[155] Vgl. *Petri*, in: Simitis u. a., DSGVO/BDSG, Art. 9 DSGVO Rn. 1.

sätzlich nicht als besonders sensibel eingestufte) Standortdaten, die von einer Vielzahl von Smartphone-Apps regelmäßig abgerufen werden, neben der Nutzung zur Anfertigung von längerfristigen Bewegungsprofilen unter anderem auch dazu genutzt werden, durch einen Abgleich mit bspw. Google Maps Rückschlüsse darauf ziehen, dass bestimmte Kirchen oder Arztpraxen besucht wurden – und so mittelbar sensible Informationen hinsichtlich Religiosität, Krankheiten und ähnlichen Kategorien zu erlangen. In ähnlicher Weise können vermeintlich neutrale Daten wie etwa die (ebenfalls von vielen Smartphone-Apps abgerufene) MAC-Adresse des Routers in einem WLAN-Netzwerk, mit dem die Geräte einer Person verbunden sind, mit öffentlichen Datenbanken abgeglichen werden, um so Rückschlüsse auf den Standort des Routers und somit der Person zu ermöglichen.[156] Derartige Rückschlusskaskaden verdeutlichen die Schwierigkeit, in der heutigen Zeit realistischer Weise Rückschlusspotentiale und etwaige zukünftige Verwendungskontexte von preisgegebenen Daten abschätzen zu können.[157] Sie legen außerdem die Einschätzung nahe, dass die starre Einteilung in sensible und weniger sensible Daten in Zeiten polyvalenter bzw. pluripotenter Datenverwendungen überholt ist.[158]

b) In der internationalen Literatur

Eine grundlegende und umfassende Abhandlung über die Gefährlichkeit von Datenverarbeitungsvorgängen innerhalb unterschiedlicher Verarbeitungsstadien und aufgrund spezifischer Verarbeitungscharakteristika veröffentlichte bereits 2006 der US-Amerikaner *Solove* in seiner Taxonomie der Privatheit.[159] Sein dabei verfolgtes Ziel war es, die diversen (potenziell) grundrechtsgefährdenden Handlungen und korrespondierenden spezifischen Gefahren aufzudecken und zu systematisieren, die im Zusammenhang mit dem weiten und flexiblen Begriff *privacy* zusammengefasst und dadurch, so *Solove*, verdeckt zu werden drohen.[160] Besonders erwähnenswert ist dies nicht zuletzt deshalb, weil

---

[156] Für eine Aufarbeitung des AccuWeather-Falls, in dem ein in eine Wetter-App eingebundener Drittanbieter trotz verweigerter Standortdatenberechtigung mittels freiem Zugang auf solche Netzwerkdaten mittelbar Standorte von Nutzern herleiten konnte, siehe *Kurtz* u. a., The Unlikely Siblings in the GDPR Family, sowie *supra* in Kapitel 1 I. 2.

[157] Zu den Schwierigkeiten, die damit für den Verantwortlichen bzgl. der Abgrenzung zwischen gewöhnlichen und sensiblen Daten einhergehen („gefährdet die Rechtssicherheit und die Verhältnismäßigkeit"), siehe *Matejek/Mäusezahl*, ZD 2019, 551 (552).

[158] Vgl. *Matejek/Mäusezahl*, ZD 2019, 551 (551): „[…] bleibt der Begriff der sensiblen Daten in zahlreichen Konstellationen unscharf und neigt (vor allem mit Blick auf neue Technologien und Analysemethoden) zum Ausufern. In vielen Fällen verschwimmen dadurch die Grenzen zu den ‚gewöhnlichen' Daten."

[159] *Solove*, University of Pennsylvania Law Review 2006, 477.

[160] Vgl. *Solove*, University of Pennsylvania Law Review 2006, 477 (485 f.); diese Problematik des sehr schwammigen und unscharfen Begriffs von privacy bereits sehr früh treffend beschreibend *Thomson*, Philosophy & Public Affairs 1975, 295 (295): „Perhaps the most striking thing about the right to privacy is that nobody seems to have any clear idea what it is."

der *privacy*-Begriff – wenngleich häufig unreflektiert als Synonym zum Datenschutz verwendet[161] – aufgrund seiner im Kern überwiegenden Verwurzelung im Privatsphären-, Rückzugs- und Abschottungsgedanken („right to be let alone")[162] insbesondere in den USA historisch häufig nicht in der Lage war, die vielfältigen unter dem Begriff des Datenschutzes diskutierten Facetten vollständig abzudecken.[163] Umso bemerkenswerter ist es, wie es *Solove* gelingt, den Begriff durch seine Systematisierung so weit zu öffnen und Gefahrenkategorien freizulegen, die auch heutige Gefahrenszenarien abzubilden vermögen.

Dabei unterteilt er in die Handlungskategorien „*information collection*", „*information processing*", „*information dissemination*" und „*invasions*" – also in Gefahren, die sich jeweils spezifisch aus Art und Umständen von Datenerhebungen, Datenverwendungen, Datenverbreitung und (nicht notwendig auf personenbezogenen Daten beruhenden) privatsphäreninvasiven Akten ergeben.[164] Für jede dieser Gefahrenkategorien formuliert *Solove* konkrete Untergruppen.

So werden auch hier im Rahmen der Datenerhebung etwa Praktiken des Überwachens (im Sinne des Aufzeichnens oder Mitschneidens von Aktivitäten des Betroffenen) als besonders gefahrensensibel im Zusammenhang mit Selbstzensur und gehemmter Persönlichkeitsausübung[165] (bei offener Überwachung)

---

[161] Vgl. zu dieser weit verbreiteten Gleichsetzung *Oostveen*, Why privacy ≠ data protection (and how they overlap) | Digital Society Blog; *Gellert/Gutwirth*, CLSR 2013, 522 (522 ff.).

[162] Im Wesentlichen zurückgehend auf *Warren/Brandeis*, Harvard Law Review 1890, 193 (193, 195, 196), die den Begriff grundlegend prägten; Thoreau, Emerson und Dickinson als Vorbilder für Warren und Brandeis betonend *Glancy*, Arizona Law Review 1979, 1; vgl. zur Verankerung des *right to privacy* in räumlich und materiell fassbaren Bereichen auch *Whitman*, The Yale Law Journal 2004, 1151 (1161 f.).

[163] Weil beispielsweise einer schutzbestimmenden und damit gefahrdefinierenden Dichotomie zwischen geheimen und bereits veröffentlichten Daten, privaten und öffentlichen Sphären oder unmittelbar beschämenden bzw. kompromittierenden und vermeintlich harmlosen Daten gefolgt wird, die aus dem analogen Bereich stammend übernommen wurde, siehe *Solove*, University of Pennsylvania Law Review 2006, 477 (563).

[164] Der von *Solove* und generell im Englischen verwendete „information"-Begriff soll dabei nicht als gleichbedeutend mit dem deutschen Informationsbegriff, wie er *supra* unter Rückgriff auf *Albers* verwendet wurde, missverstanden werden. Generell darf im Englischen von der fehlenden Differenzierung dieser beiden Begriffe ausgegangen werden. Speziell im Rahmen der aufgezählten Kategorien sind darunter, wie auch im Text erläutert, eher Daten zu verstehen.

[165] Die sogenannten „chilling effects" als Umschreibung der schleichenden Verhaltensanpassung und Vermeidung von als deviant befürchtetem Verhalten sind spätestens seit BVerfGE 125, 260 (319) und EuGH, verb. Rs. C-293/12 und C-594/12 (Digital Rights Ireland Ltd.), E-CLI:EU:C:2014:238 Rn. 37 ein stehender Begriff im Zusammenhang mit umfassender (staatlicher) Überwachung. Nichtsdestotrotz wird die Existenz solcher Abschreckungseffekte mit Verweise auf mangelnde empirische Belege in weiten Teilen der Literatur angezweifelt, siehe stellvertretend für viele und mit zahlreichen weiteren Verweisen *Hermstrüwer*, Informationelle Selbstgefährdung, S. 45 ff. Für solche Effekte argumentierend und die negativen Auswirkungen für Individuum und demokratische Gesellschaft herausstellend *Cohen*, Stanford Law Review 2000, 1373 (1426 f.); zur Frage der verfassungsrechtlichen Einordnung von Abschreckungseffekten als Grundrechtsbeeinträchtigungen siehe *Staben*, Der Abschreckungs-

oder auch der Preisgabe besonders sensibler Informationen (bei verdeckter Überwachung) deklariert, wobei die spezifische Gefährlichkeit sich beispielsweise aus dem Ausmaß, dem Kontext (in welchem der Betroffene eine Überwachung nicht erwartet[166]) oder der stetigen Ungewissheit über das momentane Ausüben der Überwachung ergeben kann.[167]

Im Rahmen von Datenverwendungen stellt *Solove* unter anderem[168] die Gefahrenkategorien Aggregation, Weiterverwendung und Unsicherheit („*insecurity*") von Daten in den Vordergrund. Dabei teilen sich die ersten beiden Kategorien eine Gefährlichkeit, die ihren Ursprung darin hat, dass die Verwendung personenbezogener Daten zu vom bzw. für den Einzelnen nicht erwarteten bzw. abzuschätzenden Ergebnissen führt: im ersten Fall durch die Kombination mit zahlreichen weiteren ihn betreffenden Daten und die daraus folgende Bildung eines umfassenden Profils über die eigene Person, aus welchem sich Rückschlüsse ziehen lassen, die weit über das hinausgehen, was der Einzelne bei der Preisgabe der isolierten Daten von sich preisgeben wollte.[169] Drohende Folge weitrechender Aggregationen von Daten sind mögliche Entscheidungen, die über den Einzelnen auf Basis eines solchen zusammengesetzten digitalen Gesamtbildes getroffen werden, ohne dass dieser selbst das zugrundeliegende Bild kennt und etwaige Lücken und Fehler anzuzweifeln oder gar zu kor-

---

effekt auf die Grundrechtsausübung, S. 130 ff.; siehe zudem *Lynskey*, The foundations of EU data protection law, S. 215 ff.

166 Hier zeigen sich die Unterschiede zwischen angloamerikanischer und europäischer Datenschutzdogmatik besonders deutlich: das amerikanische Recht mit seiner „reasonable expectation to privacy"-Doktrin stellt in starkem Maße bereits (übertragen auf die deutsche Grundrechtsprüfung) bei der Frage der Schutzbereichseröffnung darauf ab, ob in einem bestimmten Kontext überhaupt darauf vertraut werden durfte, nicht überwacht zu werden – siehe etwa *United States v. Karo* (468 U. S. 705, 714 (1984)) und *United States v. Knotts* (460 U. S. 276, 277 (1983)), in denen die Überwachung der Bewegungen der jeweils Betroffenen im eigenen Haus für unzulässig, im eigenen Auto hingegen (mit Verweis auf die fehlende Legitimität des Vertrauens darauf, auf öffentlichen Straßen nicht überwacht zu werden) für zulässig erklärt wurde. Fehlt es an einem solchen Vertrauen, ist bereits der Schutzbereich nicht eröffnet. Demgegenüber spielen solche (eher dem klassisch persönlichkeitsrechtlichen Sphärenmodell ähnelnde) Überlegungen im deutschen bzw. europäischen Datenschutz höchstens eine untergeordnete Rolle und wiegen insbesondere Überlegungen zur Sensibilität der jeweiligen Daten schwerer. Nichtsdestotrotz lässt sich vorsichtige Annäherung bereits erkennen, wenn etwa Erwg. Nr. 50 der DSGVO feststellt, dass der Frage der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Zweck im Rahmen von Art. 6 Abs. 4 auch die „vernünftigen Erwartungen der betroffenen Person, die auf ihrem Verhältnis zu dem für die Verarbeitung Verantwortlichen beruhen" zugrunde gelegt werden sollen. Auch der EGMR stellte im Rahmen seiner Prüfung von Art. 8 EMRK bereits – wenn auch mit wenigen Worten und einem gänzlich anderen Maßstab als die US-Gerichte folgend – fest, dass eine solche legitime Erwartung in Fällen der heimlichen Überwachung von Telefongesprächen am Arbeitsplatz vorliegt, vgl. *Hornung*, MMR 2007, 431 (433).

167 *Solove*, University of Pennsylvania Law Review 2006, 477 (491 ff.).

168 Hinzu kommen die Kategorien der Identifizierung und der Ausgrenzung, vgl. *Solove*, University of Pennsylvania Law Review 2006, 477 (511 ff., 521 ff.).

169 *Solove*, University of Pennsylvania Law Review 2006, 477 (508 ff.).

rigieren vermag. Auch die Gefahr von diskriminierenden Entscheidungen tritt hier erneut zutage.[170] Dieses zunächst individuelle Machtgefälle kann zudem zu einem zu strukturellen informationellen Machtasymmetrien führen.[171] Mit diesen Gefahren eng zusammen hängt auch die Kategorie der Weiterverwendung: Auch wenn Daten zu bestimmten, dem Betroffenen bekannten Zwecken erhoben wurden und später zu davon gänzlich losgelösten Zwecken weiterverwendet werden, werden berechtigte individuelle Erwartungshaltungen unterlaufen und – ggf. schwerwiegende – Tatsachen geschaffen, auf die bzw. auf dessen Entstehung der Betroffene keinen Einfluss hat.[172] Die damit einhergehende Unsicherheit könnte im schlimmsten Fall dazu führen, dass Betroffene davon Abstand nehmen, ihre Daten überhaupt zu teilen – also das Ideal eines möglichst freien Informationsflusses gefährden und damit ironischerweise den Zustand herbeiführen, dessen Eintritt Kritiker eines zu stark regulierenden Datenschutzrechts häufig befürchten.

Die Gefahrenkategorie der Unsicherheit von Daten beschreibt die Gefahr von ungewollten Datenpreisgaben, -weitergaben und -veränderungen infolge von Identitätsdiebstahl, Hacks oder andere Formen unerlaubten Zugriffs, oft im Zusammenhang mit unachtsamen Sicherheitsvorkehrungen durch den Verantwortlichen.[173]

Im Rahmen der Datenverbreitung („*information dissemination*“) diskutiert *Solove* verschiedene Beispielszenarien von gefährlichen Methoden und Praktiken der Veröffentlichung und Weiterverbreitung von personenbezogenen Daten. Als Beispiele nennt er Verschwiegenheitsverletzungen, bei denen sich die Gefährlichkeit nicht (in erster Linie) aus den Daten selbst, sondern aus der die Daten verbreitenden Person und dem zwischen ihr und dem Betroffenen bestehenden besonderen und besonders geschützten Vertrauensverhältnis ergibt[174], sowie die unabhängig von einem solchen Verhältnis problematische Weitergabe bzw. Veröffentlichung der Daten an sich.[175] Für letztere ist nach *Solove* nötig, dass den Betroffenen betreffende Daten veröffentlicht werden, die das Potential haben, ihn bloßzustellen oder (bspw. charakterlich) zu diskreditieren[176] – die Qualifikation der betroffenen Daten als derart sensibel sei zwar (gewissermaßen *on top*) auch im Rahmen der ersten Kategorie möglich, aber nicht zwingend

---

[170] Vgl. *Lynskey*, The foundations of EU data protection law, S. 197 ff.

[171] Einen ähnlichen Schwerpunkt legen in der deutschsprachigen Literatur *Bock/Engeler*, DVBl 2016, 593 (596 f.), wenn sie die informationelle Unversehrtheit als eigenständigen Wesensgehalt von Art. 8 in Abgrenzung zu Art. 7 GRCh formulieren. Siehe zum Gefühl der Machtlosigkeit infolge solcher Informationsasymmetrien auch *Lynskey*, The foundations of EU data protection law, S. 211 ff.

[172] *Solove*, University of Pennsylvania Law Review 2006, 477 (521 f.).

[173] *Solove*, University of Pennsylvania Law Review 2006, 477 (516 ff.).

[174] *Solove*, University of Pennsylvania Law Review 2006, 477 (526 ff.).

[175] *Solove*, University of Pennsylvania Law Review 2006, 477 (530 ff.).

[176] *Solove*, University of Pennsylvania Law Review 2006, 477 (527).

nötig.[177] Die Gefährlichkeit ergibt sich im ersten Fall also aus den möglichen Konsequenzen des Vertrauensbruchs, im zweiten aus den möglichen negativen Reaktionen, die Dritte nach Sichtung der Daten gegenüber dem Betroffenen zeigen könnten. In eine etwas andere Richtung geht die Kategorie der Zurschaustellung höchstprivater Daten betreffend körperliche oder emotionale Merkmale einer Person.[178] Diese müssen gerade nicht etwas als gesellschaftlich besonders negativ Konnotiertes beinhalten, das den Betroffenen von der Norm absetzt und dadurch in der öffentlichen Meinung diskreditiert, sondern sind allein aufgrund ihrer qua gesellschaftlichem und zivilisatorischem Konsens etablierten Verortung als privat und in der Öffentlichkeit tabuisiert sensibel. Dazu gehören etwa Daten im Zusammenhang mit Nacktheit und Sexualität oder körperlichen Verletzungen. Hier steht weniger die Gefahr der herabgesetzten Reputation des Betroffenen infolge der Veröffentlichung im Vordergrund, sondern seine Würde und die von ihm selbst ob der öffentlichen Wahrnehmung solch privater Umstände gefühlte Scham, die zu einer Hemmung der individuellen Persönlichkeit (und ihrer Entwicklung und Ausübung) führen kann:

„When these practices are disrupted by exposure, people can experience a severe and sometimes debilitating humiliation and loss of self-esteem. Exposure thus impedes a person's ability to participate in society. Even though most people would not view a victim of exposure as a lesser person or as being less civilized, victims feel that way. […] Disclosure is a power that controls through the imposition of social sanctions and condemnation. Exposure works in a different way, by stripping people of their dignity."[179]

Eine weitere interessante Unterkategorie der Datenweitergabe ist die der erleichterten Verfügbarkeit („*increased accessibility*").[180] Sie beschreibt Fälle, in denen bereits veröffentlichte Daten dadurch eine zusätzliche Gefahr für den Betroffenen erlangen, dass sie leichter auffindbar und erreichbar gemacht werden.[181] Als Beispiele nennt *Solove* etwa öffentlich einsehbare Dokumente über

[177] Dabei muss relativierend eingeräumt werden, dass (jedenfalls rechtlich) geschützte Vertrauensverhältnisse in der Regel deshalb geschützt sind, weil in ihrem Rahmen besonders sensible Daten verarbeitet werden, so etwa bei der nach § 9 Abs. 1 MBO-Ä garantierten ärztlichen Schweigepflicht. Zu der von *Solove* propagierten klaren Abgrenzung kommt man aber dennoch, indem man die zusätzliche Gefährlichkeit der Datenweitergabe – anders als es etwa die DSGVO in Art. 9 macht – nicht von der bloßen Sensibilität der Daten, sondern von ihrem Potential, den Betroffenen unmittelbar nachteilig dastehen zu lassen, abhängig macht. Dann wäre die ärztliche Weitergabe einer Grippediagnose nur unter dem Topos der verletzten Schweigepflicht, nicht aber dem der besonderen Gefährlichkeit der Weitergabe selbst problematisch, während bei der Diagnose einer Geschlechtskrankheit beide Merkmale erfüllt wären.

[178] *Solove*, University of Pennsylvania Law Review 2006, 477 (536 ff.).

[179] *Solove*, University of Pennsylvania Law Review 2006, 477 (537).

[180] Eine besondere eigenständige Bedeutung hat diese Kategorie in den USA vor allem deshalb, weil „*privacy*" als geschütztes Gut dort häufig – von *Solove* als „*secrecy paradigm*" umschrieben – nur geheime Daten erfasste und sich nicht auf solche erstreckte, die bereits der Öffentlichkeit zugänglich waren, siehe etwa *Cline v. Rogers* (87 F.3d 176, 179 (6th Cir. 1996).

[181] *Solove*, University of Pennsylvania Law Review 2006, 477 (539 ff.).

persönliche Insolvenz oder die kommerzielle Verwendung von öffentlichen Registerdaten (etwa aus dem Melderegister) für bspw. Marketingzwecke.[182] Wo bspw. private Adressen betroffen sind, drohen im schlimmsten Fall sogar Gefahren für die körperliche Unversehrtheit.[183] Daneben diskutiert *Solove* unter dem Überbegriff der Datenweitergabe Fälle von Erpressung[184], Aneignung[185] und verzerrter Darstellung[186]. Ein besonders virulentes aktuelles Beispiel der Auswüchse, die das Aggregieren von im Internet mehr oder weniger frei verfügbaren Daten in Verbindung mit den Möglichkeiten moderner Analysetechniken haben kann, sind die verschiedenen publik gewordenen Fälle um Unternehmen, die ihre Gesichtserkennungssoftware mit von Facebook und anderen großen Webseiten gescrapten Bildern trainierten und nun, in Fällen wie dem des Unternehmens Clearview AI,[187] staatlichen Stellen wie Strafverfolgungsbehörden, in Fällen wie dem des polnischen Unternehmens PimEyes[188] auch Privatpersonen anbieten.

Unter der Kategorie invasiver Eingriffe („*invasion*“) diskutiert *Solove* sodann zum einen die Gefahr von Handlungen, die – denkbarer-, aber nicht notwendigerweise in Verbindung mit der Erhebung oder Aufdeckung von Daten – in besonders penetranter Weise die selbstgewählte Zurückgezogenheit und Abgeschiedenheit einer Person beeinträchtigen („*intrusion*“). Als Beispiele werden neben den klassischen Formen von physischen Nachstellungen von Paparazzi und Konsorten im digitalen Raum insbesondere Spam-Mails und ähnliche Methoden genannt.[189] Zum anderen beschreibt er die Gefahr übermäßiger Einflussnahme auf die (höchst-)persönliche Entscheidungsfindung durch privatsphäreninvasive Handlungen („*decisional interference*“).[190]

---

[182] *Solove*, University of Pennsylvania Law Review 2006, 477 (540).

[183] Vgl. *Lynskey*, The foundations of EU data protection law, S. 208 ff.

[184] Beispielsweise durch das Drohen mit der Veröffentlichung von Daten, siehe *Solove*, University of Pennsylvania Law Review 2006, 477 (541 ff.).

[185] Beispielsweise durch Verwendung des Bildes des Betroffenen zum eigenen Zwecke oder Vorteil, ähnlich dem deutchen Recht am eigenen Bild, siehe *Solove*, University of Pennsylvania Law Review 2006, 477 (545 ff.); auch Identitätsbetrug ist ein unter diesem Stichwort zu diskutierendes Gefahrenszenario, vgl. *Lynskey*, The foundations of EU data protection law, S. 202 ff.

[186] Etwa durch Verwendung unrichtiger Datensätze, siehe *Solove*, University of Pennsylvania Law Review 2006, 477 (549).

[187] Siehe *Patrick Beuth*, Erst heimlich, dann unheimlich, SpiegelOnline vom 20.01.2020 (https://www.spiegel.de/netzwelt/netzpolitik/gesichtserkennung-clearview-ai-verkauft-fragwuerdige-technik-an-us-behoerden-a-54779c50-2237-451d-b7f9-018cc0c90114). Zuletzt abgerufen am 14.01.2022.

[188] Siehe *Daniel Laufer, Sebastian Meineck*, Eine polnische Firma schafft gerade unsere Anonymität ab, Netzpolitik vom 10.07.2020 (https://netzpolitik.org/2020/gesichter-such maschine-pimeyes-schafft-anonymitaet-ab/). Zuletzt abgerufen am 14.01.2022.

[189] *Solove*, University of Pennsylvania Law Review 2006, 477 (554).

[190] *Solove*, University of Pennsylvania Law Review 2006, 477 (557 ff.).

Viele dieser Kategorien decken sich mit denen von *Helen Nissenbaum*, die, auf einer etwas abstrakteren Ebene, unter dem Begriff der *kontextuellen Integrität* ebenfalls ein Framework für die Systematisierung von Gefahren aufgestellt hat.[191] Diesem zufolge liegt jedem Fluss von Daten und Informationen eine Vielzahl von informationellen Normen zugrunde, bei deren Beachtung die kontextuelle Integrität im Einzelfall gewahrt, bei deren Verstoß sie hingegen verletzt ist. Drohende Verstöße gegen die kontextuelle Integrität stellen somit eine Gefahr für Privatheit und Datenschutz dar. Welche informationellen Normen im jeweiligen Fall gelten und wie diese ausgestaltet sind, hängt von vier Faktoren ab: dem konkreten Kontext,[192] den beteiligten Akteuren (Sender, Empfänger und Subjekt des Datenflusses),[193] den Kategorien (oder Attributen) von Daten,[194] sowie den Übertragungsprinzipien.[195] Diese Kriterien sind dabei verflochten und bedingen sich teilweise gegenseitig. Ein Verstoß gegen eine informationelle Norm und damit gegen die kontextuelle Integrität kann sich aus einem konkreten Kriterium oder aus der Kombination verschiedener Kriterien ergeben. Von besonderer Bedeutung ist der jeweilige (soziale) Kontext, in dem sich eine Datenübertragung abspielt. So kann die Weitergabe von Person A an Person B in einem privaten Kontext völlig in Ordnung sein, in einem öffentlichen Kontext aber nicht; sie kann unter bestimmten, impliziten oder expliziten, Bedingungen in Ordnung sein (etwa dann, wenn sie für die betroffene Person erkennbar und vorhersehbar ist oder im Gegenzug eine Übertragung in die entgegengesetzte Richtung auslöst), ohne diese aber nicht; sie kann bei bestimmten Datenattributen in Ordnung sein (etwa, wenn der Datenträger eine Weitergabe erschwert oder unmöglich macht), bei anderen hingegen nicht.

c) Zwischenergebnis

Abstrahiert man die verschiedenen Gefahrenszenarien und vergleicht die unterschiedlichen genannten Kategorien, bildet sich ein zwischen deutscher und internationaler Literatur erstaunlich ähnliches Bild. Ein zunehmender Fokus auf den Datenverarbeitungen und Informationsverwendungen umgebenden Kontext ist allerorts festzustellen. Gleiches gilt für die Feststellung, dass Gefahren sich auf verschiedenen Ebenen und Zeitpunkten realisieren können. Zwar legt die Unterscheidung zwischen Daten und Informationen offen, dass der Großteil handfester Nachteile, etwa in Form eingeschränkter Handlungsfreiheit, sich erst auf der letztgenannten Ebene und in Abhängigkeit der Verwendungszusammenhänge ergibt. Dennoch können sich Auswirkungen für die betroffene Person auch schon aus dem bloßen Fluss von Daten und insbesondere aus der Unge-

[191] *Nissenbaum*, Privacy in context.
[192] *Nissenbaum*, Privacy in context, S. 141.
[193] *Nissenbaum*, Privacy in context, S. 141 ff.
[194] *Nissenbaum*, Privacy in context, S. 143 ff.
[195] *Nissenbaum*, Privacy in context, S. 145 ff.

wissheit über deren Umfang sowie über die Identität der Empfänger und deren Verwendungszwecke ergeben. Gefahren können sich daher nicht nur aus der Bildung und Verwendung von Informationen, sondern in Teilen auch schon aus der Erhebung, Verbreitung, Aggregation und Veröffentlichung von Daten ergeben.

2. Überindividuelle Gefahren

„Data privacy is not like a consumer good, where you click ‚I accept' and all is well. Data privacy is more like air quality or safe drinking water, a public good that cannot be effectively regulated by trusting in the wisdom of millions of individual choices. A more collective response is needed."[196]

Eine eigenverantwortliche Selbstgefährdung in Form von freiwilliger Preisgabe von ggf. sehr sensiblen Daten ist – innerhalb der bereits erwähnten Grenzen einer hinreichenden staatlich bereitgestellten Informationsinfrastruktur und somit zumutbaren Selbstschutzmöglichkeiten – dem Einzelnen freigestellt, kann sogar (insbesondere, aber nicht nur in der deutschen Dogmatik der informationellen Selbstbestimmung) gerade als Ausübung der eigenen grundrechtlich verbürgten Freiheit angesehen werden.[197] Nähme man allein die individuellen Gefahren, die mit Datenverarbeitungen einhergehen (können) in den Blick, so läge der häufig geäußerte Vorwurf eines (zu) paternalistischen Datenschutzes[198] nahe, wenn datenschutzrechtliche Normen dieser Freiheit Grenzen setzen. Eine solche Einengung des Blickes auf nur individuelle Gefahren würde aber zu kurz greifen. Quasi allen dogmatischen Rückanbindungen des Datenschutzes ist gemein, dass sie diesem eine gewisse Gemeinwohlrelevanz und somit einen über den bloßen Schutz des Individuums hinausgehende Funktion zuschreiben.

a) Demokratietheoretische Bedeutung

Dabei werden häufig etwa gesamtgesellschaftliche und demokratierelevante Gefahrenpotentiale diskutiert.[199] Mag es auch zu weit gehen, etwa das Recht auf

---

[196] *Zeynep Tufekci*, The Latest Privacy Debacle, New York Times vom 30.01.2018 (https://www.nytimes.com/2018/01/30/opinion/strava-privacy.html). Zuletzt abgerufen am 14.01.2022.

[197] Vgl. *Reinhardt*, AöR 2017, 528 (559): „Es gehört zum Kern grundrechtlicher Gewährleistungen, darüber zu befinden, in welchem Maß von den grundrechtlichen Freiheiten Gebrauch gemacht wird und welche Einschränkungen um anderer Vorteile willen in Kauf genommen werden." Siehe auch *Greve*, in: Franzius/Lejeune/von Lewinski/Meßerschmidt/Michael/Rossi/Schilling/Wysk, Beharren. Bewegen: Festschrift für Michael Kloepfer zum 70. Geburtstag, S. 665 (672).

[198] Stellvertretend für diese Ansicht und mit besonderem Eifer etwa *Veil*, Datenschutz, das zügellose Recht – Teil II; in die gleiche Richtung gehend *Krönke*, Der Staat 2016, 319 (319 ff.).

[199] Siehe etwa *von Lewinski*, Die Matrix des Datenschutzes, S. 55 ff.; *Rouvroy/Poullet*, in: Gutwirth/Poullet/de Hert/de Terwangne/Nouwt, Reinventing data protection?, S. 45 (insb.

informationelle Selbstbestimmung als „zuallererst Schutz einer auf aktiver Mitwirkung basierenden Demokratie und erst mittelbar Schutz der Rechte einzelner Bürger“[200] zu verstehen, so lässt sich jedenfalls die Existenz einer solchen Schutzrichtung nicht leugnen. Schon 1971 stellte *Simitis* die „Fundamentalbedingungen einer demokratischen Gesellschaft“[201] heraus, die bei der Verarbeitung personenbezogener Daten auf dem Spiel stünden. Auch das BVerfG betonte bereits im Volkszählungs-Urteil die große Bedeutung eines tragfähigen Mindestmaßes an informationeller Selbstbestimmung für die auf eine selbstbestimmte und freiheitlich agierende Bevölkerung angewiesene Demokratie.[202] Auch anderenorts wird die „politische Dimension des Privaten“ betont.[203] Grundvoraussetzung für eine funktionierende Demokratie sind demnach nicht allein grundlegende Institutionen und Prozesse wie freie Wahlen[204] und unabhängige und konkurrierende Parteien[205], ein pluralistischer Rundfunk[206] und eine möglichst diverse Presse- und Medienlandschaft[207]. Es bedarf zusätzlich zu dieser Demokratieinfrastruktur auch einer Bevölkerung, die sie – in Form etwa eines demokratischen Diskurses, einer Ausnutzung der bereitgestellten Partizipationsmöglichkeiten etc. – mit Leben füllt.[208] Eine fremdbestimmte Gesellschaft entspricht nicht dem Ideal einer solchen, von informierten, unabhängigen und nach neuen Erkenntnissen strebenden Bürgern getragenen Demokratie.[209] Ein echter „Wettkampf der Ideen“ unter den Parteien kann nur bestehen, wenn Bürger (zumindest theoretisch) in der Lage sind, diese Ideen zu verstehen, einzuordnen, gegeneinander abzuwägen und letztlich informierte Präferenzen zu bilden bzw. die politische Agenda durch neue, ggf. ungewöhnliche

57 ff.); ebenso *Allen*, Unpopular privacy, S. 13, dort *privacy* als *„‚foundational‘ human good“* beschreibt.

200 *Winter*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, S. 37 (45).

201 *Simitis*, NJW 1971, 673 (682).

202 Vgl. BVerfGE 65, 1 (43): „[…] nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist.“

203 *Becker/Seubert*, DuD 2016, 73 (73).

204 Vgl. *Klein/Schwarz*, in: Dürig u. a., GG, Art. 38 Rn. 67 ff. zu den einzelnen Funktionen der Wahl im demokratischen Verfassungsstaat.

205 Vgl. *Kluth*, in: BeckOK Grundgesetz, Art. 21 Rn. 59; *Klein*, in: Dürig u. a., GG, Art. 21 Rn. 150.

206 Hierzu *Grabenwarter*, in: Dürig u. a., GG, Art. 5 Rn. 518 ff.

207 Vgl. *Grabenwarter*, in: Dürig u. a., GG, Art. 5 Rn. 353 ff.

208 Zur Rolle des Bürgers in der partizipativen Demokratie *Schmidt*, Demokratietheorien, S. 232 f.; zur Entwicklung der Möglichkeiten der Bürgerbeteiligung *Stender-Vorwachs*, NVwZ 2012, 1061 (1061 ff.).

209 Vgl. *Spiecker gen. Döhmann*, in: Jestaedt, Fragmentierungen: Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Saarbrücken vom 04.–07. Oktober 2017, S. 9 (22 ff.); *Sandfuchs*, Privatheit wider Willen?, S. 48 ff.

Meinungen selbst mitzuprägen.[210] Voraussetzung dafür ist unter anderem die individuelle Möglichkeit zur Entwicklung und Entfaltung einer gefestigten, autonomen Persönlichkeit. Eine solche entsteht durch das Zusammenspiel einer Vielzahl von biologischen, kulturellen und sozialen Faktoren[211], hängt aber im Rahmen dieser Gemengelage an Abhängigkeiten nicht zuletzt von der Existenz einer als Rückzugsort und Freiraum von gesellschaftlich-sozialer Kontrolle fungierenden und damit Phasen der Persönlichkeitssuche und des Ausprobierens ermöglichenden Privatsphäre ab.[212] Im Vordringen ist in letzter Zeit zudem die Erkenntnis, dass neben einem solchen soeben beschriebenen privaten Kommunikationsraum des isolierten Individuums für die (gewissermaßen) Kommunikation mit sich selbst auch ein geschützter Kommunikationsraum notwendig ist, in welchem das Individuum seiner „selbstbestimmten kommunikativen Enthüllung des Privaten als freiem [sic] Kommunikationsakt innerhalb einer freien Kommunikationsgemeinschaft" nachgehen kann.[213]

Auch die *supra* unter A. I. beschriebene instrumentelle Schutzebene von Art. 8 GRCh stützt ein solches Verständnis von Datenschutz und Privatheit als Grundbedingung für eine funktionierende Demokratie, wenn etwa Grundrechte mit noch unmittelbarerem Demokratiebezug wie bspw. Art. 5 Abs. 1 GG oder Art. 11 GRCh durch spezifische aus Datenverarbeitungsvorgängen stammende Gefahren beeinträchtigt zu werden drohen. So verhält es sich beispielsweise mit der anonymen Äußerung politischer Ansichten, die für die demokratische Kommunikation von immenser Bedeutung ist.[214] Die Möglichkeit, solche politischen Äußerungen im Internet anonym kundzutun, kann in großem Maße davon abhängen, dass die Angabe konkreter Identifikationsmerkmale bei Nutzung einer Kommunikationsplattform nicht zwingend ist und andere, die Identifikation ermöglichende, Verarbeitungen unterlassen werden

Mit zunehmender Anzahl von Bürgern, denen Datenschutz vergleichsweise unwichtig erscheint oder die jedenfalls für sich entscheiden, einen liberalen Umgang mit „ihren" Daten ob der versprochenen Vorteile in Form von bspw. unbezahlt[215] nutzbaren Diensten zu pflegen, mit zunehmender Schwierigkeit des Überblickens und Abschätzens der Folgen selbst für solche, die sich aktiv mit der Thematik auseinandersetzen, rücken die gesamtgesellschaftlichen Implikationen des Datenschutzes stärker in den Fokus. Zwar ließe sich hier entgegenhalten, eine arglose und naive Bevölkerung, die sich um den Umgang mit „ihren" Daten keine Sorgen macht oder schlicht keine Notwendigkeit mehr für

[210] Vgl. *Boehme-Neßler*, DVBl 2015, 1282 (1286).
[211] *Boehme-Neßler*, DVBl 2015, 1282 (1287).
[212] Vgl. *Rössler*, Der Wert des Privaten, S. 304.
[213] Siehe m. w. N. *Becker/Seubert*, DuD 2016, 73 (76); die kommunikationsermöglichende Wirkung von bspw. Steuer-, Statistik- und Arztgeheimnissen betonend auch *Dammann*, ZD 2016, 307 (310).
[214] Vgl. *Kersten*, JuS 2017, 193 (201 ff.).
[215] Der Begriff „kostenlos" soll hier bewusst vermieden werden.

Privatsphäre in der heutigen Zeit sieht,[216] könne nicht zeitgleich von der Ausübung bürgerschaftlichen Engagements, etwa in Form von Demonstrationsbesuchen oder der anderweitigen Äußerung (unpopulärer oder abweichender) politischer Ansichten, abgeschreckt werden. Dieser Gedanke trifft die Problematik aber nur teilweise, kann es doch auch ohne bewusste Sorge vor den negativen Folgen eines solchen Handelns bereits ausreichen, dass die mit einem Verzicht einhergehenden Nachteile schlicht nicht gesehen oder als vernachlässigbar betrachtet werden und so eine schleichende Anpassung einsetzt.

In ähnlicher Weise können sich die Gefahren unabhängig vom Bewusstsein der Betroffenen zeigen, so etwa wenn die oben beschriebenen Persönlichkeitsprofile auf Basis personenbezogener Daten genutzt werden, um sog. Microtargeting, also das zielgenaue Ausspielen politischer Werbung durch Parteien oder andere Interessenverbände auf den Profilen und Feeds individueller, bestimmter Profilgruppen zugehöriger, Wähler, zu unterstützen.[217] Werden hierbei individuelle Tendenzen aufgezeigt und genutzt, die den Betroffenen selbst nicht offenbar und bewusst sind (etwa die Anfälligkeit für eine bestimmte Art von Verschwörungstheorien oder ähnliches), und werden diese ggf. kombiniert mit der gezielten Verbreitung falscher oder verzerrt dargestellter Tatsachen, hat dies das Potential, Wahlen in starkem Ausmaß zu beeinflussen oder gar zu entscheiden. Beispielhaft lassen sich hier in der jüngsten Vergangenheit vor allem der *supra* bereits ausgebreitete Cambridge Analytica-Skandal[218] und seine Bedeutung für die (jeweils 2016 stattgefundenen) Abstimmungen bzgl. der US-Wahlen und des Brexit-Referendums anbringen. Die auf Basis der dort gewonnenen Nutzerdaten angelegten Profile wurden genutzt, um Parteien, aber auch fremden Interessenverbänden, das zielgenaue Ausspielen von Werbung und Informationen an konkret definierte Wählerzielgruppen, etwa auf Facebook, anzubieten. Während die Nutzung dieses Angebots im Rahmen des US-Wahlkampfs 2016[219] sowie des Brexit-Referendums[220] umfassend behandelt wurde, ist der konkre-

---

[216] Dieser Ansatz kulminierte zwischenzeitlich in der sog. Post-Privacy-Bewegung, die sich von der 2010 vom Facebook-Gründer Mark Zuckerberg getätigten Aussage „the age of privacy is over" schön beschreiben lässt. Vgl. *Bobbie Johnson*, Privacy no longer a social norm, says Facebook founder, The Guardian vom 11.01.2010 (https://www.theguardian.com/technology/2010/jan/11/facebook-privacy). Zuletzt abgerufen am 14.01.2022.

[217] Für einen Überblick über den Forschungsstand zu dem Phänomen in Rechts- und Sozialwissenschaften siehe *Borgesius* u. a., ULR 2018, 82; *Kolany-Raiser/Radtke*, Microtargeting – Gezielte Wähleransprache im Wahlkampf; *iRights.Lab*, Forschungsstand: Microtargeting in Deutschland und Europa – Fehlende Transparenz und viele offene Fragen.

[218] Siehe hierzu ausführlich Kapitel 1 A. I. 2.

[219] Siehe hierzu umfassend und m. w. N. *Rahul Rathi*, Effect of Cambridge Analytica's Facebook ads on the 2016 US Presidential Election, towards data science vom 13.01.2019 (https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d). Zuletzt abgerufen am 14.01.2022.

[220] Siehe hierzu *Carole Cadwalladr & Mark Townsend*, Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica, The Guardian vom 24.03.2018

te Einfluss auf die Wahlergebnisse nach wie vor unbelegt und wurden Untersuchungen auch in anderen Wahlen meist ergebnislos wieder beendet.[221]

b) Fremdgefährdungen durch Eigengefährdungen

Eine weitere Kategorie überindividueller Gefahren kann darin gesehen werden, dass Entscheidungen, die einzelne Individuen hinsichtlich der Freigabe der sie betreffenden Daten treffen, nicht nur sie selbst betreffen, sondern negative Auswirkungen auch für andere Individuen zeitigen, sei es unmittelbar oder mittelbar.[222] Diese Gefahren werden zeigen, dass die an und für sich bereits realitätsferne Behauptung, es könne sich ja jeder, der mit gängigen Datenverarbeitungspraktiken nicht einverstanden ist, zu einem digitalen Verzicht, einer Art digitalen Abstinenz entscheiden und so die eigene Überwachung verhindern und den erwarteten negativen Folgen entgehen,[223] nicht zutreffend ist.

Auf der unmittelbarsten Ebene umfasst diese Kategorie konkret Fälle, in denen Privatnutzer eines datenverarbeitenden Dienstes durch ihr Handeln veranlassen, dass auch Daten mit Drittpersonenbezug (etwa zu Freunden, Familienmitgliedern etc.) verarbeitet und übermittelt werden. Beispiele solcher Fälle sind etwa der Einsatz von Google Home, Amazon Alexa und anderen (meist dauerhaft[224]) auf akustische Befehle hin zuhörenden Sprachassistenten und Smart Home-Geräten[225] in der eigenen Wohnung bei ggf. betroffenen Besuchern[226] (oder ähnlich unwissenden bzw. einwilligungsunfähigen Kindern[227]) oder das Synchronisieren des eigenen digitalen Kontaktbuchs (inklusive ggf. „abstinenter" Kontakte) mit Messengern wie WhatsApp oder dem Facebook

(https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions). Zuletzt abgerufen am 14.01.2022.

221 So etwa in Italien, vgl. MMR-Aktuell 2019, 415069.

222 Vgl. *Fairfield/Engel*, Duke Law Journal 2015, 95 (423 ff.).

223 In die Richtung etwa *Mayer-Schönberger*, Delete, S. 128 ff.; ähnlich *Heckmann*, K&R 2010, 1 (2) in Bezug auf das Teilen von eigenbezogenen Daten in sozialen Netzwerken.

224 Für einen Überblick über die Risikopotentiale solcher Geräte und eine Unterscheidung der verschiedenen Modi des Zuhörens siehe *Hense*, DSB 2019, 250 (253). Für eine US-amerikanische Perspektive siehe *Pfeifle*, Washington Law Review 2018, 421.

225 Neben Sprachassistenten betrifft dies (mit teils anderen Sensordaten) auch Produkte wie intelligente Autos, Fernseher, Küchengeräte und Staubsaugerroboter. Ein weiteres aktuelles Diskussionsthema in diesem Zusammenhang ist die von unter anderem Google gelebte Praxis, die aufgezeichneten Gesprächsmitschnitte von Mitarbeitern auswerten zu lassen. Der Hamburger Datenschutzbeauftragte eröffnete im August 2019 in diesem Zusammenhang ein Verwaltungsverfahren gegen Google (https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant). Link zuletzt abgerufen am 14.01.2022.

226 Siehe *Schönherr* u. a., arXiv:2008.00508 [cs] 2020 für eine Studie zu den zahlreichen Begriffen, die aufgrund (teils nur sehr entfernt gegebener) phonetischer Ähnlichkeit zu den jeweiligen Auslösebegriffen die gängigsten Smart Assistants selbst dann in den Zuhör-Modus versetzen, wenn der entsprechende Begriff in einem Lied oder einer TV-Sendung vorkommt. Siehe außerdem *Vogel*, K&R 2017, 441 (443 ff.).

227 Vgl. *Hornung*, VuR 2018, 41 zu „smarten", mithörenden Kinderspielzeugen.

Messenger. Streng genommen fallen diese Fälle allerdings eher in die Kategorie klassischer individueller Gefährdungen der betroffenen Dritten, da letztlich für jede Verarbeitung der sie betreffenden Daten (jedenfalls auch) eine unmittelbare Verantwortlichkeit des aktiven Nutzers in Betracht kommt, solange die Grenzen der Haushaltsausnahme gem. Art. 2 Abs. 2 lit. c DSGVO überschritten sind. Mit anderen Worten: Die (veranlasste) unmittelbare Verarbeitung von personenbezogenen Daten durch einen Dienste- oder Produktanbieter unter Mithilfe bzw. Veranlassung durch dessen Nutzer unterscheidet sich hinsichtlich der Individualbezogenheit der Gefährdung nicht von anderen Datenverarbeitungen, die ohne aktives Zutun des Betroffenen zustande kommen.

„Echte" überindividuelle Fremdgefährdungen liegen demgegenüber erst dann vor, wenn Datenpreisgaben und anderweitige individuelle Handlungen mit Datenverarbeitungsbezog auf einer strukturellen Ebene für Teile der Bevölkerung zu Gefährdungen oder gar konkreten Nachteilen führen, die sich nicht unmittelbar aus einer konkreten Verarbeitung ergeben. Häufig betriff diese Art von Fremdgefährdungen speziell diejenigen Bevölkerungsgruppen, die sich der Nutzung datenverarbeitungsintensiver Dienste und Produkte gezielt widersetzen. Als Beispiel anführen lässt sich die zunehmende (nationale wie internationale) Tendenz von Krankenkassen,[228] diejenigen Mitglieder durch Bonusprogramme oder günstigere Tarife zu privilegieren, die durch Nutzung der krankenkasseneigenen App oder des Fitness-Trackers eines kooperierenden Unternehmens ihre gesunde und sportliche Lebensweise belegen.[229] Werden solche Angebote, im Rahmen derer der unmittelbare Verarbeitungszweck bei freier Entscheidungsmöglichkeit noch angemessen erscheinen mag, gleichzeitig aber auch regelmäßig zusätzliche (monetäre) Weiterverwendungszwecke mitgedacht sind, so großflächig genutzt, dass das Ausnahme- zum Regelverhältnis wird, so führt das im schlimmsten Fall zu einer strukturellen Schlechterstellung derer, die sich gegen das Teilen solch sensibler Gesundheitsdaten entscheiden. Abstrahiert vom konkreten Krankenkassenszenario bedeutet dies: Etabliert sich aufgrund des freizügigen Datenpreisgabeverhaltens einer bestimmten kritischen Masse in der Gesellschaft eine bestimmte soziale oder unternehmerische Praxis, so verringert das auch den Korridor, in dem der restliche Teil der Bevölkerung seine Verhaltensfreiheit ausleben kann. Hinzu kommt, dass der Verweigerung einer bestimmten Datenpreisgabe in solchen Fällen oftmals bereits ein eigenständiger Informationsgehalt zukommt – namentlich, dass die Preisgabe unter den vom potenziellen Vertragspartner gesetzten Kriterien für den

[228] Hier ließen sich beliebig weitere Beispiele (teilweise) weniger gesellschaftsrelevanter Dienstanbieter wie KFZ-Versicherungen, Mietwohnungen oder Webshops anführen.

[229] Instruktiv zu den derzeitigen Praktiken in Deutschland *Katharina Nocun*, Tracking durch die Versicherung: Zu Risiken und Nebenwirkungen, Netzpolitik.org vom 19.05.2018 (https://netzpolitik.org/2018/tracking-durch-die-versicherung-zu-risiken-und-nebenwirkungen/). Zuletzt abgerufen am 14.01.2022.

Nutzer nicht vorteilhaft wäre (sonst würde er – jedenfalls bei unterstellter Rationalität – diese ja preisgeben[230]), dieser also im Umkehrschluss persönliche Eigenschaften aufweist, die auf den potenziellen Vertragspartner eher negativ wirken könnten.[231] Das kann dazu führen, dass die Gruppe derjenigen, die nicht in die entsprechende Datenverarbeitung einwilligen, auf Basis dieser impliziten Vermutung schlechter behandelt wird, als es auf Basis ihrer tatsächlichen Eigenschaften angemessen wäre. Ebenso kann es dazu führen, dass eigentlich unwillige Personen nun einwilligen, um genau dies zu verhindern. Damit wird letztlich das Gesamtbild verzerrt und der weit verbreitete Eindruck, ein Großteil der Nutzer messe den eigenbezogenen Daten keinen großen Wert zu, unzulässig verstärkt.[232]

3. Abgleich mit der DSGVO

Gleicht man das Spektrum dieser unterschiedlichen konkreten Gefahrenszenarien in einem ersten Schritt mit der DSGVO ab, fällt auf, dass zahlreiche der dort verankerten Normen und Instrumente – teils explizit, teils implizit – die entsprechenden Kategorien und ihre Spezifika in den Blick nehmen. Betrachtet man etwa den als abstraktes Grundprinzip in Art. 5 Abs. 1 lit. b DSGVO verankerten, aber sich für jede Erhebung und Verwendung von Daten konkret als materielle Rechtmäßigkeitsvoraussetzung manifestierenden, Zweckbindungsgrundsatz, lässt sich dieser leicht als Versuch eines Gegenentwurfs zur oben[233] beschriebenen Gefahr durch potenziell grenzenlose und im Vorfeld kaum absehbare Weiterverwendungsmöglichkeiten von Daten infolge von Verknüpfungen und Entkontextualisierungen sowie weiter wachsender Rechenkapazitäten interpretieren.[234] Auf materieller Ebene soll damit den Gefahren vorgesorgt wer-

---

[230] Vgl. *Hess/Schreiner*, DuD 2012, 105 (105 f.).

[231] Ausführlicher zu diesem und dem weitergehenden Unraveling-Phänomen *Hermstrüwer*, Informationelle Selbstgefährdung, S. 184 ff.; vgl. auch *Peppet*, Northwestern University Law Review 2011, 1153 (1176); *Acemoglu* u. a., Too Much Data.

[232] Siehe *Acemoglu* u. a., Too Much Data, S. 36 ff.: „Moreover, because the data of a subset of users reveal information about other users, the market price of data tends to be depressed, creating the impression that users do not value their privacy much."

[233] Unter A. II. 1.

[234] Zum grundlegenden Konflikt zwischen dieser, Big-Data-Anwendungen inhärenten, Herangehensweise an das Sammeln und Analysieren von Daten einerseits und dem Zweckbindungsgrundsatz andererseits siehe unter anderem *Zarsky*, Seton Hall L. Rev. 2016, 995; *Helbing*, K&R 2015, 145 (146 ff.); *Wenhold*, Nutzerprofilbildung durch Webtracking, S. 39 ff.; ausführlich und speziell die möglichen Ausnahmen der Zweckbindung zugunsten Big Data betonend *Mayer-Schönberger/Padova*, Colum. Sci. & Tech. L. Rev. 2016, 315; ausführlich zum Verhältnis zwischen Innovation und Regulierung im Rahmen des Zweckbindungsprinzips (speziell für von konstanter Entwicklung und Veränderung dominierte Startup-Unternehmen) außerdem *von Grafenstein*, The Principle of Purpose Limitation in Data Protection Laws; generell zu den Risiken von Big Data *Kuner* u. a., IDPL 2012, 47; siehe außerdem *Gürses/van Hoboken*, in: Selinger/Polonetsky/Tene, The Cambridge Handbook of Consumer Privacy, S. 579.

den, die mit *Albers* auf der Verwendungsebene einzustufen sind: konkrete, den Betroffenen schädliche und daher zu unterbindende Handlungen auf Basis der aus den verarbeiteten Daten gewonnenen Informationen. Indem der Verantwortliche bereits bei Erhebung von Daten definieren muss, zu welchem Zweck er diese erhebt und zu verarbeiten gedenkt, setzt er selbst bereits grundsätzlich[235] den Rahmen[236], innerhalb dessen er zukünftig rechtmäßig agieren darf.[237] Instrumentell kann die Zweckbindung in Kombination mit dem (ebenfalls als abstraktes Prinzip in Art. 5 Abs. 1 lit. a DSGVO verankerten) Transparenzprinzip und den daraus hervorgehenden Informationspflichten in Art. 12 ff. DSGVO zudem als Versuch betrachtet werden, die das Individuum treffenden Unsicherheiten zu mildern[238] – indem dieses stets vor[239] oder jedenfalls schnellstmöglich nach[240] Erhebung über die Tatsache, aber auch die wichtigsten Umstände der Verarbeitung und insbesondere den definierten Zweck informiert werden muss. Gleiches gilt für die Weiterverarbeitung zu einem neuen, mit dem bisherigen Zweck kompatiblen Zweck[241] oder einer Weitergabe der Daten an Dritte[242]. Auch diese Informationspflichten lassen sich wieder aufgliedern in einen instrumentellen Wert und einen Wert an sich: instrumentell als Gewährleistung der notwendigen Transparenz für den Betroffenen, um Gebrauch von seinen Möglichkeiten zum Selbstdatenschutz zu machen (etwa die Rechtmäßigkeit der Verarbeitung oder die Richtigkeit der verarbeiteten Daten zu überprüfen); als Wert an sich zur Abmilderung der oben beschriebenen Unsicherheit hinsichtlich des Wissens, das andere über die eigene Person haben, und somit zur (versuchten) Aufrechterhaltung der zu einer stabilen Persönlichkeitsentwicklung und -entfaltung beitragenden Mindestsicherheit.

Gleichzeitig offenbart sich mit zunehmender Konkretisierung der betrachteten Gefahren die bereits erwähnte Dimension des Datenschutzes als Vor-

---

235 Von den Ausnahmen in Art. 6 Abs. 4 DSGVO einmal abgesehen.

236 Eine elementare Rolle spielt dabei die (stark debattierte) Frage, wie breit ein selbst definierter Zweck formuliert sein darf: je breiter, desto geringer die Einschränkungen für den Verantwortlichen, desto geringer aber auch die Vorhersehbarkeit für den Betroffenen und desto geringer also auch die Schutzwirkung. Siehe *Art. 29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, S. 15 f.: „[…] it must be detailed enough to determine what kind of processing is and is not included within the specified purpose." Vage und generelle Zwecke wie „Verbesserung des Nutzererlebnisses" oder „Marketingzwecke" seien daher nicht spezifisch genug.

237 Siehe *Art. 29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, S. 4 f.

238 Vgl. *Art. 29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, S. 13 f.: „There is a strong connection between transparency and purpose specification."

239 Vgl. Art. 13 Abs. 1 DSGVO, bei Erhebung direkt beim Betroffenen.

240 Vgl. Art. 14 Abs. 3 DSGVO, bei anderweitiger Erhebung.

241 Vgl. Art. 13 Abs. 3, 14 Abs. 4 DSGVO.

242 Vgl. Art. 13 Abs. 1 lit. e, 14 Abs. 1 lit. e DSGVO. Gleichzeitig muss der Empfänger der Daten als datenerhebender Verantwortlicher natürlich seinerseits seiner Informationspflicht aus Art. 14 Abs. 1 DSGVO nachkommen. Zumindest auf dem Papier ist somit gewährleistet, dass der Betroffene über jede Person, die ihn betreffende Daten speichert und in Verwendung hat, Bescheid weiß.

feldschutz, der nicht konkrete Handlungen und ihre negativen Wirkungen auf den Einzelnen verbietet und verhindert, sondern auf einer abstrakteren Ebene durch Strukturierung der Daten- und Informationsflüsse, die die nachgelagerten Handlungen überhaupt erst ermöglichen, für eine Reduzierung des Eintrittsrisikos konkreter schädlicher Folgen sorgt. Eine Suche innerhalb der DSGVO nach Normen, die konkrete Handlungen in konkreten Kontexten auf Basis von Datenverarbeitungen verbieten, wird daher[243] erfolglos verlaufen. Ebenso, wie die DSGVO dem Ideal der Technikneutralität verschrieben ist, ist sie in großen Teilen jedenfalls auf der Oberfläche auch einer gewissen Wirkungsneutralität verschrieben. Werden personenbezogene Daten ohne taugliche Rechtsgrundlage verbreitet, so ist dies unabhängig davon rechtswidrig, ob die verbreiteten Daten bei Kenntnisnahme durch ein bestimmtes Publikum eine Bloßstellung für den Betroffenen bedeuteten, also kompromittierende Wirkung entfalten können oder nicht.[244]

Nichtsdestotrotz werden auch im Rahmen der DSGVO und insbesondere auf Ebene der Rechtsgrundlagen von Datenverarbeitungen Überlegungen hinsichtlich der diesen nachgelagerten Handlungen und Entscheidungen angestellt. Einfallstor für solche Überlegungen ist zunächst wieder der Zweckbindungsgrundsatz, durch den der Korridor, in dem sich mögliche Folgehandlungen abspielen dürfen bzw. können, definiert wird. Zieht man diesen zur Prüfung der verschiedenen in Art. 6 Abs. 1 DSGVO aufgezählten Erlaubnistatbestände heran, ergibt sich faktisch eine Art Abschätzung der (Gefährlichkeit der) späteren Handlungen und Entscheidungen. Im Rahmen der Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) geschieht dies durch den Betroffenen selbst, der auf Basis der ihm erteilten Informationen eine Entscheidung *pro* oder *contra* Verarbeitung trifft. Im Rahmen des Tatbestandes der überwiegenden berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DSGVO) bedarf es neben einer einzelfallabhängigen Abwägung zwischen den gegenüberstehenden Interessen zunächst der Anerkennung der vom Verantwortlichen verfolgten oder vertretenen Interessen als *berechtigt* – Verarbeitungen, durch die Interessen und Zwecke erreicht werden sollen, die nicht im Einklang in der Rechtsordnung sind, werden also bereits hier ausgeschlossen.[245] Auch bei der nachgelagerten Interessensabwägung kann für die eine oder die andere Seite erschwerend oder erleichternd zurückgegriffen werden auf Faktoren wie die Menge und Sensibi-

[243] Mit wenigen Ausnahmen wie bspw. Art. 22 DSGVO, der ausschließlich automatisierte Entscheidungen auf Basis der Verarbeitung personenbezogener Daten im Grundsatz verbietet.

[244] Die Wirkung erlangt dann erst wieder auf Rechtsfolgenebene, also etwa bei der Frage nach einem möglichen Schaden im Rahmen eines etwaigen Schadensersatzes (vgl. Art. 82 Abs. 1 DSGVO), oder bei der Berechnung eines möglichen Bußgeldes (vgl. Art. 83 Abs. 2 lit. a DSGVO) Relevanz.

[245] Vgl. *Schantz*, in: Simitis u. a., DSGVO/BDSG, Art. 6 Abs. 1 DSGVO Rn. 98; *Art. 29-Datenschutzgruppe*, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, S. 25.

lität der zu verarbeitenden Daten sowie, im Rahmen des Topos der vernünftigen Erwartungen der betroffenen Person,[246] die Öffentlichkeit der Daten oder das Vorliegen besonderer Vertraulichkeitsgründe durch Berufsgeheimnisse oder ähnliches.

Während sich also nicht für alle genannten konkreten Gefahrenszenarien explizit ein Gegenpart innerhalb der DSGVO finden lässt, lassen die zahlreichen offenen Formulierungen und Abwägungstatbestände genügend Spielräume, um die jeweiligen Spezifika der unterschiedlichen Gefahren mit einfließen zu lassen – sowohl auf Tatbestandsseite als auch auf Rechtsfolgenebene im Rahmen der Bestimmung von Bußgeldern oder im Rahmen der Determinierung eines Schadens bzw. einer Schadenshöhe.

III. Der Regelungszweck: Risikovorsorge, Gefahrenabwehr oder Rechtsgüterausgleich?

Versuchte man mit dem soeben hergeleiteten Verständnis den Zweck der Regulierung privater Datenverarbeitungen in der DSGVO in einem Satz zusammenzufassen, so wäre der folgende zumindest eine erste Annäherung: Das private Datenschutzrecht im Rahmen der DSGVO strukturiert und begrenzt die Möglichkeiten der Verarbeitung personenbezogener Daten mit dem Ziel des Ausgleichs der Interessen und Grundrechte von Datenverarbeiter und Betroffenem unter dem Eindruck der mit der Verarbeitung einhergehenden Gefahren und Risiken.[247] Ein solches Verständnis nähert sich dem an, das bereits 1998 *Hoffmann-Riem* anklingen ließ, als er (zum Recht auf informationelle Selbstbestimmung) konstatierte, dieses wandele sich „vom Grundrecht zur Abwehr staatlicher Eingriffe zum Element der Sicherung einer mehrdimensionalen und mehrpoligen kommunikativen Entfaltung in der Informationsgesellschaft“ und ermächtige wie auch verpflichte den Gesetzgeber, eine „funktionierende, Chancengleichheit ermöglichende Kommunikationsinfrastruktur“ zu schaffen.[248] Dabei soll die Verwendung des Begriffs „Ausgleich“ nicht darüber hinwegtäuschen, dass die Stoßrichtung hier im Grundsatz geprägt ist vom Gedanken eines – wenn auch grundrechtlich nicht besonders stark determinierten – Schutzes. *Marsch* bringt dies gut auf den Punkt, wenn er beschreibt, dass die Strukturermächtigung des Art. 8 Abs. 1 GRCh den Ausgestaltungskorridor des Gesetzgebers „zugunsten der Betroffenen und damit zu Lasten der Datenverarbeiter“ verschiebt.[249]

---

[246] Vgl. Erwg. 47 S. 1 Hs. 2 DSGVO.

[247] Vgl. auch *Bunnenberg*, JZ 2020, 1088 (1090): „Aufgrund ihrer freiheits-, gleichheits- und demokratiegefährdenden Effekte kann die im Bereich der Verbraucherdatenverarbeitung zu verzeichnende Dynamik nicht unreguliert bleiben.“

[248] *Hoffmann-Riem*, AöR 1998, 513 (525).

[249] *Marsch*, Das europäische Datenschutzgrundrecht, S. 269.

Nichtsdestotrotz stellt sich, verlagert man den Blick auf die einen Abstraktionsgrad höher gelagerte Ebene des Grundcharakters der Regelung, die Frage, welchen übergelagerten Regelungszweck man ihr zuschreiben möchte. Einerseits bietet sich mit Blick auf die zuvor geschilderte Idee des Vorfeldschutzes und der Verhinderung der mit der Verarbeitung personenbezogener Daten durch Private einhergehenden Gefahren oder gar der Materialisierung der Risiken des Entstehens solcher Gefahren ein Verständnis an, das sich dem speziellen Gefahrenabwehr- oder Risikovorsorgerecht[250] einerseits und dem (Technik-)Regulierungsrecht[251] andererseits annähert, indem durch Aufstellung präventiver Verarbeitungsbedingungen die Verarbeitungsfolgen in geordnete, „verbindlich vorgezeichnete" Bahnen zu lenken versucht werden.[252] Die Regelungskonzeption wäre dann, im Einklang mit der soeben geschilderten Stoßrichtung, eine betroffenenzentrierte und von einem Schutzgedanken geleitete.

Demgegenüber wird häufig die besondere gesellschaftliche Bedeutung eines freien Informationsflusses[253] ins Feld geführt, die möglicherweise ein stärker auf Ausgleich zentriertes Verständnis rechtfertigt. Richtigerweise ist der Informationsfluss – und zwar unabhängig vom oben behandelten freien Daten*verkehr*, der in erster Linie den *wirtschaftlichen* Verkehr betrifft[254] – insofern die natürliche Kehrseite des Datenschutzes, als ein höheres Niveau an Datenschutz stets eine größere Informationsflussbegrenzung darstellt, und umgekehrt.[255] Dementsprechend liegt die Annahme eines besonders engen Bezugs zwischen dem

[250] Insoweit man das Ziel negativ definiert als die Abwesenheit von bzw. das Geringhalten der verarbeitungsbezogenen Gefahren unter einem bestimmten Level. Vgl. auch *Albers*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 213 (232): „Consequently, it is less the steering idea which characterizes or should characterize data protection law than, similar to environmental law, the idea of risk regulation."

[251] Insoweit man das Ziel positiv und der Daseinsvorsorge dienend formuliert als Schaffung eines Rahmens an Verarbeitungsbedingungen, der die Tätigkeiten der verarbeitenden Privaten so begrenzt und lenkt, dass er dem Einzelnen in Zeiten ubiquitärer Datafizierung garantiert, seine Grundrechte weiterhin in größtmöglichem Maße auszuüben, vgl. *Lepsius*, in: Fehling/Ruffert, Regulierungsrecht, S. 1055 Rn. 1 ff. Die demokratietheoretische Bedeutung einer solchen Garantie betonend *Spiecker gen. Döhmann*, in: Jestaedt, Fragmentierungen: Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Saarbrücken vom 04.–07. Oktober 2017, S. 9 (55); auch *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 244 betonen die Wurzeln des Datenschutzrechts im Technik-, Technikfolgen- und Technikregulierungsrecht.

[252] *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 18.

[253] Siehe insbesondere zur Bedeutung des freien Informationsflusses für menschliche Entfaltung und Teilhabe *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann, Verwaltungsrecht in der Informationsgesellschaft, S. 9 (55.).

[254] Vgl. etwa *Schantz*, in: BeckOK Datenschutzrecht, Art. 1 DSGVO Rn. 2; sowie *Sobotta*, in: Grabitz u. a., Das Recht der Europäischen Union, Art. 16 AEUV Rn. 34, der diese Binnenmarktsdimension des Datenschutzrechts auf den ursprünglichen Erlass der DSRL auf Basis der Binnenmarktkompetenz des damaligen Art. 95 EGV (heute Art. 114 AEUV) zurückführt.

[255] Zur gesellschaftlichen Dimension personenbezogener Daten und insbesondere zur Differenzierung zwischen Daten und Informationen siehe *Albers*, Informationelle Selbstbestimmung.

hinter dem einfachgesetzlichen privaten Datenschutzrecht stehenden Datenschutzgrundrecht und den das Konzept des freien Informationsflusses normativ ausformenden Kommunikationsgrundrechten wie der Meinungs- und Informationsfreiheit gem. Art. 11 GRCh[256] auf der Hand.

Allein daraus erschließt sich aber nicht, weshalb dem freien Informationsfluss eine grundlegende Sonderrolle zukommen sollte, die über die Berücksichtigung hinausgeht, die bei in Grundrechte eingreifenden Gesetzen im Rahmen der Verhältnismäßigkeit und insbesondere der Angemessenheit, teils mittels praktischer Konkordanz,[257] sowieso zuteil kommen muss. Ein struktureller Unterschied zu anderen Grundrechten, die typischerweise in Konflikt zueinanderstehen oder anderen Gesetzen, die primär die Ausübung eines konkreten Grundrechts beschränken, ist nicht ersichtlich; auch das Versammlungsrecht beschränkt in allererster Linie das Grundrecht auf Versammlungsrecht im Interesse des Schutzes der öffentlichen Sicherheit und ist seiner Materie nach dennoch besonderes Polizeirecht und kein „Ausgleichsgesetz". Oder, mit den Worten von *Hoffmann-Riem*: „Es ist keine Besonderheit des Datenschutzes, daß Schutzmaßnahmen komplex ansetzen und dabei zugleich Begrenzungen anderer Entfaltungsfreiheiten sein können."[258]

Genauso wenig, wie dem Datenschutz bzw. der von ihm geschützten Entfaltungsfreiheit ein genereller Vorrang gegenüber der Informationsfreiheit einzuräumen ist,[259] besteht eine besonders herausragende normative Stellung des Ideals eines freien Informationsflusses als die Regelungsrichtung des privaten Datenschutzrechts prägendes Gut. Zwar darf die Tatsache nicht außen vor gelassen werden, dass in der modernen Informationsgesellschaft unbestritten ein enger Konnex zwischen Datenschutz und Informationsfluss – und damit letzt-

---

[256] Diese haben ihrerseits eine fundamentale gesellschaftliche Funktion mit Blick auf das demokratische Gemeinwesen. Vgl. *Jarass*, in: Jarass, Grundrechtecharta, Art. 11 Rn. 4 sowie die Ausführungen des EuGH, Rs. C-340/00 (K/Cwik), Slg. 2001, I-10269 Rn. 18 und Rs. C-112/00 (Schmidberger), Slg. 2003, I-5659 Rn. 79.

[257] Siehe *Hesse*, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, Rn. 72.

[258] *Hoffmann-Riem*, AöR 1998, 513 (524).

[259] Entgegen der insoweit entweder missverständlichen oder fehlgeleiteten Formulierung (bezogen auf die, ebenfalls in Art. 11 GRCh normierte, Meinungsfreiheit) in EuGH, Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317 Rn. 81, wonach die Rechte der betroffenen Person „im Allgemeinen gegenüber dem Interesse der Internetnutzer" überwiegen sollen. Die Einzelfallabhängigkeit dieser Aussage des EuGH betonend daher BVerfG, Beschluss v. 06.11.2019, 1 BvR 276/17 Rn. 141: „[…] gibt es weder in der Grundrechtecharta selbst noch in der Rechtsprechung des Europäischen Gerichtshofs Anhaltspunkte, dass sich bei einer Abwägung zwischen dem Schutz des Persönlichkeitsrechts einerseits und der Meinungsfreiheit andererseits diese nicht grundsätzlich gleichberechtigt gegenüberstünden." Vgl. dazu auch *Reinhardt*, AöR 2017, 528 (562), der konstatiert, dass das grundsätzliche Gleichgewicht „in den Entscheidungen des Gerichtshofs nicht immer zum Ausdruck" kommt. Für ein gewisses Überwiegen des Schutzes personenbezogener Daten streitend aber *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Art. 1 DSGVO Rn. 26.

lich Kommunikation – besteht. Dieser Tatsache lässt sich aber auch Rechnung tragen, indem man das (einfachgesetzliche) Datenschutzrecht als *einen* legislativen Teilbereich der gesellschaftlichen Informationsordnung[260] oder „Informations- und Kommunikationsinfrastruktur“[261] ansieht, die in ihrer Gänze den oben beschriebenen Ausgleich anstrebt, während der isolierte Teil sich gezielt dem einen, namentlich dem Schutzzweck, widmen kann.

Dem privaten Datenschutzrecht in Form der die Verarbeitung personenbezogener Daten durch Private betreffenden Regelungen innerhalb der DSGVO ist daher ein primär auf Schutz und erst sekundär auf Ausgleich ausgerichteter Regelungszweck zu entnehmen.

B. Der Verantwortliche als Herzstück des Regelungskonzepts der DSGVO

Das Fundament des in der DSGVO ausgestalteten einfachgesetzlichen Datenschutzrechts und damit die Basis ihres auf Schutz ausgerichteten Regelungskonzepts ist der Grundsatz des Verbots mit Erlaubnisvorbehalt: Jede Verarbeitung personenbezogener Daten ist im Grundsatz verboten und bedarf eines im konkreten Fall tragbaren Erlaubnistatbestands, der der – grundsätzlich abschließenden[262] – Liste in Art. 6 DSGVO zu entnehmen ist. Lässt dieses Fundament zunächst ein klassisch imperatives *command and control*-Schutzsystem vermuten, bei dem der Staat ein klares rechtskonformes Verhalten vorgibt und die Normadressaten auf die Konformität ihres Verhaltens hin überwacht und überprüft, offenbart ein genauerer Blick ein komplexes Netz an Instrumenten unterschiedlichster Art, die nicht nur das konkrete Datum und seine Verarbeitung, sondern auch das jeweilige Verarbeitungsumfeld in den Blick nehmen.[263]

So ist das Vorliegen eines tauglichen Erlaubnistatbestandes zur Datenverarbeitung nur die Spitze eines Eisbergs verschiedener Pflichten und Voraussetzungen, deren Missachtung einen Verarbeitungsakt trotz einschlägigen Erlaubnisgrundes rechtswidrig machen und Sanktionen und andere negative Folgen auslösen kann. Der Träger dieser Bündelung an Pflichten und insgesamt der Bürde, die Voraussetzungen für die Rechtmäßigkeit der Datenverarbeitung zu erfüllen, ist der *Verantwortliche*. Diese datenschutzrechtliche Figur kann auf eine lange Tradition zurückblicken und hat in ihrer Bedeutung und Ausformung

[260] *von Lewinski*, Die Matrix des Datenschutzes, S. 63.

[261] *Hoffmann-Riem*, AöR 1998, 513 (523).

[262] Die Öffnungsklauseln in Art. 6 Abs. 2 und 3 DSGVO verschaffen den Mitgliedstaaten die begrenzte Möglichkeit, durch Erlass eigener Rechtsvorschriften das Ausmaß gesetzlicher Erlaubnistatbestände zu erweitern.

[263] Vgl. *Albers*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 213 (230): „Rather than merely steering the steps of processing data, appropriate regulation concepts require many different elements.“

auch nach Ablösung der DSRL (samt ihren mitgliedstaatlichen Umsetzungen) durch die DSGVO weiterhin und im Großen und Ganzen unverändert Bestand.[264] Gekennzeichnet ist sie durch das Ideal eines zentralen Akteurs, dessen aufgrund der Erfüllung bestimmter Voraussetzungen vermutete Nähe zu und Einflussmöglichkeiten auf eine(r) Datenverarbeitung es nahelegen, ihm die Einhegung der aus dieser resultierenden Gefahren zu überantworten. Damit einher geht (der Versuch) einer(r) Lenkung und Steuerung des Verantwortlichen in unterschiedlichster Weise, bezogen nicht nur auf die Verarbeitungshandlungen selbst, sondern auch auf die Handlungs- und Entscheidungsstrukturen und -prozesse, in welche die Datenverarbeitungen eingebettet sind, auf die genutzten Techniken und insgesamt das Bewusstsein für die Datenschutzrelevanz des eigenen Handelns.

Im Folgenden soll dieses Regelungskonzept in seiner Komplexität und Bandbreite aufgezeigt und systematisiert werden (I.). Die hier vorgenommene Betrachtung der einzelnen Instrumente geht dabei von einem (utopischen) Idealzustand vollständig effizienter und wirksamer Instrumente aus, gleichzeitig sollen aber mitunter auch kurze relativierende Abgleiche mit bestehenden Praxiserfahrungen und wissenschaftlichen Kritikpunkten eingestreut werden. Dabei sollen alle Konzepte und Instrumente stets auf den Fokalpunkt der Figur des Verantwortlichen rückangebunden und in ihrer Bedeutung für diese erklärt werden. Es soll damit aufgezeigt werden, dass der Verantwortliche *die* zentrale Figur ist, von der der Erfolg der verschiedenen datenschutzrechtlichen Regulierungsinstrumente und damit des gesamten Regelungskonzepts abhängt. Am Ende dieses Abschnitts soll die Erkenntnis stehen, dass sich eine Systematik anbietet, die zwischen der regulatorischen Bedeutung der *Auswahl* der Verantwortlichenfigur (welche Voraussetzungen soll ein Akteur erfüllen, um Verantwortlicher zu sein?) einerseits und ihrer inhaltlichen *Ausgestaltung* (welche Pflichten treffen einen Verantwortlichen? Wie weit reichen diese?) andererseits unterscheidet. Mittels der gewonnenen Erkenntnisse aus Analyse und Systematisierung des Gesamtkonzepts sollen zudem einige Grundprämissen formuliert werden, von deren Vorliegen in der Realwelt die DSGVO (teils implizit, teils explizit) ausgeht und deren tatsächliches Vorliegen für ein Funktionieren des derzeitigen Gesamtkonzepts notwendig ist (II.). Abschließend soll im Rückblick auf die oben unter A. erlangten Erkenntnisse abgeglichen werden, inwieweit das von der DSGVO gewählte Regelungskonzept der Verantwortlichkeit verfassungsrechtlich vorgegeben ist bzw. wie viel Spielraum dem Verordnungsgeber bei der Konzeptgestaltung verbleibt (III).

---

[264] Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 9: „A general observation regarding the concepts of controller and processor in the GDPR is that they have not changed compared to the Directive 95/46/EC and that overall, the criteria for how to attribute the different roles remain the same."

I. Die Komponenten des Regelungskonzepts

Die Auffächerung des Regelungskonzepts soll dabei dergestalt erfolgen, dass zunächst ein Überblick über die verschiedenen Instrumente und ihre wichtigsten Charakteristika und Bedeutungsunterschiede gegeben werden soll, derer sich die DSGVO bedient (1.). Im Anschluss sollen einige der beispielhaft genannten Instrumente hinsichtlich ihrer Steuerungswirkung (2.) und dem jeweiligen Anknüpfungspunkt der Steuerung (3.) noch einmal aufgegriffen und tiefergehend behandelt werden.

1. Die Instrumente des Datenschutzes

a) Der Selbstdatenschutz

Wenngleich, wie oben bei A. I. beschrieben, die informationelle Selbstbestimmung deutscher Prägung keine (vollständige) Kongruenz mit dem europäischen Datenschutzgrundrecht aufweist, kommt dennoch dem Betroffenen und seiner Fähigkeit zum selbstbestimmten und eigenständigen Schutz vor verarbeitungsbedingten Risiken eine gewichtige Bedeutung als Instrument im datenschutzrechtlichen Regelungskonzept zu.[265]

Dabei sind zunächst die unmittelbar die Verarbeitung betreffenden normativen Teilinstrumente in den Blick zu nehmen, die den Betroffenen in die Lage versetzen sollen, Verantwortliche zu kontrollieren und seine eigenen Rechte wahrzunehmen und durchzusetzen. Die Einwilligung als eine, wenn nicht gar (jedenfalls hinsichtlich der praktischen Bedeutung[266] und nach dem Kenntnisstand vieler Laien) *die* Rechtsgrundlage für Datenverarbeitungen gem. Art. 6 Abs. 1 lit. a DSGVO verdeutlicht die Bedeutung des Selbstschutzes.[267] Aus regulatorischer Sicht stellt sie zudem das mildere Mittel zur gesetzlichen Rechtsgrundlage dar, indem sie die Frage der Legitimität einer Verarbeitung der Privatautonomie des Betroffenen überlässt.[268] Dieser Fixpunkt wird ergänzt durch zahlreiche weitere Rechte, die teils der wirksamen und wirklich selbstbestimm-

---

[265] Ausführlich zum Konzept des Selbstdatenschutzes *Karaboga* u. a., Selbstdatenschutz, White Paper des Forums Privatheit.

[266] Vgl. *Reinhardt*, AöR 2017, 528 (557): „Im Fall der Datenverarbeitung durch private Unternehmen hingegen hängt regelmäßig von der Zustimmung ab, in welchem Maß und zu welchen Zwecken auf personenbezogene Daten zugegriffen werden kann."

[267] Nichtsdestotrotz geht es zu weit, mit *Bunnenberg*, Privates Datenschutzrecht, S. 85 den Regulierungsansatz des Datenschutzrechts als „Einwilligungsmodell" zu bezeichnen und von der „zentralen Stellung" der Einwilligung zu sprechen.

[268] Diese regulatorische Zurückhaltung auf inhaltlicher Ebene kann dabei durchaus auch negativ gesehen werden, indem die legislative Entscheidung über Zulässiges und Unzulässiges auf das Individuum übertragen wird. Vgl. *Solove*, Harv. L. Rev. 2013, 1880 (1880): „It attempts to be neutral about substance – whether certain forms of collecting, using, or disclosing personal data are good or bad – and instead focuses on whether people consent to various privacy practices."

ten Erteilung von Einwilligungen, teils der generellen Kontrolle des Handelns von Verantwortlichen dienen.[269] Diesem Zweck dienen vor allen Dingen die Betroffenenrechte der DSGVO, so etwa die Informationspflichten und das Auskunftsrecht in Art. 12–15, die Berichtigungs- und Löschungsrechte in Art. 16–17, das Recht auf Einschränkung der Verarbeitung in Art. 18 und das Widerspruchsrecht in Art. 21 Abs. 1.[270] Insbesondere das letztgenannte Recht sichert die Selbstbestimmung des Betroffenen bei Verarbeitungen, die nicht auf seine Einwilligung, sondern auf die Rechtsgrundlagen der Verarbeitung zum Zwecke einer Aufgabe im öffentlichen Interesse (Art. 6 Abs. 1 lit. e) oder zur Wahrung der berechtigten Interessen des Verantwortlichen (Art. 6 Abs. 1 lit. f) gestützt werden. Ist hier also die Verarbeitung grundsätzlich unabhängig vom Willen des Betroffenen möglich und im jeweiligen Einzelfall auch rechtmäßig,[271] ermächtigt ihn das Widerspruchsrecht, den Verantwortlichen zur Vornahme einer (im Falle des Art. 6 Abs. 1 lit. f. DSGVO erneuten) Interessensabwägung zu zwingen. Ist der Widerspruch erfolgreich, muss der Verantwortliche die Verarbeitung einstellen, sodass eine *ex nunc*-Rechtswidrigkeit der Verarbeitung eintritt.[272] Die bisher gespeicherten Daten sind dann zu löschen (vgl. Art. 17 Abs. 1 lit. c DSGVO). Voraussetzung dafür ist, dass sich gerade aus der Person des jeweiligen Betroffenen Gründe ergeben, aufgrund derer das bei Betrachtung der bloßen Verarbeitungsumstände festgestellte Ergebnis *pro* Verarbeitung nun zugunsten des Betroffenen ausfällt. Dem Verantwortlichen verbleibt dann die Möglichkeit, seinerseits „zwingende schutzwürdige Gründe" (Art. 21 Abs. 1 S. 2 DSGVO) nachzuweisen, um die Fortführung der Verarbeitung zu rechtfertigen.[273] Das Recht stellt damit ein individualzentriertes Korrektiv zu den (notwendigerweise) streng typisiert und ohne Zutun des Betroffenen erfolgenden Abwägungsentscheidungen der beiden genannten Verarbeitungsgrundlagen dar. Würde es dem Verantwortlichen unzumutbar und wohl auch faktisch unmöglich sein, etwa bei der Abwägung der eigenen berechtigten Interessen mit denen der Betroffenen auch außergewöhnliche individuelle Umstände zu berücksichtigen, ist er so zumindest gezwungen, diese bei individuellem Vorbringen zu berücksichtigen und seine Verarbeitung(en) entsprechend zu beenden.

---

[269] Vgl. etwa *Reinhardt*, AöR 2017, 528 (560): „Die prinzipielle Auskunftspflichtigkeit der datenverarbeitenden Stellen soll auch zu einem datenschutzrechtskonformen Umgang mit personenbezogenen Daten anhalten."

[270] Zur Stellung dieser Rechte und Pflichten im Gefüge des Grundrechts auf Datenschutz gem. Art. 8 GRCh siehe *Reinhardt*, AöR 2017, 528 (542 f.).

[271] Es geht hier also, anders als bei den *supra* beschriebenen Betroffenenrechten, nicht darum, den Betroffenen zum Anprangern und zur Beendigung einer rechtswidrigen Verarbeitung zu ermächtigen. Vgl. *Forgó*, in: BeckOK Datenschutzrecht, Art. 21 DSGVO Rn. 2.

[272] Vgl. *Schulz* in: Gola, DSGVO, Art. 21 Rn. 17.

[273] Eine weitere Ausnahme von der Wirkung des Widerspruchs formuliert die Norm im selben Satz für Fälle, in denen die weitere Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

Daneben existieren mittelbar das Verhalten von Verantwortlichen beeinflussende Maßnahmen, die weniger auf konkrete Verarbeitungen im Einzelfall und mehr auf das Bewusstsein des Einzelnen hinsichtlich seines eigenen verarbeitungsrelevanten Handelns hinwirken. Sie können ebenfalls einen normativen Ursprung haben, wenn etwa Art. 57 Abs. 1 lit. b DSGVO den Aufsichtsbehörden die Aufgabe erteilt, die Öffentlichkeit (und damit potenzielle Betroffene) zu sensibilisieren und aufzuklären, erfahren ihre Wirkung aber erst durch eine generelle und nicht zwingend auf konkrete Verarbeitungen bezogene Verhaltensanpassung der Nutzer. Dazu gehört insbesondere die Nutzung technischer Tools, sog. *privacy enhancing technologies* (PETs),[274] die bspw. eine anonym(er)e Nutzung von Diensten erlauben,[275] ein besseres Verständnis von Datenschutzerklärungen bzw. besser informierten Einwilligungen anstreben[276] oder generell die Ausübung der oben beschriebenen Rechte erleichtern[277]. Sie wirken ebenfalls auf ein datenschutzkonformes oder gar überobligatorisch datenschutzfreundliches Agieren von Verantwortlichen hin, indem sie (im Falle der Betroffenenrechte und der sie betreffenden PETs) das Verständnis und damit die Kontrolle durch Betroffene steigern oder (im Falle von Tools wie Trackmenot) möglicherweise datenschutzkonforme, aber unerwünschte Verarbeitungen verhindern. Eng damit verknüpft ist schließlich auch die Hoffnung, dass aufgeklärte und mit einem Bewusstsein für den Schutz der sie betreffenden Daten agierende Nutzer aktiv nur noch solche Dienste nutzen, die sich durch datenschutzfreundliche Ausgestaltungen auszeichnen, sodass entsprechende Marktanreize gesetzt werden und die (über die gesetzlichen Vorgaben hinausgehende) Datenschutzfreundlichkeit von Diensten sich als Wettbewerbsvorteil etabliert.[278]

b) Der Systemdatenschutz

Ein in gewisser Weise bereits „alter Hut" der datenschutzrechtlichen Instrumente, der mit Einführung der DSGVO aber auf ein neues Bedeutungslevel

---

[274] Für einen Überblick, auch über die rechtlichen Rahmenbedingungen, siehe *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt.

[275] Siehe hier exemplarisch die von *Helen Nissenbaum* mitentwickelten Tools Trackmenot (http://trackmenot.io/) und AdNauseam (https://adnauseam.io/). Des Weiteren erwähnenswert ist der Privacy Badger der *Electronic Frontier Foundation* (https://www.eff.org/privacybadger). Ein guter Überblick findet sich zudem beim *Guardian* (https://www.theguardian.com/technology/2020/feb/16/internet-privacy-settings-apps-to-protect-you-). Links zuletzt abgerufen am 14.01.2022.

[276] Vgl. etwa die Ansätze bei *Fatema* u. a., Compliance through informed consent, S. 60 ff.; *Utz* u. a., (Un)informed Consent, S. 973 ff.; *Jarovsky*, EDPL 2018, 447 (447 ff.); zu den kognitiven Limitierungen des Individuums, die solche Anstrengungen erst notwendig machen, siehe *Solove*, Harv. L. Rev. 2013, 1880 (1883 ff.).

[277] Siehe hierzu etwa *Clifford* u. a., German Law Journal 2019, 679 (679 ff.).

[278] Vgl. *Spindler/Thorun*, MMR-Beilage 2016, 1 (9); hierzu, auch an die Verantwortlichen appellierend, *Schröder*, ZD 2012, 193 (194).

mit normativer Absicherung[279] gehoben wurde, ist der Systemdatenschutz.[280] Einzug gefunden hat er dort primär unter den ungleich moderneren Schlagworten *privacy by design* und *privacy by default* und, etwas genereller, dem Prinzip der Datenminimierung, während das bisherige Verständnis im Grunde identisch geblieben ist:[281] Mit Blick auf die rapide technische Entwicklungsgeschwindigkeit und die oftmals fernab von Plan- und Vorhersehbarkeit emergent auftretenden Weiterentwicklungen konkreter einzelner Systeme sollen bereits bei der Planung und Implementation von Systemen datenschutz- und datensicherheitsrechtliche Grundprinzipien und Schutzvorkehrungen eingeschrieben werden, sodass kritische Features bereits in der Entwicklungsphase auffallen und (im Idealfall) verworfen oder jedenfalls hinreichend modifiziert werden, anstatt später ein bereits eingefügtes Element nachträglich entfernen, und überhaupt erkennen, zu müssen.[282] Gleichermaßen soll so gesichert werden, dass auch bei späteren Entwicklungen und Änderungen bestimmte Grundprinzipien gewahrt bleiben und Betroffenenrechte jederzeit einfach ausgeübt werden können.[283] Im Zentrum stehen dabei einerseits über Art. 32 Abs. 1 DSGVO die Schutzziele der Datensicherheit, die organisatorisch und technisch zu gewährleisten sind. Auf diese ist der Systemdatenschutz jedoch nicht begrenzt:

„Die Unerlässlichkeit einer technologischen Reaktion auf eine zunehmend komplexere Informations- und Kommunikationstechnologie rechtfertigt […] nicht die implizite oder gar explizite Verdrängung normativer Verarbeitungsprämissen durch eine nachgerade fetischisierte Datensicherheit.“[284]

Art. 25 Abs. 1 DSGVO verlangt daher unter dem Schlagwort des Datenschutzes durch Technikgestaltung explizit auch die Einführung technischer und organisatorischer Maßnahmen zur Gewährleistung jeglicher Grundprinzipien in Art. 5 Abs. 1 DSGVO sowie der Betroffenenrechte, sowohl bei Festlegung der

---

279 Vgl. *Simitis*, in: Simitis, BDSG, Einleitung Rn. 114, der betont, dass trotz unbestrittener Effektivität von Vorkehrungen des Systemdatenschutzes diese isoliert „noch lange keine Alternative zu gesetzlichen Verarbeitungsrestriktionen“ darstellen und daher der normativen Einbettung bedürfen.

280 Grundlegend und umfassend zum technischen Datenschutz und seinen historischen Bezügen *Pohle*, Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung.

281 Siehe die an die Arbeit der kanadischen Datenschutzbeauftragten *Ann Cavoukian* angelehnte Aufzählung begriffsprägender Eigenschaften bei *Schulz*, CR 2012, 204 (205).

282 Vgl. *European Data Protection Board*, Guidelines 4/2019 on Article 25 (Data Protection by Design and by Default), S. 10: „Early consideration of DPbDD is crucial for a successful implementation of the principles. From a cost-benefit perspective, it would be in the controllers' interest to take this into account sooner rather than later […].“

283 Vgl. *Hansen*, in: Simitis u. a., DSGVO/BDSG, Art. 25 DSGVO Rn. 14 ff.; zudem *Baumgartner/Gausling*, ZD 2017, 308 (309 f.).

284 *Simitis*, in: Simitis, BDSG, Einleitung Rn. 115.

Verarbeitungsmittel wie auch zum eigentlichen Zeitpunkt der Verarbeitung und fortwährend darüber hinaus.[285]

Eine zweite große Rolle spielt die normative Wirkung, die der Technik selbst zukommt: „*code is law*“,[286] und in Code eingeschriebene Regelungen haben im Rahmen der jeweiligen Nutzungsumgebung das Potential, Verhalten ebenso stark, wenn nicht gar stärker, zu beeinflussen wie rechtliche Normen.[287] Dabei hat Code für die Nutzer der jeweiligen Soft- oder Hardware letztlich immer einen gewissen Regelungscharakter, indem er bestimmte Verhaltensweisen erlaubt, verunmöglicht oder durch die Art der Ausgestaltung des Nutzerinterfaces nahelegt oder von ihnen abrät. Gleichzeitig können verfestigte Code-Strukturen – seien sie bewusst herbeigeführt oder emergent entstanden – die Erfüllung rechtlicher Anforderungen ihrerseits faktisch unmöglich machen.[288] Diese normative Wirkmacht zu nutzen und durch entsprechende Verpflichtung der Verantwortlichen in die Richtung der regulatorisch gewünschten Werte zu bewegen, bevor es zu spät ist, ist daher ein Ziel des Systemdatenschutzes.[289] So können die oben beschriebenen technischen Maßnahmen etwa darin bestehen, Verstöße gegen bestimmte Prinzipien, Datenzugriffe durch nicht zugriffsberechtigte Mitarbeiter oder Verarbeitungen, die nicht dem zuvor festgelegten Zweck entsprechen, systemseitig unmöglich zu machen bzw. Verantwortliche jedenfalls rechtzeitig vorzuwarnen.[290] Als unzureichend kritisiert wird das Konzept in seinem in der DSGVO Niederschlag gefundenen Ausmaß jedoch zuweilen deshalb, weil es „nur“ den Verantwortlichen als datenverarbeitenden Akteur verpflichtet, während dieser in der Praxis regelmäßig fertige Software für seine Zwecke lizensiert und daher auf den Gestaltungsprozess keinen Einfluss hat. Die Hersteller und Entwickler der jeweiligen Software hingegen haben auf die später vom Verantwortlichen vorgenommenen Datenverarbeitungen keinen Einfluss und kommen somit nicht selbst als Verantwortliche in Betracht. Es droht somit, so die Kritik,[291] die Gefahr, dass das Konzept in der Praxis bestenfalls auf eine

---

[285] Krit. zu der jetzigen Reichweite von Art. 25 DSGVO und mit eigenen Verbesserungsvorschlägen *Rubinstein/Good*, IDPL 2020, 37 (37 ff.).

[286] *Lessig*, Code and other laws of cyberspace.

[287] Instruktiv zum Einsatz digitaler „*impossibility structures*“ zur Durchsetzung von Recht *Rademacher*, JZ 2019, 702 (702 f.); die in die Technik gesetzten Erwartungen im Datenschutzrecht betonend *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 245.

[288] Vgl. *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 247.

[289] *Simitis*, in: Simitis, BDSG, Einleitung Rn. 115 spricht hier davon, „sich also gerade der Technologie zu bedienen, die genauso den Anstoß für eine Verarbeitungsregelung gegeben hat“.

[290] Für ein Beispiel der Absicherung garantierter Eigenschaft in einem System mittels Methoden der formalen Informatik siehe *Adams* u. a., CLSR 2019, 105337.

[291] Vgl. *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 248.

Pflicht zur Auswahl möglichst datenschutzfreundlicher Software und einen Appell[292] sowie etwaige Marktanreize[293] an die Entwickler, die entsprechenden Konzepte freiwillig zu befolgen, hinausläuft.[294]

Hinzu tritt die in einigen der Normen (so etwa Art. 32 DSGVO) bereits anklingende Ebene der Organisationsstrukturen und Entscheidungsprozesse, die die Entwicklung von Verarbeitungssystemen prägen und begleiten und der konkreten Datenverarbeitung ebenfalls vorgelagert sind. Auch hier – und deshalb nicht nur auf der rein technischen Ebene – setzt Systemdatenschutz an.[295]

Das Instrument des Systemdatenschutzes weist zudem eine enge Verknüpfung zu dem oben beschriebenen Instrument des Selbstdatenschutzes auf.[296] Wenn Art. 25 Abs. 2 DSGVO unter dem Schlagwort des Datenschutzes durch datenschutzfreundliche Voreinstellungen bestimmt, dass technische und organisatorische Maßnahmen sicherstellen müssen, dass standardmäßig die verarbeiteten Daten hinsichtlich ihrer Menge, des Verarbeitungsumfangs, der Dauer ihrer Speicherung und des Ausmaßes ihrer Zugänglichkeit nur auf das Maß begrenzt bleiben, das für den jeweiligen Zweck erforderlich ist, so ist das zunächst eine Konkretisierung des Datenminimierungsprinzips aus Art. 5 Abs. 1 lit. c DSGVO. Darüber hinaus soll damit aber gerade technisch und organisatorisch ein Freiraum abgesichert werden, innerhalb dessen der Betroffene frei und aktiv über das Ausmaß der Verarbeitung entscheiden kann. Davon betroffen ist insbesondere die Frage der Zulässigkeit der Ausgestaltung einer Einwilligung als Opt-in, Opt-out[297] oder Mandated Choice-Verfahren.[298] Daneben kommen die oben beschriebenen PETs in Betracht, mittels derer es den Betroffenen er-

---

[292] Einen solchen enthält auch Erwg. 78 S. 4 DSGVO: „[…] sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen […]"

[293] Normativ unterfüttert werden diese Anreize dann, wenn die Hersteller und Entwickler als Auftragsverarbeiter agieren. Hier wirkt die Pflicht des Verantwortlichen nach Art. 28 Abs. 1, 3 DSGVO zur Auswahl eines geeigneten Auftragsverarbeiters als Transmissionsriemen zur mittelbaren Verpflichtung auch des Herstellers. Vgl. *Moser*, in: Simitis u. a., DSGVO/BDSG, Art. 25 Rn. 5 f. ebenso Baumgartner, in: *Ehmann/Selmayr*, Datenschutz-Grundverordnung, Art. 25 Rn. 5 f.

[294] *Schulz*, CR 2012, 204 (208) befürwortet diesen status quo mit Blick auf die unverhältnismäßige (grundrechtliche) Belastung von Softwareentwicklern bei Ausweitung des Konzepts.

[295] Vgl. *Albers*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 213 (230): „Hence, data protection through system design aims at the legal shaping of the social, organizational, procedural and technical contexts in which personal data and information are handled."

[296] *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 246 sehen in den Möglichkeiten der Technik ein „ebenso willkommenes wie naheliegendes Selbstverteidigungsmittel […]".

[297] Zu der generellen Unwirksamkeit einer Opt-out-Ausgestaltung, bei der ein bereits angekreuztes Kästchen keine eindeutige und unmissverständliche Einwilligungserklärung darstellt, siehe EuGH, Rs. C-673/17 (Planet49), ECLI:EU:C:2019:801 Rn. 61 ff.

[298] Siehe dazu *Martini/Weinzierl*, RW 2019, 287.

leichtert wird, ihre Betroffenenrechte auszuüben oder die von ihnen genutzten Geräte ihrerseits technisch so zu modifizieren, dass Zugriffe auf bestimmte Daten verunmöglicht oder zumindest erschwert werden, sodass auch sie sich nicht nur die normative, sondern auch die sachverhaltserleichternde und transparenzförderliche Wirkmacht der Technik zu Eigen machen können.[299]

c) Die (regulierte) Selbstregulierung

Eine Schnittmenge zu den eben beschriebenen Pflichten zur Implementation organisatorischer und technischer Maßnahmen weisen auch diejenigen Instrumente der DSGVO auf, die den Normadressaten Möglichkeitsräume bei der Umsetzung der ihnen auferlegten Pflichten gewähren. Unter dem Begriff der regulierten Selbstregulierung, gelegentlich auch Co-Regulierung, werden solche staatlichen Instrumente verstanden, die ein gewisses, recht abstrakt gehaltenes Ergebnis bei der Erfüllung einer Pflicht vorgeben, dabei aber genügend Freiraum für die Wahl und das Erarbeiten eines konkreten Lösungsstandards oder eines Zielwerts lassen.[300] Abzugrenzen sind diese Instrumente von der bloßen Selbstregulierung, bei der Unternehmen sich eigene, meist industrie- oder branchenweite Ziele und Selbstverpflichtungen setzen, die aber nicht auf Basis eines staatlichen Handlungsrahmens entstehen und deren Wirksamkeit und deren Einhaltung nicht bzw. jedenfalls nicht von staatlicher Seite überprüft wird.[301] Beispiele dafür sind, je nach Breite des Begriffsverständnisses, branchenweit entwickelte und etablierte Kodizes, aber auch implizit entstandene und verfestigte Prozesse.

Zu einem staatlichen Instrument *regulierter* Selbstregulierung werden solche Prozesse daher erst dann, wenn sie staatlich veranlasst sind und eine zwischengeschaltete Instanz staatlicher Kontrolle hinsichtlich der von Unternehmen oder Branchen erarbeiteten Standards und Maßnahmen aufweisen, also die Überprüfung wahlweise der erarbeiteten Standards selbst, deren Umsetzung

---

[299] Vgl. *Simitis*, in: Simitis, BDSG, Einleitung Rn. 115: „[…] den Betroffenen eine reale Chance einräumen, Kommunikation so zu gestalten, dass sie nicht zwangsläufig zur Diffusion ihrer Daten gerät."

[300] Vgl. *Spindler/Thorun*, MMR-Beilage 2016, 1 (2); *Collin*, JZ 2011, 274 (275) spricht von „Regelungsinstrumente[n], die gesellschaftlicher Betätigung den nötigen Entfaltungsraum gewährleisten und zugleich die Erfüllung gemeinwohlrelevanter Kernziele absichern sollen." Siehe auch *Di Fabio*, in: Hailbronner, Kontrolle der auswärtigen Gewalt: Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, S. 235 (235 ff.).

[301] Siehe bereits *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, S. 261 (300 ff.); *Schmidt-Preuß*, in: Hailbronner, Kontrolle der auswärtigen Gewalt: Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, S. 160 (160 ff.); vgl. zudem *Schulz/Held*, Regulierte Selbstregulierung als Form modernen Regierens, S. A-3; *Spindler/Thorun*, MMR-Beilage 2016, 1 (8).

durch die einzelnen Normadressaten oder auch beides vorsehen. Mit anderen Worten:

„Regulierte Selbstregulierung steht dabei als Chiffre für verschiedene Regelungsstrukturen, in denen staatliche Steuerung sich auf die mehr oder weniger starke Überformung typischerweise gesellschaftlicher Selbstregulierung beschränkt. Über die schon begrifflich angezeigte Koppelung der verschiedenen Handlungsrationalitäten wird versucht, die Kapazität zur gemeinwohlverträglichen und gemeinwohlförderlichen Problemlösung insgesamt zu erhöhen."[302]

Die mit solchen Instrumenten verbundene Hoffnung liegt darin, einerseits die Innovationskräfte von Unternehmen und Branchen zu utilisieren, um so Ergebnisse und Standards zu erreichen, die von staatlicher Seite so nicht zu erwarten oder vorherzusehen gewesen wären. Andererseits wird erwartet, dass die Freiheiten lassenden Anforderungen eine generelle Steigerung der Normakzeptanz zur Folge haben, weil Normadressaten keine strikten Vorgaben „aufgedrückt" bekommen, sondern Verfahren und Lösungen erarbeiten können, die branchenspezifischen Besonderheiten gerecht werden und als realitätsnäher wahrgenommen werden.[303] Damit können zudem Marktanreize geschaffen und eine stetige Verbesserung des Grundniveaus im jeweiligen Bereich erreicht werden, indem Marktteilnehmer sich etwa mit den von ihnen etablierten Branchenstandards brüsten.[304] Gleichzeitig soll diese den Pflichtigen eingeräumte Freiheit aber durch einen Rest an Kontrolle und Rechenschaft eingezäunt werden, um zu verhindern, dass die gefundenen Verfahren und Ansätze entweder gar nicht den in sie gesetzten Anforderungen entsprechen oder schlicht nur vorgeschoben, aber nicht eingehalten werden. Es entsteht so eine Kombination aus traditionell imperativer Regulierung und freiwilliger Selbstregulierung. Generell kann davon gesprochen werden, dass das mit der regulierten Selbstregulierung verbundene Instrumentarium regelmäßig „dort zum Einsatz kommt, wo die konventionelle Top-down-Steuerung nicht mehr ausreichend Widerhall in der internen Logik der gesellschaftlichen Teilsysteme findet."[305] Dazu passt, dass die Nutzung eines solchen Instrumentariums (meist in Kombination mit anderen, auch klassischen Arten der staatlichen Regulierung) im Bereich der Informationsgesellschaft vielerorts als notwendige Voraussetzung wirksamer Regulierung angesehen wird.[306]

---

[302] *Eifert*, in: Hoffmann-Riem, Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, S. 137 (137).

[303] *Schulz/Held*, Regulierte Selbstregulierung als Form modernen Regierens, S. A-8.

[304] Siehe dazu in Bezug auf das Datenschutzrecht *Hornung/Hartl*, ZD 2014, 219 (219 f.).

[305] *Collin*, JZ 2011, 274 (275).

[306] Siehe hierzu und zu den besonderen Herausforderungen der Informationsgesellschaft *Spindler/Thorun*, MMR-Beilage 2016, 1 (5 ff.).

Das prominenteste Beispiel eines solchen Instruments in der DSGVO sind die Verhaltensregeln in Art. 40.[307] Nach Art. 42 Abs. 1, 2 DSGVO können Wirtschaftsverbände und andere Vertretervereinigungen Verhaltensregeln erarbeiten, die zu einer Präzisierung und Konkretisierung unbestimmter Normen der Verordnung beitragen sollen.[308] Hier stehen ausweislich Erwg. 28 der Verordnung zwei Ziele im Vordergrund: zum einen die Erleichterung einer „wirksamen Anwendung [der] Verordnung" vor dem Hintergrund zahlreicher abstrakter und unbestimmter Regelungen mit oftmals geforderten Abwägungsentscheidungen. Zum anderen ist (in ähnlicher Formulierung auch unmittelbar in Art. 40 Abs. 1 DSGVO) „den Besonderheiten der in bestimmten Sektoren erfolgenden Verarbeitungen und den besonderen Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen Rechnung zu tragen […]." Zielobjekt für solche Verhaltensregeln können dabei grundsätzlich alle Normen der DSGVO sein. Art. 40 Abs. 2 der Verordnung nennt bloß beispielhaft einige Bereiche wie die Fairness und Transparenz von Verarbeitungen, die Möglichkeiten der Pseudonymisierung von personenbezogenen Daten, das Verständnis von berechtigten Interessen des Verantwortlichen oder die Maßnahmen zum Systemdatenschutz in Art. 24 und 25. Wurden solche Verhaltensregeln erarbeitet, können diese gem. Art. 41 Abs. 5 S. 2 DSGVO von den Aufsichtsbehörden genehmigt werden, sofern sie „ausreichend geeignete Garantien" bieten. Verantwortliche können sich diesen Verhaltensregeln dann – freiwillig, oder verpflichtend im Rahmen ihrer Mitgliedschaft in einem Wirtschaftsverband – unterwerfen und ihre Einhaltung gegenüber unabhängigen Überwachungsstellen, die gem. Art. 41 Abs. 1, 2 DSGVO von einer Aufsichtsbehörde akkreditiert werden müssen, beweisen. Die zentrale Folge und der zentrale Anreiz für Verantwortliche liegt darin, dass die Tatsache übernommener und eingehaltener Verhaltensregeln als Indiz für die Einhaltung zahlreicher Verantwortlichenpflichten gilt: Nach Art. 24 Abs. 3 DSGVO können sie bspw. als „Gesichtspunkt" für hinreichende technische und organisatorische Maßnahmen, nach Art. 32 DSGVO als „Faktor" berücksichtigt werden.[309] Für grundsätzlich rechtfertigungsbedürftige Datentransfers in Drittländer außerhalb der EU können vom empfangenden Verantwortlichen umgesetzte Verhaltensregeln gem. Art. 40 Abs. 3 DSGVO gar die benötigte Garantie des angemessenen Datenschutzniveaus darstellen, sofern sie zuvor von der Europäischen Kommission nach Art. 40 Abs. 9 für allgemein gültig erklärt wurden.

---

[307] Für einen Überblick über die verschiedenen co-regulatorischen Instrumente zu Zeiten der DSRL siehe *Hirsch*, Seattle U. L. Rev. 2011, 439 (442 ff.).

[308] Vgl. hierzu *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (327 ff.); *Spindler*, ZD 2016, 407 (407 ff.).

[309] Wie der Wortlaut schon vermuten lässt, besteht hier aber nach hM keine aufsichtsbehördliche Pflicht zur Berücksichtigung, vgl. *Spindler*, ZD 2016, 407 (409 f.).

Auch wenn die Umsetzung solcher Möglichkeiten keine vollumfassende Garantie gegen eigenes Fehlverhalten darstellt, da ihre Einhaltung nur als Indiz für rechtskonformes Verarbeiten berücksichtigt werden soll, bieten sie Verantwortlichen doch ein gutes Maß an Rechtssicherheit und Vertrauen. Durch Umsetzung von Verhaltenspflichten, die von einer Aufsichtsbehörde abgesegnet wurden und deren erfolgreiche Umsetzung bestätigt wurde, können sie sich im entsprechenden Bereich verhältnismäßig sicher sein, datenschutzkonform zu agieren. Durch die Möglichkeit, die Kontrolle durch eine akkreditierte Überwachungsstelle vornehmen zu lassen, lässt sich zudem eine Überprüfung der eigenen Bemühungen vornehmen, ohne unmittelbar Angst vor möglichen Sanktionen zu haben, wie es bei den Aufsichtsbehörden der Fall wäre.

Als Steuerungsinstrument stellen sie und – mit Abstrichen – die Zertifizierungsmaßnahmen aus Art. 42 DSGVO[310] daher grundsätzlich einen gangbaren Weg dar, den Willen der Verantwortlichen zur Normbefolgung zu steigern. Gleichzeitig sorgen sie für erhöhte Transparenz gegenüber Betroffenen und können Anreize für Verantwortliche dahingehend setzen, dass diese ihre Praxiserfahrung und ihr Innovationspotential bei der Erarbeitung neuer Verhaltensregeln in Rahmen ihrer Mitgliedschaft in bspw. Wirtschaftsverbänden aktiv einbringen und ausleben[311] und damit die Aufsichtsbehörden dabei unterstützen, einige der dringend konkretisierungsbedürftigen Vorgaben der DSGVO mit Leben zu füllen.[312]

d) Regulierung zur prozeduralen Steigerung von Handlungswissen

Einige der Instrumente der DSGVO sind zudem im Vergleich zu den anderen Instrumenten zeitlich und denklogisch etwas vorgelagert und dienen dem Zweck, das nötige Handlungswissen und die nötige Reflektionsfähigkeit zur Erfüllung dieser beim Verantwortlichen dauerhaft sicherzustellen.[313] Darunter verstanden wird also jede Art der (staatlichen oder privaten) Regulierung, die ihrerseits eine komplementäre Regulierungsform (mit)reguliert.[314] Besonders im Fokus

---

[310] Vgl. *Scholz*, in: Simitis u. a., DSGVO/BDSG, Art. 42 DSGVO Rn. 4, wonach auch diese Norm einen Teil desjenigen Bereichs des Datenschutzes darstellt, der „mit den und nicht gegen die für die Datenverarbeitung Verantwortlichen betrieben wird". Ausführlich zur Bedeutung der Zertifizierung unter der DSGVO *Hofmann*, Dynamische Zertifizierung, S. 162 ff.

[311] Vgl. *Spindler/Thorun*, MMR-Beilage 2016, 1 (8).

[312] Die damit verbundene Erwartung beschreibt *Köndgen*, AcP 2006, 477 (512) zutreffend: „In einer Welt dezentralisierten Wissens und dezentralisierter Diskurse erhöht das Rechtssystem durch die Zulassung privatisierten Rechts sein gesellschaftliches Wissen und seine Lernfähigkeit."

[313] Vgl. *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (21) in Bezug auf die DSFA: „Man setzt insoweit also bis zu einem gewissen Grad darauf, dass schon durch die inhaltliche Befassung mit den Datenschutzfragen im Rahmen der Folgenabschätzung ein Problembewusstsein geschaffen wird, das die Rechtskonformität sichert […]."

[314] Vgl. *Parker*, in: McBarnet/Voiculescu/Campbell, The new corporate accountability:

stehen bei der wissenschaftlichen Betrachtung die Fälle, in denen derartige Regulierungsinstrumente eingesetzt werden, um Einfluss auf unternehmensinterne Selbstregulierungsprozesse zu nehmen. Dabei wurden (rechtliche Pflichten zur Durchführung von) Folgenabschätzungen bereits früh als grundlegendes Beispiel solcher (zuweilen als „Meta-Regulierung" bezeichneter)[315] Instrumente genannt und beleuchtet. Durch sie, so die Überlegung, könnten Unternehmen (oder genereller: alle Normunterworfenen) dafür verantwortlich gemacht werden, ein funktionierendes und auf das Regulierungsziel ausgerichtetes System an internen Regulierungs- und Governanceprozessen einzuführen. Ähnlich wie im Falle der regulierten Selbstregulierung sollten die Normunterworfenen dabei nicht zu konkreten Maßnahmen verpflichtet werden, sondern ein gewisses Maß an Freiheit und Gestaltungsmöglichkeit genießen, um ihre Praxisnähe sowie Kompetenzen und Kreativität möglichst effizient und in regulatorisch gelenkten Bahnen einzubringen.[316] Gleichzeitig setzt ein solches Regulierungssystem Feedbackschleifen und Pflichten zur Weitergabe und Veröffentlichung von Informationen voraus, die eine Kontrolle (durch staatliche Stellen oder andere Stakeholder) ermöglichen. Hinzu kommt die Einbettung dieser Form von Regulierung in ein Gesamtkonzept mit weiteren Regulierungsregimen (wie etwa der klassisch staatlichen Regulierung und der – regulierten oder klassischen – Selbstregulierung), um insgesamt die wirksame Regulierung eines Realweltausschnitts zu gewährleisten.

Innerhalb der DSGVO kann das Regime um die Datenschutzfolgenabschätzung in Art. 35 als Instrument eines solchen Regulierungssystems betrachtet werden. Es verpflichtet Verantwortliche dazu, eigenständig, flexibel[317] und präventiv die mit ihren geplanten Verarbeitungen und Verarbeitungsumgebungen einhergehenden Risiken ein- und abzuschätzen und taugliche Gegenmaßnahmen zu entwickeln und implementieren, bevor die infragestehenden Verarbeitungen eingeführt werden. Voraussetzung dafür ist gem. Abs. 1 S. 1 der Norm ein voraussichtlich hohes Risiko für Betroffene durch die infragestehende Verarbeitung.

Die Durchführung setzt ein systematisches Verständnis und einen vollständigen Überblick über die eigenen internen Prozesse und Systemarchitekturen voraus,[318] ist doch der erste Schritt der eigentlichen Folgenabschätzung gem.

---

corporate social responsibility and the law, S. 207 (211): „[…] can also entail any form of regulation (whether by tools of state law or other mechanisms) that regulates any other form of regulation."

315 *Binns*, International Data Privacy Law 2017, 22.

316 Vgl. *Binns*, International Data Privacy Law 2017, 22 (31): „[…] leverag[ing] regulatees' ability to learn and discover effective measures to achieve regulatory goals."

317 *Art. 29-Datenschutzgruppe*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, S. 17 […] „flexibility to determine the precise structure and form of the DPIA […]."

318 Zur Frage, wie technische Tools Verantwortliche bei der Modellierung interner Datenflüsse, aber auch bei der Überprüfung der Einhaltung von DSGVO-Pflichten unterstützen kön-

Art. 35 Abs. 7 lit. a DSGVO die systematische Beschreibung dieser. In der Überprüfungs- und Bewertungsphase gilt es, sowohl gem. Abs. 7 lit. b auf normativer Ebene die Rechtmäßigkeit der Verarbeitung, also die Einhaltung der weiteren materiellen Pflichten der DSGVO, zu überprüfen, als auch auf faktischer und technischer Ebene Risiken in Form von konkreten Gefahrenszenarien durchzuspielen und zu bewerten. Normativ muss der Verantwortliche insbesondere noch einmal überprüfen und sodann dokumentieren, ob bzw. dass die konkrete Verarbeitung, aber auch jeder ihrer einzelnen Ausgestaltungsaspekte[319], für den konkret gewählten Zweck notwendig und verhältnismäßig ist.[320] Auf Ebene der Risiken sind primär solche im Zusammenhang mit der Datensicherheit, etwa durch – externe oder interne – Angreifer in den Blick zu nehmen und Szenarien anhand von möglichen Angriffsmotiven und -zielen durchzuspielen.[321] Nach Bewertung der jeweiligen Risiken[322] sind darauf abgestimmt gem. Abs. 7 lit. d der Norm Maßnahmen zu konzipieren und implementieren und ist das verbleibende Restrisiko zu ermitteln, das hinreichend geringgehalten sein muss, um zum Ergebnis der Durchführbarkeit der beabsichtigten Verarbeitung zu kommen.[323]

Die Datenschutzfolgenabschätzung als regulatorisches Instrument liegt somit quer über allen weiteren Verantwortlichenpflichten[324] und sichert deren Einhaltung durch den Verantwortlichen dadurch ab, dass dieser – wie beschrieben bereits *im Vorfeld*[325] einer beabsichtigten Verarbeitung – dazu gezwungen wird, sich der Rechtmäßigkeit der Verarbeitung sowie der Identifizierung und Minimierung weiterer Risiken für den Betroffenen zu vergewissern. Sie schafft damit eine zusätzliche Reflektionsschleife, durch die der Verantwortliche für einen Moment dazu gebracht wird, innezuhalten und die Perspektive eines Außenstehenden einzunehmen und seine Verarbeitungspläne sowie insgesamt

---

nen, siehe *Schulz* u. a., in: Leenes/Hallinan/Gutwirth/de Hert, Data protection and privacy: data protection and democracy, S. 145 (145 ff.).

[319] Vgl. *Jandt*, DuD 2017, 562 (565).

[320] Vgl. *Jandt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 35 DSGVO Rn. 39 ff.

[321] Vgl. *Jandt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 35 DSGVO Rn. 45.

[322] Zur Frage der Operationalisierbarkeit und Kalkulierbarkeit von Risikohöhen siehe *Karg*, in: Simitis u. a., DSGVO/BDSG, Art. 35 DSGVO Rn. 24 ff. *Bieker/Bremert*, ZD 2020, 7 (12 ff.); *Krings/Ohrtmann*, DSB 2019, 193 (195) m. w. N. zu u. a. Empfehlungen verschiedener Aufsichtsbehörden; *Ritter* u. a., ZD 2019, 531 (531 ff.).

[323] Vgl. *Karg*, in: Simitis u. a., DSGVO/BDSG, Art. 35 DSGVO Rn. 11: „[…] nicht allein eine Risikomanagementaufgabe, sondern eine Risikominimierungsverpflichtung."

[324] Besonders hervorzuheben ist hier die Verbindung zu Art. 24, 25 und 32 sowie den Grundprinzipien in Art. 5 DSGVO. Vgl. *Karg*, in: Simitis u. a., DSGVO/BDSG, Art. 35 DSGVO Rn. 62, der von einer „engen normativen Verflechtung" zu Art. 25 spricht.

[325] Vgl. *Art. 29-Datenschutzgruppe*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, S. 14, wonach die Entscheidung für oder gegen den endgültigen Einsatz der Verarbeitung(en) noch nicht gefallen sein darf: „[…] seen as a tool for helping decision-making concerning the processing."

seine verarbeitungsrelevante Architektur und Prozesse mit Blick auf die Rechte und Interessen des Betroffenen[326] zu betrachten und zu bewerten.[327]

Bei Feststellung eines hohen Risikos und gleichzeitiger Abwesenheit von Sicherheitsvorkehrungen und Gegenmaßnahmen[328] muss das Gesamtergebnis der Abschätzung inklusive aller wichtigen Details gem. Art. 36 Abs. 1 DSGVO der zuständigen Aufsichtsbehörde zur Konsultation vorgelegt werden. Ein gewisses, wenn auch eingeschränktes, Maß an externer Kontrolle ist damit, zumindest in der Theorie, gegeben. Eine Pflicht zur Konsultation in Fällen mit hohem Risiko auch dann, wenn der Verantwortliche Gegenmaßnahmen avisiert hat, fehlt aber[329] ebenso wie die in anderen Rechtsgebieten gängige Veröffentlichung von Folgenabschätzungsergebnissen[330]. Auch die Einsicht und Kontrolle durch weitere Stakeholder fällt eher restriktiv aus und beschränkt sich auf Abs. 9 der Norm, nach welchem bei der Durchführung einer Datenschutzfolgenabschätzung die Standpunkte von Betroffenen nur *gegebenenfalls* und unter Berücksichtigung *gewerblicher und öffentlicher Geheimhaltungsinteressen* eingeholt werden sollen – genauere Voraussetzungen für die Notwendigkeit einer Einholung fehlen genauso wie eine Pflicht zur inhaltlichen Auseinandersetzung mit mitgeteilten Standpunkten.[331]

e) Instrumente zur Rechtsdurchsetzung – die Besonderheit des Rechtsgebietsdualismus

Einen weiteren Beitrag zur Verhaltenslenkung der Verantwortlichen als Normadressaten der DSGVO leisten die Instrumente, die sich der Rechtsdurchsetzung

---

[326] Vgl. *Art. 29-Datenschutzgruppe*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, S. 17.

[327] Dass *Karg*, in: Simitis u. a., DSGVO/BDSG, Art. 35 DSGVO Rn. 10 f. das entstehende Bewusstsein hinsichtlich der Verarbeitungsfolgen für Betroffene, und nicht die Selbstreflektion des Verantwortlichen, als primären Zweck der Norm ausmacht, widerspricht diesem Verständnis nur scheinbar. Denn auch wenn das Bewusstsein für Risiken primäres Ziel ist, ist die Selbstreflektion die Art und Weise, wie die Norm dieses zu erreichen versucht.

[328] Dies kann der Fall sein, wenn schlicht keine tauglichen Maßnahmen verfügbar sind, aber auch dann, wenn der Verantwortliche den notwendigen Aufwand bspw. als unzumutbar und unverhältnismäßig empfindet. Vgl. *Jandt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 36 DSGVO Rn. 5.

[329] A. A. aber *Karg*, in: Simitis u. a., DSGVO/BDSG, Art. 35 DSGVO Rn. 19 ff., nach dem eine Pflicht immer dann besteht, wenn der Verantwortliche nach eigener Einschätzung das Risiko nicht auf das geforderte Niveau reduzieren kann.

[330] Vgl. § 19 Abs. 2 UVPG.

[331] Vgl. *Jandt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 35 DSGVO Rn. 56 ff.; nach dem Verständnis der *Art. 29-Datenschutzgruppe*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, S. 15 sollten Entscheidungen, die von der Stellungnahme der befragten Verantwortlichen abweichen, jedoch begründet und dokumentiert werden.

widmen. Ihre Qualität, ihre Reichweite, aber auch die Ausgestaltung der Berechtigungen derer, die sich ihrer bedienen dürfen, haben Einfluss auf die Wahrscheinlichkeit einer Sanktionierung von Fehlverhalten der Verantwortlichen und damit auf die Wahrscheinlichkeit ihrer Bereitschaft zur Normbefolgung. Hier lässt sich ein weiterer Sonderweg des Datenschutzrechts erkennen, der konsequent die mit dem Selbstdatenschutz verfolgte Nutzbarmachung des Betroffenen fortsetzt: ein Dualismus der Rechtsdurchsetzungsregime hinsichtlich ihrer Rechtsgebiete, ein „doppeltes Netz“[332] zur Absicherung der Rechtsdurchsetzung.[333] Neben der klassisch verwaltungsrechtlichen Rechtsdurchsetzung durch Aufsichtsbehörden steht Betroffenen sowie unter anderem Verbraucherverbänden und Mitbewerbern von Verantwortlichen auch der Zivilrechtsweg offen.[334] Verklammert werden diese beiden parallellaufenden Stränge zudem dadurch, dass Betroffene und sie vertretende Verbände die Möglichkeit haben, gem. Art. 77 Abs. 1 (ggf. i. V. m. Art. 80 Abs. 1 und 2 sowie nationalem Recht) DSGVO Beschwerde bei der zuständigen Aufsichtsbehörde wegen einer behaupteten rechtswidrigen Datenverarbeitung einzulegen und diese so zum Tätigwerden zu animieren.

Mit dieser ersten Erkenntnis über den Dualismus der Rechtsdurchsetzungsregime der DSGVO geht eine zweite einher: Auch die Verantwortlichenpflichten selbst sind teilweise – also zumindest insoweit, wie ihre Verletzung sowohl durch Aufsichtsbehörden als auch durch nichthoheitsrechtliche Akteure wie Betroffene geltend gemacht werden kann – nicht nur öffentlich-rechtlicher, sondern auch privatrechtlicher Natur. Mit *Wehr* sind öffentlich-rechtliche Pflichten nämlich nur solche, „die innerhalb eines Rechtsverhältnisses bestehen, an denen ein Träger öffentlicher Gewalt notwendig beteiligt ist“[335]. Entscheidend abzustellen ist ihm zufolge bei der Bestimmung, wer die sog. Normverwirklichungskompetenz aufweist, wen die Rechtsordnung also dazu ermächtigt, für die Erfüllung der Pflicht durch den Verpflichteten zu sorgen.[336] Dass dies im Rahmen einer einzelnen Pflichtennorm wahlweise ein Träger hoheitlicher Pflichten oder ein Privater sein kann, führt dabei zu keinem Widerspruch, son-

[332] *Schwichtenberg*, PinG 2017, 104 (106) hinsichtlich des Verhältnisses zwischen Aufsichtsbehörden und Verbraucherverbänden.

[333] Einmalig ist dieser Sonderweg freilich nicht. Einen guten rechtsgeschichtlichen Überblick liefert *Masing*, Die Mobilisierung des Bürgers für die Durchsetzung des Rechts, S. 62 ff. Mit Blick auf das Unionsrecht zudem *Schmid*, Die Instrumentalisierung des Privatrechts durch die Europäische Union; grundlegend und teils krit. zum Verhältnis zwischen privater und administrativer Rechtsdurchsetzung *Schröder*, Die Verwaltung 2017, 309 (309 ff.).

[334] Siehe auch *Thon*, RabelsZ 2020, 24 (27): „Datenschutz steht im Spannungsfeld von staatlicher und privater (Selbst-)Regulierung, von staatlicher und privater Rechtsdurchsetzung.“ Ein vergleichbarer Dualismus der Rechtsdurchsetzung findet sich etwa im Kartellrecht. Vgl. *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (17).

[335] *Wehr*, Rechtspflichten im Verfassungsstaat, S. 159.

[336] *Wehr*, Rechtspflichten im Verfassungsstaat, S. 160.

dern vielmehr zu der Einordnung der betreffenden Norm als sowohl öffentlich-rechtlich wie privatrechtlich.[337]

So gestaltet es sich auch bei der datenschutzrechtlichen Verantwortlichkeit, wie im Folgenden gezeigt werden soll. Die aus ihr resultierenden Pflichten können einerseits allesamt durch die mit Hoheitsbefugnissen ausgestatteten Aufsichtsbehörden überwacht und Verstöße durch diese geahndet werden – manche Pflichten müssen sogar explizit diesen gegenüber erbracht bzw. erfüllt werden (aa.)[338]. Gleichzeitig eröffnet die DSGVO gerade auch den Betroffenen, bestimmten Verbänden sowie Mitbewerbern die Möglichkeit der eigenständigen Geltendmachung etwaiger Verstöße gegen einige der Pflichten in Form von unter anderem Schadensersatzansprüchen (bb.).[339]

aa) Verwaltungsrechtliche Rechtsdurchsetzung

Auf der einen Seite steht der klassisch verwaltungsrechtliche Weg der Rechtsdurchsetzung. Gem. Art. 57 Abs. 1 lit. a. DSGVO kommt die Aufgabe, die Umsetzung der datenschutzrechtlichen Vorschriften zu überwachen und durchzusetzen, *primär* den Aufsichtsbehörden zu. Auch hier lässt sich ein zweigeteilter Weg feststellen. Die Aufsichtsbehörden haben einerseits die Möglichkeit, mittels Bußgeldern (deren Rahmen im Vergleich zur Rechtslage unter der DSRL teils drastisch erhöht wurde), Untersagungsverfügungen und ähnlichen Maßnahmen zu sanktionieren und damit existierende datenschutzrechtswidrige Verhaltensweisen zu unterbinden und, idealerweise, betroffene Verantwortliche zukünftig von der Wiederholung und potenziell betroffene Verantwortliche generell von der Ausübung der sanktionierten Praktiken abzuschrecken und abzuhalten. Gleichzeitig bietet sich ihnen der kooperativere Weg, gewillte Verantwortliche bei ihren Compliance-Bemühungen zu beraten und unterstützen und konkrete Verwendungen und Verhaltensweisen zu genehmigen sowie breitflächig Branchen und Verantwortliche für Risiken zu sensibilisieren;[340] teilweise

---

[337] *Wehr*, Rechtspflichten im Verfassungsstaat, S. 161, 164; gleichzeitig ist die Bedeutung der Unterscheidung zwischen privatem und öffentlichem Recht auf unionsrechtlicher Ebene ungleich geringer als im nationalen Recht. Vgl. *Jarass*, ZEuP 2017, 310 (313 ff.).

[338] So zum Beispiel die vorherige Konsultation im Rahmen einer Datenschutzfolgenabschätzung nach Art. 36 Abs. 1 DSGVO.

[339] Dass auch Privatrecht regulierende Wirkung haben kann und zu diesem Zweck eingesetzt wird, ist gemeinhin anerkannt, vgl. *Jansen/Michaels*, RabelsZ 2007, 345 (355 ff.). Den entsprechenden Einsatz von Privatrecht zu diesem Zweck befürwortend *Hellgardt*, Regulierung und Privatrecht, S. 7 ff.; ebenfalls eher positiv *Lurger*, ZEuP 2018, 788 (796 f.); einen guten Überblick über Für und Wider von Privatrecht als Regulierungsinstrument liefert *Schweitzer*, AcP 2020, 544 (549 ff.); Parallelen zu dieser Betrachtungsweise finden sich zudem bereits bei *Hoffmann-Riem*, in: Hoffmann-Riem/Schmidt-Aßmann, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, S. 261 (261 ff.).

[340] Die Janusköpfigkeit einer solchen Behörde, die mangels funktionaler Trennung gewissermaßen gleichzeitig „good cop“ und „bad cop“ spielt, kann dabei mit Blick auf das für eine wirksame Beratungstätigkeit notwendige Vertrauen der Normunterworfenen durchaus kritisch

fordert die DSGVO diese kooperative Zusammenarbeit sogar explizit von den Aufsichtsbehörden.[341]

Der Aufbau von Art. 58 DSGVO, der die Befugnisse der Aufsichtsbehörden normiert, unterteilt diese in solche, die auf Untersuchung (Abs. 1), Abhilfe (Abs. 2) und Genehmigung bzw. Beratung (Abs. 3) gerichtet sind. Grundsätzlich tragen all die dort genannten Maßnahmen letzten Endes zur Durchsetzung der DSGVO bei, doch stehen naturgemäß die unter den Abhilfebefugnissen gefassten Sanktionen mit ihrer Abschreckungs- und teilweise Prangerwirkung[342] sowie Beratungsbefugnisse mit ihrer erhofften Kooperationswirkung im Vordergrund.

Im Folgenden sollen einige der wichtigsten Befugnisse näher beleuchtet werden.

(1) Bußgelder und andere Sanktionen

Das schärfste Schwert, das den Aufsichtsbehörden zur Verfügung steht, ist sicherlich die Möglichkeit der Verhängung von Bußgeldern nach Art. 58 Abs. 2 lit. i DSGVO. Im Vergleich zur Rechtslage unter der DSRL wurde nicht nur der Bußgeldrahmen merklich angehoben,[343] durch die einheitliche und im Vergleich zur DSRL stark konkretisierte Normierung der Voraussetzungen für Bußgelderteilungen in Art. 83 DSGVO sollte zudem eine unionsweite Harmonisierung der Bußgeldpraxis erreicht werden.[344] Der generalpräventive Charakter dieses Sanktionsinstruments wird bereits anhand des Wortlauts in Abs. 1 (und ebenso den Erwägungsgründen 148 und 152) deutlich, der die Verhängung eines Bußgeldbetrags fordert, der „wirksam, verhältnismäßig und abschreckend" ist.[345] Insbesondere das Merkmal der Verhältnismäßigkeit darf hier nicht mit dem deutschen Verhältnismäßigkeitsgrundsatz verwechselt werden und stellt –

gesehen werden, vgl. *Wolff*, PinG 2017, 109 (110). *Brink*, ZD 2020, 59 (60) betont deshalb die Notwendigkeit für stetige Transparenz der Behörde bzgl. der Funktion, in der sie jeweils agiert.

[341] Ausführlich zu dieser gewandelten Rolle der Aufsichtsbehörden *Roßnagel*, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, S. 42 ff.

[342] Zur Zulässigkeit der Veröffentlichung von Bußgeld-Adressaten siehe *Kropp*, PinG 2019, 220 (222 ff.).

[343] Über die Höchstgrenze von bis zu 4 % des gesamt weltweit erzielten Jahresumsatzes bzw. 20 Mio. Euro wurde ausgiebig diskutiert und geschrieben. Siehe etwa *Nolde*, PinG 2017, 114 (116); *Schönefeld/Thomé*, PinG 2017, 126 (127); *Faust* u. a., ZD 2016, 120.

[344] Vgl. *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 83 DSGVO Rn. 1, 6; einen Überblick über die weitgehende Freiheit der Mitgliedstaaten unter der DSRL liefert *Weiß*, PinG 2017, 97 (97).

[345] Vgl. *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 83 Rn. 19ff; *Holländer*, in: Beck-OK Datenschutzrecht, Art. 83 DSGVO Rn. 2; *Kotschy*, in: Kuner u. a., GDPR, S. 1184 spricht von „a ‚deterrent' effect, by creating a credible threat of being investigated and fined, which changes the perceived balance of the expected benefits and expected costs of non-compliance sufficiently to encourage controllers to choose in favour of compliance."

etwas kontraintuitiv – primär eine Untergrenze dar, die dann unterschritten ist, wenn ein Bußgeld im Verhältnis zu den betroffenen Interessen der EU zu gering ausfällt.[346] Gleichwohl muss die ein Bußgeld aussprechende Aufsichtsbehörde nach Maßgabe deutschen Verwaltungsrechts die (klassische) Verhältnismäßig beachten.[347] Die Abs. 4–6 der Norm regeln, welche Verstöße eine Bußgeldsanktionierung rechtfertigen. Dabei zählen Abs. 4 und 5 enumerativ Pflichten auf, deren Verletzung durch einen Verantwortlichen (oder Auftragsverarbeiter) sanktionierbar ist und unterscheiden sich hinsichtlich der maximalen Bußgeldhöhe. Abs. 6 stellt klar, dass auch die Nichtbefolgung von Anweisungen der Aufsichtsbehörden ein sanktionierbares Handeln darstellt.

Abs. 2 S. 2 der Norm zählt die Kriterien auf, die bei der Entscheidung über die Verhängung und die Höhe eines Bußgelds von den Aufsichtsbehörden zu berücksichtigen sind. Von diesen ist zuvorderst die Frage nach Vorsätzlichkeit oder Fahrlässigkeit bzgl. der relevanten Pflichtverletzung von Bedeutung. Nach der Ansicht eines Teils der Literatur[348] ist darin eine Verschuldensabhängigkeit des Instruments zu sehen – wo der Verantwortliche oder Auftragsverarbeiter die infragestehende Pflicht weder fahrlässig noch vorsätzlich verletzt hat, darf ein Bußgeld demnach mit Blick auf dessen strafähnlichen Charakter nicht ausgesprochen werden. Dem halten andere Stimmen, teils mit Verweis auf die zumindest europarechtlich betrachtete Irrelevanz des deutschen Schuldprinzips,[349] teils gestützt auf die Entstehungsgeschichte[350] oder schlicht den Wortlaut[351] der Norm, die Ansicht entgegen, etwaiges Verschulden sei einzig und allein für die Bemessung eines auszusprechenden Bußgeldes relevant. Während die letztgenannten Argumente überzeugender scheinen, dürfte eine endgültige Entscheidung aus zwei Gründen von geringer (Praxis-)Relevanz bleiben: Einerseits dürfte zumindest ein Organisationsverschulden in Zweifelsfällen meist

[346] Vgl. *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 83 DSGVO Rn. 21. siehe auch m. w. N. *Neun/Lubitzsch*, BB 2017, 1538 (1541).

[347] Zum Einklang dieser beiden konträr wirkenden Zielrichtungen siehe LG Bonn, Urt. v. 11.11.2020, Az. 29 OWi1/20, BeckRS 2020, 35663, Rn. 69: „Die Geldbuße muss spürbar sein; sie darf jedoch nicht als unangemessene Härte im Sinne einer überzogenen Reaktion auf den konkreten Verstoß erscheinen." Hierbei besteht aber nur eingeschränktes, durch die Rechtsgrundsätze des Unionsrechts prädeterminiertes, Ermessen. Vgl. Nemitz, in: *Ehmann/Selmayr*, Datenschutz-Grundverordnung, Art. 83 Rn. 9.

[348] Siehe etwa *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 83 DSGVO Rn. 8; *Holländer*, in: BeckOK Datenschutzrecht, Art. 83 DSGVO Rn. 18; *Popp*, in: Sydow, DSGVO, Art. 83 Rn. 13.

[349] Vgl. *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 73 DSGVO Rn. 26; auch *Bülte*, StV 2017, 460 (460) spricht insofern von originär unionsrechtlichem Sanktionsrecht. Gleichwohl wird anerkannt, dass hier eine verfassungsrechtliche Problematik hinsichtlich der Integrationsfestigkeit des deutschen Schuldprinzips aufgeworfen wird, vgl. *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 83 DSGVO Rn. 36. Dazu auch *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 83 DSGVO Rn. 14.

[350] *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 83 Rn. 10, 35.

[351] Ebenfalls *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 83 DSGVO Rn. 35.

festzustellen sein,[352] andererseits kennt die Norm ausreichend zusätzliche Kriterien, die bei der Festlegung der Höhe zu berücksichtigen sind und sich, im Falle einer tatsächlich einmal fehlenden Schuld des betroffenen Verantwortlichen, bis hin zur oben beschriebenen Untergrenze der Verhältnismäßigkeit mildernd auswirken können. Konkret zu berücksichtigen sind dabei etwa Art, Schwere und Dauer des jeweiligen Verstoßes, aber auch die unternommenen Anstrengungen im Vorfeld der Pflichtverletzung (bspw. die Existenz und Tauglichkeit der implementierten organisatorischen und technischen Maßnahmen gem. Art. 25 und 32, die etwaige Einhaltung von genehmigten Verhaltensregeln und Zertifizierungsverfahren gem. Art. 40 und 42 DSGVO, oder die Existenz früherer Verstöße) und im Anschluss an diese (bspw. die zugunsten des bzw. der Betroffenen getroffenen Maßnahmen zur Schadensminimierung sowie der Wille zur Kooperation mit der zuständigen Aufsichtsbehörde).

Seinem generalpräventiven und verhaltenssteuernden Charakter kommt das Bußgeld gerade auch durch diese differenzierte Ausgestaltung zumindest auf dem Papier nach: Wo eine starre Vorschrift in Verbindung mit den, wie bereits mehrfach beschrieben, abstrakten und nicht immer klar konturierten Pflichten der DSGVO Verantwortliche eher von Compliance-Bemühungen abschrecken könnte – aus Angst, am Ende doch mit harschen Sanktionen belegt zu werden, weil die Bemühungen sich nachträglich als nicht ausreichend herausstellten –, sorgt der Kriterienkatalog des Art. 83 Abs. 2 DSGVO dafür, dass sie die Behördenpflicht zur Berücksichtigung ihrer Bemühungen schwarz auf weiß im Gesetz stehen sehen. Auch die Tatsache, dass – etwa bei besonders geringfügigen Verstößen – gänzlich auf ein Bußgeld verzichtet und stattdessen eine mildere Maßnahme wie bspw. eine Verwarnung gem. Art. 58 Abs. 2 lit. b DSGVO ausgesprochen werden kann,[353] sowie die noch zu behandelnde Behördenaufgabe zur Kooperation mit und Unterstützung von Verantwortlichen, sollen Verantwortliche davon überzeugen, dass jegliche investierten Bemühungen berücksichtigt werden. Nichtsdestotrotz obliegt es letztlich den jeweiligen Aufsichtsbehörden, dieses theoretische Konzept in die Praxis zu übertragen.[354] Hier offenbaren sich teils größere Unklarheiten und Unbestimmtheiten für bemühte Verantwortliche, wie zuletzt die breite Kritik an dem Bußgeldkonzept der DSK[355] zeigte.[356]

---

[352] So auch *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 83 DSGVO Rn. 37; auch *Frenzel* in: Paal/Pauly, DSGVO/BDSG, Art. 83 Rn. 14 kann dies nicht leugnen, verweist aber auf den weiterhin bestehenden Konflikt mit dem deutschen Schuldprinzip.

[353] So jedenfalls die wohl herrschende Meinung, die die Geltung des Opportunitätsprinzips, also ein Entschließungsermessen der Behörden, auch hinsichtlich des „Ob" einer Geldbuße, bejahen. Vgl. *Neun/Lubitzsch*, BB 2017, 1538 (1542).

[354] Siehe *Golla*, jipitec 2017, 70 (77) für eine Bestandsaufnahme der Instrumente, mittels derer die DSGVO die bestehenden Defizite zu beheben versucht.

[355] Ein Gremium quasi-institutionellen Charakters, das sich aus dem Bundesdatenschutzbeauftragten und den einzelnen Landesdatenschutzbeauftragten zusammensetzt.

[356] Hierzu ausführlich *Timner* u. a., CR 2019, 782 (783 ff.).

Hinzu kommt die chronische Unterausstattung der meisten Aufsichtsbehörden, aus der sich eine eher geringe Sanktionswahrscheinlichkeit ergibt und die einem „credible thread of being investigated and fined“[357] entgegensteht.

Für insbesondere schwere Verstöße nicht Compliance-bemühter Verantwortlicher erlaubt Art. 84 Abs. 1 S. 1 DSGVO die Normierung weitergehender Sanktionen. Dies betrifft einerseits genuin strafrechtliche Sanktionen, andererseits weitere administrative Sanktionen, die nicht durch die DSGVO harmonisiert wurden, etwa für besonders schwere Verstöße. In Deutschland wurden auf Basis dieser Öffnungsklausel die Strafvorschriften der §§ 42, 43 BDSG nF eingeführt.[358]

(2) Verarbeitungsbeschränkungen und andere Abhilfemaßnahmen

Die bereits angeführte Einbettung der Bußgeldbefugnis in Art. 58 Abs. 2 S. 1 DSGVO sowie der Verweis in Art. 83 Abs. 2 S. 1 DSGVO auf die dortigen Maßnahmen täuscht insofern, als der Großteil der dortigen Maßnahmen keine Sanktionen im engeren Sinne darstellen – bei ihnen steht die Wiederherstellung datenschutzkonformer Zustände im Vordergrund, während eine Abschreckungswirkung maximal als geringer Nebeneffekt angesehen werden kann.[359] Die Bezeichnung als Abhilfemaßnahmen, wie in Art. 58 DSGVO selbst gewählt, ist daher treffender.[360] Anders als bei der Bußgeldsanktionierung ist hier unstrittig, dass keine der Abhilfemaßnahmen ein Verschulden des Verantwortlichen voraussetzen.

Exemplarisch für eine solche Maßnahme mit weniger stark generalpräventiver, dafür aber umso stärkerer Einzelfallwirkung, steht die Verarbeitungsbeschränkung. Sieht die Aufsichtsbehörde keine andere Möglichkeit, einen datenschutzkonformen Zustand (wieder)herzustellen – etwa, weil der Verantwortliche sich gänzlich unkooperativ zeigt oder weil die beanstandete Verarbeitung durch ihn oder jedermann faktisch nicht rechtskonform gestaltet werden kann –,[361] kann sie nach Art. 58 Abs. 2 lit. f DSGVO in verschiedenen Abstufungen ein gänzliches Verbot oder eine andere (zeitliche, räumliche, quantitative oder qualitative) Beschränkung der Verarbeitung verlangen und durchsetzen. Diese Maßnahme stellt die *ultima ratio* unter den „echten“ Abhilfemaßnah-

[357] *Kuner*, in: Kuner u. a., GDPR, S. 1184.

[358] Siehe zur Erläuterung dieser und für eine Übersicht weiterer sonstiger Sanktionsmöglichkeiten im deutschen Recht *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 84 DSGVO Rn. 15 ff. Ausführlich zu den Straftatbeständen des BDSG aF *Golla*, Die Straf- und Bußgeldtatbestände der Datenschutzgesetze als Teil des Schutzes des informationellen Selbstbestimmungsrechts.

[359] Vgl. *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 83 DSGVO Rn. 8; *Neun/Lubitzsch*, BB 2017, 1538 (1539).

[360] A. A. aber jedenfalls zur Verwarnung *Martini/Wenzel*, PinG 2017, 92 (96), die hier von einem „hybriden Sanktionsinstrument“ sprechen.

[361] Vgl. *Polenz*, in: Simitis u. a., DSGVO/BDSG, Art. 58 DSGVO Rn. 40.

men dar und ist deshalb nur verhältnismäßig, wenn keine der anderen, milderen Maßnahmen in Art. 58 ebenso geeignet zur Beendigung der rechtswidrigen Lage ist; gleiches gilt für das Verbot als *ultima ratio* unter den verschiedenen Beschränkungsmaßnahmen.[362]

Das Instrumentarium dieser milderen Abhilfemaßnahmen umfasst unter anderem die Warnung und die Verwarnung als Appelle an die Compliance-Bemühungen des Verantwortlichen. Während die Warnung bei einem vermuteten oder bevorstehenden, aber noch nicht (sicher festgestellt) eingetretenen Datenschutzverstoß ausgesprochen wird,[363] setzt die Verwarnung bereits einen ermittelten Verstoß voraus.[364] Beiden gemein ist, dass ihre Aussprache keine Rechtspflicht zur Behebung der betreffenden Verstöße nach sich zieht, also nur den Status einer „gelben Karte"[365] innehat und den Verantwortlichen dazu bewegen soll, noch rechtzeitig die goldene Brücke zurück zur Datenschutzkonformität zu beschreiten.[366] Dabei soll insbesondere die Verwarnung eine niedrigschwellige Alternative zur oben behandelten Geldbuße darstellen.[367] Ihre Missachtung kann sodann gem. Art. 83 Abs. 2 lit. f DSGVO als Kriterium zur Bemessung einer etwaigen späteren Geldbuße herangezogen werden.

Neben diesen beiden Maßnahmen kennt der Katalog in Art. 58 DSGVO eine Vielzahl weiterer Befugnisse in Form von insbesondere Anweisungen, die hier aber nicht näher beleuchtet werden sollen.[368]

Wenngleich die beschriebenen Abhilfemaßnahmen für sich genommen also nur eine begrenzte Wirkung als generalpräventives Steuerungsinstrument aufweisen, können sie als Hybrid zwischen den im nächsten Abschnitt zu beleuchtenden Beratungsmaßnahmen und den oben behandelten „echten" Sanktionen Verantwortliche im Idealfall zum Umdenken und Handeln bewegen, bevor ein Verstoß eintritt oder ein bereits eingetretener Verstoß zu schwerwiegenderen Schäden führt. Zudem können sie in ihrer Gesamtheit und kann ihre reine Existenz, wie im letzten Abschnitt beschrieben, dazu beitragen, dass Verantwortliche Vertrauen in den Eigenwert von Compliance-Bemühungen und -anstrengungen bilden, selbst wenn diese sich im Nachhinein als unzureichend herausstellen sollten. Entscheidend dafür ist jedoch einmal mehr die praktische Handhabung der Maßnahmen durch die Aufsichtsbehörden. Da die DSGVO ein ergebnisloses Ausschöpfen der Abhilfemaßnahmen als Voraussetzung für die Erteilung einer Geldbuße nicht verlangt und Abhilfemaßnahme und Sanktionen

362 Vgl. *Polenz*, in: Simitis u. a., DSGVO/BDSG, Art. 58 DSGVO Rn. 40.
363 Vgl. *Martini/Wenzel*, PinG 2017, 92 (92 f.).
364 Vgl. *Polenz*, in: Simitis u. a., DSGVO/BDSG, Art. 58 Rn. 24, 29.
365 *Martini/Wenzel*, PinG 2017, 92.
366 *Martini/Wenzel*, PinG 2017, 92 (96) sprechen von einem „förmliche[n] Tadel", der den Verantwortlichen nicht nur zur Beseitigung, sondern auch zur Unterlassung zukünftiger Verfehlungen bewegen soll.
367 Siehe Erwg. 148 S. 2 DSGVO.
368 Siehe dazu etwa *Brink*, ZD 2020, 59 (59 f.).

auch kombiniert verhängt werden dürfen, ist hier Fingerspitzengefühl gefragt, um weder übers Ziel hinauszuschießen noch schwerwiegende Verstöße zu gering zu sanktionieren.

(3) Beratung und Kooperation

Zuletzt verbleibt den Aufsichtsbehörden nach Art. 57 Abs. 1 lit. d die Aufgabe und nach Art. 58 Abs. 3 die Befugnis, die Durchsetzung der DSGVO durch Beratung und unterstützende Zusammenarbeit mit kooperationswilligen Verantwortlichen gemeinsam anzustreben.[369] Darunter fällt sowohl die bilaterale Unterstützung konkreter Verantwortlicher als auch die an die generelle Öffentlichkeit gerichtete Information, Schulung und Sensibilisierung. *Roßnagel* spricht insoweit von der Aufgabe zur „offensive[n] allgemeine[n] Aufklärung und Beratung".[370]

In Anbetracht der teils sehr komplizierten Sach- und Rechtslage für Verantwortliche ist diese zusätzliche Ebene der Durchsetzung sehr sinnvoll, wenn nicht gar zwingend notwendig. Als Instrument der Verhaltenssteuerung dient sie im konkreten Fall der individuellen Motivation des jeweiligen Verantwortlichen, gleichzeitig aber auch breitflächig, sofern sie genügend Vertrauen in die Aufsichtsbehörden generiert, damit Verantwortliche ohne Angst vor Sanktionen ihre Bemühungen offenlegen und überprüfen lassen bzw. konkrete Unklarheiten und Fragestellungen äußern. Entscheidend für diese informellen, bilateralen Beratungs- und Kooperationsmaßnahmen ist die breit und vage gefasste Aufgabennormierung in Art. 57 DSGVO. Sie statuiert grundlegend die Doppelrolle der Aufsichtsbehörden als nicht bloß Kontroll-, sondern auch Unterstützungsinstanz.[371] Dass Art. 58 Abs. 3 DSGVO zusätzlich konkret formulierte Befugnisse normiert, ist der Tatsache geschuldet, dass diese zum Großteil trotz ihres primären Leistungs-, auch einen Eingriffscharakter aufweisen.[372] Bei einigen wie der Beratung im Rahmen von Datenschutzfolgenabschätzungen (lit. a), der Billigung von Verhaltensregeln und Zertifizierungskriterien (lit. d und f) und der Genehmigung von verbindlichen internen Vorschriften (lit. j) liegt dies daran, dass die Erfüllung konkreter Verantwortlichenpflichten von der Mitwirkung der Behörde abhängt bzw. Entscheidungen zu treffen sind, deren Ablehnung die Handlungsmöglichkeit des Verantwortlichen einschränkt. Bei anderen Maßnahmen wie der Anfertigung von Stellungnahmen (lit. b.) liegt der Eingriff

[369] Ausführlich zu dieser Kommunikationsaufgabe *Roßnagel*, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, S. 32 ff.

[370] *Roßnagel*, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, S. 87.

[371] Einen expliziten Beratungsauftrag der Aufsichtsbehörden kannte die DSRL nicht, wohl aber das BDSG aF. Siehe dazu *Brink*, ZD 2020, 59 (60 f.).

[372] Vgl. *Polenz*, in: Simitis u. a., DSGVO/BDSG, Art. 58 DSGVO Rn. 49; *Ziebarth*, in: Sydow, DSGVO, Art. 58 Rn. 77; siehe auch *Brink*, ZD 2020, 59 (59).

darin, dass bspw. die Warnung vor konkreten Verarbeitungspraktiken ein negatives Licht auf Verantwortliche werfen kann, die diese öffentlichkeitswirksam vornehmen. Dementsprechend ist es nur konsequent, dass Abs. 4 der Norm geeignete Garantien in Form von Rechtsbehelfen oder formellen Verfahren gegen die aufgezählten Maßnahmen verlangt. Ebenfalls zu einem Eingriff werden alle ergriffenen (auch informellen) Maßnahmen der Beratung mittelbar dann, wenn die Behörde gem. Art. 31 DSGVO die Zusammenarbeit vom Verantwortlichen gegen dessen Willen verlangt.[373]

Unabhängig von den konkreten Einzelmaßnahmen verbleiben hier erneut Zweifel, inwieweit in der Praxis davon ausgegangen werden kann, dass Verantwortliche mit Blick auf die gleichzeitige Befugnis von Aufsichtsbehörden zur Wahrnehmung von Kooperations- und Beratungsaufgaben *und* zur Sanktionierung das nötige Vertrauen entwickeln sollen, das Grundvoraussetzung für eine offene und ehrliche Wahrnehmung der angebotenen Beratungsleistungen ist.[374] Zudem kommt es erneut auf das Fingerspitzengefühl und die „innerbehördliche Ausgewogenheit“[375] in der Beratungspraxis der Aufsichtsbehörden an. Der baden-württembergische Landesdatenschutzbeauftragte *Stefan Brink* jedenfalls berichtet aus seiner Erfahrung von tendenziell eher zurückhaltenden Verantwortlichen, denen jede selbst initiierte Kontaktaufnahme „offenbar einer Selbstanzeige“ gleichkomme.[376]

bb) Zivilrechtliche Rechtsdurchsetzung

Eine Besonderheit des Datenschutzrechts ist es, dass – quasi als Pendant auf Rechtsdurchsetzungsseite zum oben beschriebenen Selbstdatenschutz – neben dieser klassisch verwaltungsrechtlichen und damit hoheitlichen Rechtsdurchsetzung durch Aufsichtsbehörden auch der zivilrechtliche Weg für verschiedene Akteure offensteht.

(1) Schadensersatz

Nach Art. 82 Abs. 1 DSGVO besteht die Möglichkeit des Betroffenen, seinen durch einen Datenschutzverstoß entstandenen Schaden vom Verantwortlichen (oder Auftragsverarbeiter) ersetzen zu lassen.[377] Dabei ist er nicht auf materiel-

---

[373] Vgl. *Martini*, in: Paal/Pauly, DSGVO/BDSG, Art. 31 DSGVO Rn. 14a. Ob die Norm eine Rechtspflicht oder bloß Obliegenheit darstellt, kann dahinstehen, da ihre Missachtung jedenfalls Sanktionen nach sich zieht.

[374] Vgl. *Wolff*, PinG 2017, 109 (110); *Brink*, ZD 2020, 59 (60).

[375] *Brink*, ZD 2020, 59 (60).

[376] *Brink*, ZD 2020, 59 (61).

[377] Auf andere Rechtsfolgen gerichtete Rechtsbehelfe wie der auf Unterlassen werden von Art. 82 DSGVO nicht umfasst, müssen aber gem. Art. 79 DSGVO vom nationalen (Prozess-) Recht der Mitgliedstaaten gewährleistet werden. Vgl. *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 82 DSGVO Rn. 29; a. A. *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 82 DSGVO Rn. 10.

le Schäden begrenzt, denn die Norm umfasst explizit auch immaterielle Schäden.[378] Dies war vor Einführung der DSGVO noch anders: Die DSRL enthielt sich in ihrem die Materie behandelnden Art. 23 einer expliziten Äußerung und sprach schlicht von „jede[m] Schaden einer Person". Die Folge waren stark divergierende Stimmen im Schrifttum, die dieser sprachlichen Enthaltung entweder das Fehlen einer Einschränkung und damit eine Erstreckung auf immaterielle Schäden[379] oder im Umkehrschluss und entsprechend dem (primär deutschen) teleologischen Gedanken der Ausnahmerolle der Ersatzfähigkeit immaterieller Schäden das Fehlen einer solchen Erstreckung[380] annahmen.[381] Jedenfalls für die deutsche Umsetzung in § 7 BDSG aF wurde eine entsprechende Erstreckung meist abgelehnt.[382] Auch die Reichweite des Art. 82 DSGVO ist weiter als die des § 7 BDSG aF, indem nun sämtliche Verstöße gegen DSGVO-Normen umfasst werden,[383] während seinerzeit nur unrichtige oder unzulässige Datenverarbeitungen als Verletzungshandlungen infrage kamen.[384] Praktisch bedeutet diese Erweiterung des Umfangs, dass nun auch Verstöße relevant werden, die zeitlich der eigentlichen Verarbeitung von Betroffenendaten vor- oder nachgehen und nicht in unmittelbarem Zusammenhang mit dieser stehen. Denkbar sind so bspw. Verstöße gegen Organisationspflichten wie die zum Bestellen eines Datenschutzbeauftragten, zur Einführung technisch-organisatorischer Schutzmaßnahmen oder zur Durchführung einer Datenschutzfolgenabschätzung. Letztlich können so jegliche Verstöße, die von Aufsichtsbehörden moniert und sanktioniert werden können, auch von Betroffenen im Rahmen eines Anspruchs geltend gemacht werden.

Damit zeigt sich die herausgehobene Stellung[385] dieses zusätzlichen Durchsetzungswegs als nahezu gleichberechtigte zweite Säule nicht nur der reaktiven Kompensation von bereits geschehenen Verstößen und bereits eingetretenen Schäden, sondern gerade auch der präventiven Abschreckung[386] und damit Verhaltenssteuerung – wer datenschutzwidrig agiert, muss sich nicht nur um

[378] Zu Möglichkeiten der Berechnung beider Arten von Schadensersatz siehe *Strittmatter* u. a., CR 2019, 789 (791 ff.). Siehe zudem *Jacquemain*, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, S. 172.

[379] Vgl. *Brühann/Zerdick*, CR 1996, 429 (435).

[380] So im Ergebnis *Born*, Schadensersatz bei Datenschutzverstößen, S. 84 f.

[381] Ein guter und umfassender Überblick über den Streitstand findet sich bei *Jacquemain*, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, S. 165 ff.

[382] Siehe etwa m. w. N. *Simitis*, in: Simitis, BDSG, § 7 Rn. 32.

[383] Vgl. hierzu *Jacquemain*, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, S. 154 ff. sowie den Wortlaut von Erwg. 146 S. 1 DSGVO.

[384] Vgl. *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 82 DSGVO Rn. 10; siehe auch, die damit einhergehenden Gefahren der vielen abstrakten Pflichten betonend, *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 82 DSGVO Rn. 8 f.; zur alten Rechtslage nach § 7 BDSG aF siehe *Simitis*, in: Simitis, BDSG, § 7 Rn. 14 ff.

[385] *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 82 DSGVO Rn. 1 spricht vom „Herzstück zur Durchsetzung der Schutzvorschriften der DSGVO".

[386] So auch schon m. w. N. *Wehrt/Mohr*, JURA 1995, 536 (536) zum deliktsrechtlichen

behördliche, sondern auch um zivilrechtliche Konsequenzen sorgen. Als verhaltenssteuerndes Instrument soll der Schadensersatzanspruch des Betroffenen daher – ganz in der Tradition der EuGH-Rechtsprechung, die die *Wirksamkeit* des zu leistenden Schadensersatzes betont[387] – weit ausgelegt werden[388], eine präventiv-abschreckende Wirkung zeitigen und Verantwortliche so davon überzeugen, dass sich die Einhaltung aller DSGVO-Bestimmungen, insbesondere auch der präventiven Schutzmaßnahmen, lohnt.[389] Grundvoraussetzung für die Wirksamkeit dieses Instruments ist dabei einmal mehr, dass der harmonisierten Normierung auch eine harmonisierte Anwendung folgt. Insbesondere die deutsche Rechtsprechungspraxis, die bisher – auch nach Wirksamwerden der DSGVO – gerade immateriellen Schadensersatz sehr restriktiv zugesprochen hat,[390] muss sich dafür an die unionsrechtlich durch den EuGH und den Wortlaut der DSGVO vorgegebene Linie anpassen.[391]

(2) Verbandsklagerecht

Das Eintreten des gewünschten Steuerungseffekts durch das Instrument des zivilrechtlichen Schadensersatzes hängt in starkem Maße davon ab, wie umfangreich Betroffene in Fällen eingetretener Datenschutzverstöße von ihm Gebrauch machen. Ein Abschreckungseffekt kann nur dort eintreten, wo die tatsächliche Gefahr besteht, auf Schadensersatz in Anspruch genommen zu werden.[392] Weil jedoch einzelne Betroffene oftmals als eher prozessträge gelten[393] und gera-

---

Schadensersatz im deutschen Recht, der klassischerweise nach wie vor als streng kompensationsbezogen verstanden wird.

[387] EuGH Rs. C-407/14 (Arjona Camacho), ECLI:EU:C:2015:831 Rn. 45; EuGH Rs. C-460/06 (Paquay), ECLI:EU:C:2007:601 Rn. 45.

[388] Vgl. Erwg. 146 S. 3 DSGVO.

[389] Vgl. *Boehm*, in: Simitis, BDSG, Art. 82 DSGVO Rn. 26 m. w. N.; so etwa *Schantz*, NJW 2016, 1841 (1847); siehe auch *Born*, Schadensersatz bei Datenschutzverstößen, S. 112 f.; eine mikroökonomische Analyse des Schadensersatzes in seiner Rolle als finanzieller Regelungsmechanismus findet sich bei *Jacquemain*, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, S. 285 ff.

[390] Siehe den Überblick über die aktuelle Rechtsprechung und Teile der Literatur bei *Strittmatter* u. a., CR 2019, 789 (789 f.) mit Verweisen auf LG Karlsruhe, Urt. v. 02.08.2019 – 8 O 26/19; OLG Dresden, Hinweisbeschl. v. 11.06.2019 – 4 U 760/19, BeckRS 2019, 12941 Rn. 13; AG Diez, Urt. v. 07.11.2018 – 8 C 130/18; zur generell einschränkenden Anwendung des datenschutzrechtlichen Schadensersatzes urteilend zuletzt auch OLG Dresden, Beschl. v. 11.06.2019 – 4 U 760/19, vgl. den Kommentar von *Piltz*, OLG Dresden: Kein Schadensersatz und Schmerzensgeld für Bagatellverstöße gegen die DSGVO.

[391] So auch das Fazit von *Strittmatter* u. a., CR 2019, 789 (796 f.). Als Schritt in diese Richtung angesehen werden kann jüngst ArbG Düsseldorf, Urt. v. 05.03.2020 – 9 Ca 6557/18. Dort wurde ein Anspruch in Höhe von 5.000 Euro aufgrund einer unvollständigen Datenauskunft nach Art. 15 DSGVO zugestanden.

[392] Vgl. *Entorf*, in: Ott/Schäfer, Die Präventivwirkung zivil- und strafrechtlicher Sanktionen: Beiträge zum VI. Travemünder Symposium zur ökonomischen Analyse des Rechts vom 25. – 28. März 1998, S. 1 (4 ff.).

[393] Der Gedanke der rationalen Apathie (rational apathy) besagt, dass insbesondere bei

de im Datenschutzrecht Rechtsgutverletzungen häufig zu für den Einzelnen eher geringen, aber insgesamt durchaus beachtlichen Streuschäden führen[394], wird das Instrumentarium zivilrechtlicher Rechtsdurchsetzung in der DSGVO um ein weiteres Element ergänzt: Nach Art. 80 Abs. 1 können Betroffene Einrichtungen wie Nichtregierungsorganisationen oder Interessenverbände also auch[395] damit beauftragen, ihre Rechte gegen Verantwortliche für sie geltend zu machen, wobei dies für das Recht auf Schadensersatz nur unter der Maßgabe gilt, dass das nationale Recht der Mitgliedstaaten ein solches Vorgehen vorsieht[396]. Diese Art der Beauftragung erspart Betroffenen Kosten und Aufwand und verringert so – jedenfalls in der Theorie – die Hemmschwelle zum Tätigwerden.[397] Auch nimmt es ihnen die Arbeit, den korrekten Verantwortlichen zu identifizieren und die – oftmals komplizierte – Sachlage abschließend zu bewerten, um die Erfolgschancen zu kalkulieren.

Dennoch stellt die Voraussetzung der Beauftragung nach wie vor eine Hürde in Form eines aktiven Tätigwerdens des Betroffenen dar. Demgegenüber steht das verbleibende Risiko, einen Prozess zu verlieren.[398] Grundvoraussetzung ist zudem, dass Betroffene überhaupt Kenntnis darüber erlangen, dass im Zusammenhang mit Verarbeitungen von sie betreffenden Daten gegen Vorschriften der DSGVO verstoßen worden sein könnte.[399] Abhilfe schaffen könnte hier Art. 80

Verbrauchern die Wahrscheinlichkeit einer Durchsetzung der eigenen Rechte in starkem Maße von der Höhe der aufzubringenden Kosten im Verhältnis zum erwarteten Gewinn abhängt. Übersteigt der Aufwand den erwarteten Nutzen, so wird ein Verbraucher sein Recht tendenziell nicht einklagen, vgl. *Weber*, The law and economics of enforcing European consumer law, S. 35. Zu diesem Problem konkret in Bezug auf das Datenschutzrecht auch *Pohl*, PinG 2017, 85 (87). Genereller zu den Abschreckungseffekten des deutschen Zivilprozessrechts für Verbraucher *Pollmann*, A Comparative Law and Economics Analysis of the Proposed German „Model Declaratory Action", S. 4 ff.

394 Vgl. *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 80 DSGVO Rn. 1 mit zusätzlichem Verweis auf die deutsche Rechtstradition, speziell bei immateriellen Schäden nur geringe Schadensersatzsummen zuzusprechen; siehe auch *Uebele*, GRUR 2019, 694 (694): „[…] so dass eine Geltendmachung in Anbetracht der Prozessrisiken häufig unterbleibt." Auch *Jacquemain*, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, S. 366 betont die hohen Risiken für das klagende Individuum, die nach seiner Ansicht „dieses Individualrechtsschutzinstrument praktisch leerlaufen" lassen.

395 Neben dem *supra* beschriebenen Recht auf Vertretung gegenüber der Aufsichtsbehörde.

396 Im deutschen Recht ist eine solche rechtliche Regelung, allerdings beschränkt auf Verbraucherverbände im Rahmen ihres Aufgabenbereichs, in § 79 Abs. 2 S. 2 Nr. 3 ZPO zu finden. Vgl. *Werkmeister*, in: Gola, DSGVO, Art. 80 Rn. 9.

397 Vgl. *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 80 DSGVO Rn. 1; *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 80 DSGVO Rn. 2 spricht von einer „effektiveren Nutzung der Rechtsbehelfe".

398 Diese Ungewissheit besteht bei den stark abstrakt gehaltenen Vorgaben der DSGVO in besonderem Maße. Vgl. *Golla*, jipitec 2017, 70 (74): „[…]data subjects will have a hard time determining whether a violation has occurred, which can prevent them from filing complaints."

399 Empirische Studien zur Rechtsdurchsetzung durch Betroffene im Datenschutzrecht sind selten. Einen gewissen Einblick gibt etwa *Deutsches Institut für Menschenrechte*, „Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten" – eine Studie der EU-Grund-

Abs. 2 DSGVO, der den Mitgliedstaaten die Möglichkeit eröffnet, ein „echtes" Verbandsklagerecht einzuführen, bei dem Verbände unabhängig von einer aktiven Beauftragung tätig werden dürfen.[400] Dabei verbleibt den Mitgliedstaaten weitreichender Spielraum hinsichtlich Umfang und Ausgestaltung eines solchen Rechts. Im deutschen UKlaG findet sich eine, jedoch inhaltlich eingeschränkte, Umsetzung in § 2 Abs. 2 Nr. 11[401] für Verbraucherangelegenheiten sowie in § 1 für Verstöße im Rahmen von AGB-Bestimmungen. Ein solches beauftragungsfreies Tätigwerden von Verbänden im Namen der potenziell geschädigten Betroffenen würde die zivilrechtliche Rechtsdurchsetzung mit Blick auf die beschriebenen Hürden sicher verbessern. Einem derart weiten Verständnis der Norm schiebt jedoch zumindest in Bezug auf das Recht auf Schadensersatz die DSGVO in Erwg. 142, letzter Satz, selbst explizit einen Riegel vor.[402] Auf dem Klageweg durchgesetzt werden können daher ohne Beauftragung vor allem die Betroffenenrechte wie das auf Löschung unbefugt verarbeiteter und gespeicherter Daten – was mit Blick auf die Konsequenzen und einen möglicherweise entgegenstehenden Willen einzelner Betroffener zuweilen kritisch betrachtet wird.[403]

Nichtsdestotrotz bietet sich mit Art. 80 Abs. 1 und 2 DSGVO in Kombination mit den jeweiligen nationalen Gesetzen zumindest auf dem Papier ein sinnvoller zweiter Weg, der das Potential hat, einerseits überforderte Aufsichtsbehörden zu entlasten[404] und andererseits überforderte Betroffene bei der Wahrnehmung ihrer Rechte zu unterstützen und so das generelle Durchsetzungsniveau der DSGVO zu steigern.

(3) Wettbewerbsrechtlicher Schutz von Marktteilnehmern

Während die beiden eben behandelten Instrumente die Rechtsdurchsetzung auf dem Zivilrechtsweg durch Betroffene oder diese unterstützende Akteure betra-

---

rechteagentur. Demnach gehören die Komplexität der datenschutzrechtlichen Bestimmungen sowie fehlender Zugang zu Informationen zu den größten Hürden. Vgl. auch *Elbrecht/Schröder*, K&R 2015, 361 (361).

[400] Eine solche, explizit normierte, Öffnungsklausel kannte die DSRL noch nicht. Nichtsdestotrotz stand Mitgliedstaaten auch damals die Möglichkeit offen, Verbandsklagen national zu normieren. Vgl. die Ausführungen von *GA Bobek*, Schlussanträge zur Rs. C-40/17, Rn. 28 ff., insbesondere 34. Diesen Ausführungen folgend sodann EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 51 und 59.

[401] Siehe dazu und speziell zu den Einschränkungen ausführlich *Halfmeier*, NJW 2016, 1126 (1127 ff.).

[402] Vgl. auch *Boehm*, in: Simitis u. a., DSGVO/BDSG, Art. 80 DSGVO Rn. 12; *Werkmeister*, in: Gola, DSGVO, Art. 80 Rn. 10 f.

[403] Vgl. *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 80 DSGVO Rn. 15.

[404] A. A. aber *Schwichtenberg*, PinG 2017, 104 (105 f.) mit Verweis auf die Gefahr redundanter Ressourcenaufwendungen, wenn Verbraucherverbände und Aufsichtsbehörden sich mit denselben Fällen beschäftigen, und drohender Rechtsunsicherheit, wenn sie dabei zu unterschiedlichen Ansichten bzw. Ergebnissen kommen.

fen, kommt im deutschen Recht daneben noch eine zusätzliche Ebene in Betracht: die Sanktionierung von Datenschutzverstößen aus Wettbewerbsperspektive. So erlaubt das UWG über § 3a die Anwendung von Lauterkeitsrecht überall dort, wo die Durchsetzung von „Marktverhaltensregelungen", also wettbewerblich relevanten Normen außerhalb des UWG,[405] infrage steht. Der dahinterstehende Grundgedanke leuchtet ein: Auch die systematische Verletzung datenschutzrechtlicher Normen durch ein Unternehmen kann den freien Wettbewerb verfälschen, wenn gleichzeitig Konkurrenten Geld und Aufwand darin investieren, datenschutzkonform zu agieren, und die Verstöße nicht hinreichend sanktioniert werden.[406] Entscheidend ist, dass der jeweiligen Norm zumindest auch der Zweck entnommen werden kann, Mitbewerber oder Verbraucher als Marktteilnehmer in ihrer wettbewerblichen Entfaltungsfreiheit zu schützen. Als Steuerungsinstrument hat diese Ebene das Potential, aus einer zusätzlichen Richtung Druck auf Verantwortliche auszuüben. Wo diese also keine Notwendigkeit für datenschutzkonformes Handeln sehen, weil sie bspw. eine Sanktionierung durch Aufsichtsbehörden aufgrund der Überlastung dieser und eine Inanspruchnahme durch Betroffene aufgrund fehlender Sensibilität oder Prozessfreudigkeit nicht befürchten, könnte die Gefahr einer Abmahnung durch datenschutzkonforme Mitbewerber das Ergebnis dieser Kosten-Nutzen-Rechnung möglicherweise beeinflussen. Die Möglichkeit von Mitbewerbern, im eigenen Interesse die Einhaltung von Datenschutzvorschriften durch ihre Konkurrenten durchzusetzen (§ 8 Abs. 3 Nr. 1 sowie § 9 UWG), würde dann mittelbar zu deren Konformitätsbereitschaft beitragen und somit, quasi reflexhaft, die generelle Durchsetzung des Datenschutzrechts fördern.[407]

Zuweilen wird die Legitimität wettbewerblicher Rechtsbehelfe jedoch aus zwei Gesichtspunkten in Zweifel gezogen. Einige Stimmen argumentieren, der DSGVO und der in ihr normierten, insbesondere zivilrechtlichen, Rechtsbehelfe komme eine grundsätzliche Sperrwirkung zu, sodass ein weitergehendes Zurückgreifen auf gesetzesexterne Rechtsbehelfe unzulässig sei.[408] Des Weiteren wird, letztlich in eine ähnliche Richtung gehend, argumentiert, es sei trotz fehlender Sperrwirkung schlicht keine der Normen der DSGVO als Marktverhaltensregel iSd § 3a UWG zu verstehen, weil diese allesamt eine andere, rein auf den Schutz von Privatsphäre und personenbezogenen Daten mit

---

[405] *Podszun/Toma*, NJW 2016, 2987 (2989 f.); instruktiv auch das Beispiel bei *Diercks*, CR 2019, 95 (95 f.).

[406] Vgl. *Podszun/Toma*, NJW 2016, 2987 (2989).

[407] Neben Mitbewerbern können jedenfalls die Ansprüche auf Beseitigung und Unterlassung auch Wirtschafts- und Verbraucherschutzverbände sowie Industrie-, Handels- und Handwerkskammern durchsetzen, vgl. § 8 Abs. 3 Nr. 2, 3 und 4 UWG.

[408] In diese Richtung argumentierend zur Rechtslage unter der DSRL *Zech*, WRP 2013, 1434 (1434); so explizit auch für die DSGVO argumentierend *Köhler*, in: Köhler u. a., Gesetz gegen den unlauteren Wettbewerb, § 3a UWG Rn. 1.40a und 1.74b; *Ohly*, GRUR 2019, 686 (688); *Baumgartner/Sitte*, ZD 2018, 555 (557 f.).

Blick auf die innere und äußere Entfaltungsfreiheit bezogene Zielrichtung hätten.[409]

Überzeugender ist mit Blick auf die heutzutage kaum zu bestreitende wettbewerbliche Relevanz von Datenverarbeitungen, etwa bei der Nutzung zu Werbezwecken, aber auch mit Blick auf die teilweise immensen Kosten der Implementation von technischen und organisatorischen Maßnahmen zum Datenschutz, ein Mittelweg. Dass Kapitel VIII der DSGVO das Regime der Rechtsbehelfe *für Betroffene* abschließend regelt, lässt sich nicht bestreiten. Macht man sich die Betonung auf den Betroffenen aber bewusst, lässt sich ebenfalls nicht bestreiten, dass wettbewerbsrechtliche Rechtsbehelfe durch Mitbewerber zwar im Ergebnis hinsichtlich der Gesamtlage auch Betroffenen zugutekommen (können), in erster Linie aber dem Schutz der Mitbewerber dienen.[410]

Eine gänzliche Sperrwirkung der DSGVO gegenüber externer und über die Öffnungsklauseln hinausgehender Rechtsbehelfe wird dementsprechend inzwischen von der überwiegenden Anzahl der Stimmen in der Literatur[411] und auch großen Teilen der Rechtsprechung[412] – zurecht – abgelehnt. Es verbleibt dabei die – insofern auch sachgerechte – Differenzierung auf Tatbestandsebene danach, ob die jeweils infrage stehende Norm eine Marktverhaltensregel im Sinne des § 3a UWG darstellt[413] und, nachgelagert, ob deren Missachtung im konkreten Fall „geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen".[414] Ein Herausfiltern derjenigen Normen, die *allein* dem Schutz der Betroffenen dienen[415] – bspw., so könnte man argumentieren, die Betroffenenrechte in Art. 15 ff. DSGVO – erreicht so bereits den Zweck, den viele Verfechter einer kompletten Sperrwir-

[409] Vgl. die Nachweise in *Podszun/Toma*, NJW 2016, 2987 (2989); in diese Richtung gehend urteilten etwa in Bezug auf das BDSG aF das OLG Dresden, Urt. v. 26.03.2013 – 14 U 1776/12 BeckRS 2014 sowie das LG Leipzig, Urt. v. 17.10.2012 – 5 O 1044/12, BeckRS 2014, 15222.

[410] Vgl. *Diercks*, CR 2018, S001 Rn. 14.

[411] Instruktiv und ausführlich *Diercks*, CR 2018, S001; gut argumentierend auch *Aßhoff*, CR 2018, 720 (726 f.); *Schreiber*, GRUR-Prax. 2018, 371; sehr ausführlich und noch weiter hinsichtlich der Aktivlegitimation gem. § 8 Abs. 3 UWG differenzierend *Uebele*, GRUR 2019, 694 (697 ff.); siehe zudem *Wolff*, ZD 2018, 248 (250 ff.), der konzise die Wettbewerbselemente der europäischen Datenschutztradition herausarbeitet.

[412] So jüngst explizit zur DSGVO KG Berlin, Urt. v. 20.12.2019 – 5 U 9/18 (noch nicht rechtskräftig), OLG Stuttgart, Urt. v. 27.02.2020 – 2 U 257/19 (noch nicht rechtskräftig), und OLG Hamburg, Urt. v. 25.10.2018 – 3 U 66/17, BeckRS 2018, 27136 Rn. 34 ff. Im Ergebnis gleichlaufend, ohne aber inhaltlich auf den Streit einzugehen LG Würzburg, Beschluss v. 13.09.2018 – 11 O 1741/17; ebenso noch zur Rechtslage unter der DSRL LG Hamburg, Beschluss. v. 08.10.2018 – 2–06 O 349/18.

[413] Siehe hierzu etwa die Aufzählung von entsprechenden Normen aus dem BDSG aF bei *Podszun/Toma*, NJW 2016, 2987 (2990); in diese Richtung argumentierend auch *Paal*, in: Körber/Kühling, Regulierung – Wettbewerb – Innovation, S. 143 (158).

[414] Vgl *Schreiber*, GRUR-Prax. 2018, 371 (373 f.).

[415] So auch die Differenzierung des OLG Hamburg, Urt. v. 25.10.2018 – 3 U 66/17, BeckRS 2018, 27136 Rn. 41, das einen solchen Charakter für § 28 Abs. 7 BDSG aF ablehnte.

kung anführen. Auch die von Kritikern angeführte Sorge, es könne sich einer regelrechte Welle missbräuchlicher Abmahnungen unter den Wettbewerbern entwickeln[416], hat sich empirisch nach bisherigen Erfahrungswerten nicht bestätigen können.[417]

2. Die Steuerungswirkung

Hinsichtlich des eben beschriebenen und sehr vielschichtigen Instrumentariums, mit dem das Verhalten des Verantwortlichen in eine Richtung gesteuert werden soll, die unter dem Überbegriff der Datenschutzkonformität beschrieben wird, lassen sich verschiedene Wirkungen aufzeigen, die damit vom Verordnungsgeber als regelnde Instanz erreicht werden sollen. Der modernen Regelungswissenschaft[418] entsprechend dienen die Instrumente also nicht nur der Erreichung von Rechtskonformität als Alleinzweck, sondern dienen auch dazu, das beim Verantwortlichen vorhandene Wissen und seine Kompetenz kooperativ nutzbar zu machen.[419]

Die nachfolgenden Wirkungskategorien lassen sich dabei nicht alle streng voneinander trennen, teilweise gibt es Überschneidungen. Ebenso lassen sich viele der beispielhaft angeführten Pflichten der DSGVO nicht isoliert einer Zielrichtung zuordnen, sondern wirken auf mehrere der angestrebten Wirkungen hin.

a) Verantwortlichkeitszuschreibung als Form von Komplexitätsmanagement

Hinter dem Akt der Verantwortungszuschreibung steht zunächst die Idee, alle auf einer nachgelagerten Ebene formulierten Pflichten gebündelt dem Akteur zu übertragen, der ihnen (bei einer typisierten Betrachtung) in möglichst effektiver und effizienter Weise nachkommen kann.[420] Wie jede Art von Regulierungsmodell (und generell jedes theoretische Modell), macht das Konzept datenschutzrechtlicher Verantwortlichkeitszuschreibung die Realität ungemein komplexer Informations- und Datenflüsse handhabbar, indem es sie auf ein be-

---

[416] Zur diesbezüglichen Unsicherheit siehe *Baumgartner/Sitte*, ZD 2018, 555.

[417] Siehe m. w. N. *Aßhoff*, CR 2018, 720; zu den zwischenzeitlichen gesetzgeberischen Vorkehrungen gegen möglichen Missbrauch von Abmahnungen siehe *Lurtz*, ZD-Aktuell 2018, 06292; zum selben Thema *Köhler*, ZD 2019, 285.

[418] Grundlegend hierzu *Schuppert*, Governance und Rechtsetzung, S. insb. 97 ff.

[419] Vgl. *Hoffmann-Riem*, in: Röhl, Wissen – zur kognitiven Dimension des Rechts, S. 159 (177), der hinsichtlich der Komplexität moderner Regelungsmaterien konstatiert: „Eine Reduktion der Problemwahrnehmung auf das dem Staat verfügbare (vielfach erkennbar oder unerkennbar suboptimale) Wissen würde ein Risiko unangemessener Problemlösung bewirken. Es gilt auch, andere Wissensträger zu nutzen." Ausführlich dazu auch *Schuppert*, Wissen, Governance, Recht., S. 83 ff.

[420] Das ergibt sich im Umkehrschluss bereits aus dem funktionalen Ansatz bei der Bestimmung des Verantwortlichen. Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 12.

greifbares und nutzbares Maß simplifiziert und dabei gleichzeitig versucht, den gewählten Ausschnitt der Realität möglichst realitätsgetreu und repräsentativ zu halten.[421]

Für den Verordnungsgeber als Regelungsgeber bedeutet dies eine Art von Komplexitätsmanagement in mehrfacher Hinsicht.

aa) Management von Akteurskomplexität

Der Komplexität der an einem konkreten Akt der Datenverarbeitung beteiligten Akteure versucht der Verordnungsgeber Herr zu werden, indem er sich den anhand typisierter Kriterien zentral erscheinenden Akteur heraussucht und mit aus verschiedenen Bereichen stammenden Pflichten belegt – um somit auch nur diesen zur Kontrolle der Einhaltung jener Pflichten beaufsichtigen zu müssen. Diese Art von Komplexitätsmanagement zeigt sich z. B. darin, dass der Verantwortliche in einem abgestuften Maße als solcher erkennbar sein muss – gegenüber dem Betroffenen etwa durch Information bei bzw. zeitnah nach der Verarbeitung der Daten[422], gegenüber der Aufsichtsbehörde etwa im Vorfeld der Verarbeitung im Wege der Übermittlung des Ergebnisses einer etwaigen Datenschutzfolgenabschätzung[423] oder im Nachgang einer Datenpanne[424]. Auch die Vorschriften über die Auftragsverarbeitung in Art. 28 DSGVO verfolgen diesen Zweck, wenn dem Verantwortlichen als „Herrscher" über alle relevanten Entscheidungskompetenzen Auswahl- und Überwachungspflichten gegenüber dem von ihm gewählten Auftragsverarbeiter treffen. Weder Aufsichtsbehörden noch Betroffene müssen sich also mit diesem zusätzlichen Akteur unmittelbar befassen, ihnen gegenüber bleibt der Verantwortliche zentraler Ansprechpartner und Auskunftsstelle über die relevanten Verarbeitungsgegebenheiten. Indem er im Grundsatz für datenschutzrechtswidriges Verhalten seines Auftragsverarbeiters haften muss,[425] delegiert der Gesetzgeber die Kontrolle des Auftragsverarbeiters an ihn – die Wahl eines seriösen und belegbar datenschutzkonform aufgestellten Akteurs ist demnach in seinem eigenen Interesse. Genauso verhält es sich im Umkehrschluss mit dem Auftragsverarbeiter, dessen Eigeninteresse an datenschutzkonformem Handeln darin begründet liegt, sonst (eine solide Auswahlkontrolle durch den Verantwortlichen vorausgesetzt) keine Aufträge erteilt zu bekommen und ggf. eine eigene Haftung auszulösen.[426]

---

[421] Zu den Hauptmerkmalen des allgemeinen Modellbegriffs siehe *Stachowiak*, Allgemeine Modelltheorie, S. 128 ff.

[422] Art. 13, 14 DSGVO.

[423] Art. 35 DSGVO.

[424] Art. 33 Abs. 1 DSGVO.

[425] Ein Regress beim Auftragsverarbeiter bzw. dessen unmittelbare Haftung setzen nach Art. 82 Abs. 2 S. 2 DSGVO voraus, dass dieser eine Pflicht verletzt hat, die die Verordnung (etwa in Art. 32 Abs. 1) oder der Verantwortliche (etwa die in Art. 28 aufgezählten) speziell ihm bzw. generell Auftragsverarbeitern auferlegt hat.

[426] Siehe die vorherige Fußnote.

Diese Zuordnung erfolgt über zwei Zuordnungsobjekte, die über die Tatbestandsvoraussetzungen der Verantwortlichkeit in Art. 4 Nr. 7 DSGVO definiert werden: die *Verarbeitung* von personenbezogenen Daten einerseits und die *Zweck- und Mittelentscheidung* über diese Verarbeitung andererseits. Dabei beschreibt der Begriff der Verarbeitung den zusammengefassten Lebenssachverhalt, dessen Verantwortung der Verordnungsgeber dem Verantwortlichen überträgt.[427] Der Verarbeitungsbegriff und seine Auslegung ist also eine mögliche Stellschraube für die Reichweite dessen, worauf sich der Strauß an Pflichten des Verantwortlichen bezieht. Ein großer Spielraum zum Verstellen dieser Schraube verbleibt jedoch nicht, da der Begriff einerseits stark handlungs- bzw. tätigkeitsbezogen (und somit in seiner Faktizität kaum offen für Fiktionen oder andere Anknüpfungspunktkreationen ist) ist und andererseits alle denkbaren datenbezogenen Handlungsformen umfasst.[428] Da Art. 4 Nr. 2 DSGVO, der den Begriff definiert, zudem neben dem einzelnen Vorgang auch ganze Vorgangs*reihen* unter den Begriff fasst, wird offenbar, dass das zweite Zuordnungsobjekt, namentlich die Beherrschung von Zwecken und Mitteln der Verarbeitung, das eigentlich flexible Element bei der Zuschreibung der Verantwortlichkeitssphäre „Verarbeitung" ist. Wie sich das Verständnis dieses Begriffspaars über die Jahre und insbesondere seit der Zäsur des Wirtschaftsakademie-Urteils[429] des EuGH[430] gewandelt hat und wie es nach heutigem Stand zu verstehen ist, soll unten in Abschnitt C. ausführlich behandelt werden.

Ein Beispiel für ein in einem anderen Bereich etabliertes Regelungskonzept dieser Art zur Reduzierung von Akteurskomplexität findet sich im Rundfunkrecht. Auch hier wird die Figur des Rundfunkveranstalters genutzt, um die Erfüllung bestimmter Pflichten und Einhaltung bestimmter Standards gebündelt einem Akteur zuzuschreiben, der somit zu einem gewissen Ausmaß die Verantwortung für die Rechtmäßigkeit eines gesamten Lebenssachverhalts – namentlich der Veranstaltung von Rundfunk bzw. des Anbietens eines Rundfunkprogramms – übertragen bekommt, an dem neben ihm noch weitere Akteure (in diesem Fall etwa die Produzenten der einzelnen Inhalte) beteiligt sind. Zwar haften auch diese (aus der Perspektive der Rundfunkregulierung) peripheren Akteure naturgemäß für etwa Persönlichkeitsrechtsverletzungen der von ihnen

[427] Gleichzeitig ist er gem. Art. 2 Abs. 1 DSGVO Voraussetzung für die Eröffnung des sachlichen Anwendungsbereichs der DSGVO.

[428] Art. 4 Nr. 2 DSGVO zählt insoweit nur beispielhaft das Erheben, Erfassen, Ordnen, Speichern, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen, Übermitteln, Verbreiten, Abgleichen, Verknüpfen, Einschränken, Löschen und Vernichten von Daten auf.

[429] Siehe EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388.

[430] Alternativ ließe sich der Stein des Anstoßes bereits in EuGH, Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317, finden. In diesem Urteil legte der EuGH zum ersten Mal den Leitsatz der weiten Auslegung der Verantwortlichkeit im Interesse eines wirksamen Betroffenenschutzes fest.

produzierten Inhalte. Dennoch entschied sich der Gesetzgeber dazu, Rundfunkveranstaltern eine eigenständige Verantwortung für die Sphäre des von ihm (dem Gesetzgeber) selbst definierten Lebenssachverhalts der Rundfunkveranstaltung aufzuerlegen, welche (die Verantwortung) mit den Programmgrundsätzen in § 41 RStV nicht zuletzt auch die Achtung von Persönlichkeitsrechten[431] umfasst.

bb) Management von fachlich-technischer Komplexität

Zugleich verkörpert dieser zentrale Akteur idealerweise auch die auf technischer Ebene mit den Einzelheiten und Gefahren der Verarbeitung vertrauteste Figur[432] und erleichtert somit den zur Überwachung und Durchsetzung der DSGVO[433] verpflichteten und ermächtigten Aufsichtsbehörden[434] ihre Arbeit, indem diese sich (zumindest teilweise) seiner technischen Expertise bedienen und damit auch die auf dieser Ebene vorherrschende Komplexität durch Auslagerung teilweise auflösen können. Dies geschieht etwa im Bereich der allgemeinen Beratungstätigkeit, die die Aufsichtsbehörden gem. Art. 57 Abs. 1 lit. d DSGVO zugunsten der Verantwortlichen auszuüben haben: Der hier entstehende Austausch führt indirekt auch zu Kompetenzgewinnen innerhalb der Aufsichtsbehörde[435] und geben ihr die Gelegenheit, „ihre Vorstellungen vom datenschutzgerechten Umgang mit personenbezogenen Informationen anhand praktischer Fallgestaltungen zu entwickeln, fortzuentwickeln, zu verbreiten und zu realisieren".[436] Auch im Bereich der regulierten Selbstregulierung[437] in Form von Verhaltensregeln gem. Art. 40 Abs. 1 und Zertifizierungen gem. Art. 42 Abs. 1 DSGVO wird in einem gewissen Rahmen den Verantwortlichen und ihren Interessenverbänden[438] die Möglichkeit gegeben, durch ihre Expertise zielgerechtere Handlungswege und Lösungsmöglichkeiten zu finden und in Standards zu gießen, als sie der Verordnungsgeber oder auch die Aufsichtsbehörden selbst hätte konkret vorgeben können.[439]

---

[431] In Form der „gesetzlichen Bestimmungen zum Schutz der persönlichen Ehre" in § 41 Abs. 1 S. 4 RStV.

[432] Vgl. *Binns*, International Data Privacy Law 2017, 22 (32): „[…] regulatees are likely to consistently have greater expertise than the regulator".

[433] Siehe die Aufgabenbeschreibung in Art. 57 Abs. 1 lit.a DSGVO.

[434] Definiert und beschrieben in Art. 51 ff. DSGVO.

[435] *Roßnagel*, Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, S. 89.

[436] *Brink*, ZD 2020, 59 (60).

[437] Siehe *supra* in Abschnitt 1. c).

[438] Siehe zur historischen Rolle der Wirtschaftskammern in diesem Zusammenhang *Kluth*, in: Spiecker Döhmann/Collin, Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, S. 73 (86).

[439] Vgl. generell zur Nutzung privatisierten Rechts (als welches die beschriebenen Ergebnisse der Standardsetzung im weitesten Sinne angesehen werden können) zur Steigerung

Noch besser verdeutlicht wird dieser Effekt aber durch die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung in Art. 35. Im Rahmen dieser muss der Verantwortliche die von ihm beabsichtigten Verarbeitungsschritte mitsamt der von ihnen verfolgten Zwecke systematisch reflektieren und beschreiben, die daraus resultierenden Risiken für Betroffene abschätzen und hinsichtlich ihrer Schwere für die Rechte und Interessen der Betroffenen bewerten.[440] Zudem müssen Abhilfemaßnahmen für die erkannten Risiken gefunden und in ihrer voraussichtlichen Wirksamkeit beschrieben und bewertet werden. Das Ergebnis einer solchen Folgenabschätzung muss gem. Art. 36 Abs. 1 DSGVO zumindest in Fällen eines zu erwartenden hohen Risikos der Verarbeitung bei gleichzeitiger Abwesenheit geplanter Abhilfemaßnahmen der zuständigen Aufsichtsbehörde vorgelegt werden. Diese bedient sich somit der vorhandenen Kompetenz des Verantwortlichen und muss nur das Ergebnis dessen Abschätzungsprozesses bewerten. Hier offenbart sich freilich bereits ein möglicher Nachteil dieser Art von Komplexitätsmanagement: Sie ist auf ein hinreichendes Vertrauen in den Verantwortlichen angewiesen, sowohl hinsichtlich seiner tatsächlichen Fachkompetenz als auch hinsichtlich seiner sorgfältigen Pflichterfüllung und wahrheitsgetreuen Dokumentation seiner (unternehmens-)internen Prozesse und Verarbeitungsumstände. Ist die Aufsichtsbehörde nicht in der Lage, die Risikoeinschätzung des Verantwortlichen zu überprüfen und kontrollieren, ist das Instrument letztlich nutzlos.

Zur Absicherung des Vertrauens in den Verantwortlichen trägt eine weitere beispielhafte Pflicht der DSGVO bei, die zwingend mit in den Blick genommen werden muss: Die Pflicht zur Benennung eines Datenschutzbeauftragten gem. Art. 37. Sie besteht nicht für jeden Verantwortlichen, sondern hängt von der besonderen Kritikalität der von diesem vorgenommenen Datenverarbeitungen ab.[441] Ein solcher kann vom Verantwortlichen wahlweise als interner Datenschutzbeauftragter (also direkt bei ihm Beschäftigter) oder aber in Form eines Beraters als externer Datenschutzbeauftragter benannt werden.[442] In jedem Fall dient er dazu, das auf Seiten des Verantwortlichen existierende Fachwissen zu erhöhen[443] und als zwischengelagerte (aber dennoch klar im Lager des Verantwortlichen stehende) Stelle den Austausch zwischen Verantwortlichem und

gesellschaftlichen Wissens und staatlicher Lernfähigkeit *Köndgen*, AcP 2006, 477 (481 ff., 512 f.).

[440] Siehe ausführlich zu den Einzelheiten und der Bedeutung dieses Instruments *supra* in Abschnitt 1. d).

[441] Art. 37 Abs. 1 lit. b. und c. DSGVO knüpft im Rahmen privater Datenverarbeitungen die Pflicht zur Bestellung daran, dass die jeweilige Kerntätigkeit die umfangreiche, regelmäßige und systematische Überwachung oder die umfangreiche Verarbeitung von gem. Art. 9 und 10 DSGVO besonders geschützten Daten voraussetzt. Daneben verbleibt den Mitgliedstaaten nach Art. 37 Abs. 4 S. 1 aE DSGVO die Möglichkeit, eigene zusätzliche Voraussetzungen zu normieren.

[442] Vgl. *Drewes*, in: Simitis u. a., DSGVO/BDSG, Art. 37 DSGVO Rn. 50 ff.

[443] Vgl. *Klug*, ZD 2016, 315 (318).

Aufsichtsbehörde zu gewährleisten bzw. erleichtern. Das zeigt sich etwa darin, dass seine Kontaktdaten gegenüber der Aufsichtsbehörde,[444] aber auch gegenüber Betroffenen[445] veröffentlicht werden müssen. Das Recht stellt zudem hohe Anforderungen an seine Kompetenzen und fachlichen Qualitäten (und koppelt diese an die Risikohöhe der konkreten Verarbeitungsvorhaben des jeweiligen Verantwortlichen, sodass die Anforderungen mit zunehmender Kritikalität der Verarbeitungen steigen[446]), aber auch an seine Unabhängigkeit und Integrität[447]. Durch diese Methode, das Wissen um und den Einblick in die genaueren Umstände und Einzelheiten der Datenverarbeitungen beim Verantwortlichen mit datenschutzrechtlichem Fachwissen, Lösungsansätzen zur Risikominimierung und direkter Möglichkeit zur Einflussnahme zu kombinieren, soll im Rahmen einer vertrauensvollen Zusammenarbeit eine möglichst weitgehende datenschutzfreundliche Ausgestaltung von internen Strukturen und Prozessen beim Verantwortlichen erreicht und das Verständnis und die Akzeptanz für die Bedeutung einer solchen Ausgestaltung gefördert werden. Gleichzeitig erleichtert die Existenz eines auch fachlich geschulten Ansprechpartners für die Aufsichtsbehörden den Austausch mit und die Kontrolle des Verantwortlichen. Soweit keine konkreten Anhaltspunkte für datenschutzwidriges Verhalten vorliegen, können sie sich zu einem gewissen Grad auf die vom Datenschutzbeauftragten erhaltenen Informationen verlassen und müssen, so das Konzept, nicht im Detail nachprüfen. Das erspart nicht zuletzt Behördenressourcen. Somit kann in solchen Fällen zumindest teilweise das oben beschriebene Problem der Angewiesenheit auf ein ehrliches und konstruktives Entgegenkommen des Verantwortlichen aufgelöst werden. An die Stelle dieser verringerten Unsicherheit tritt jedoch direkt die nächste: Auch ein vorbildlich unabhängiger und qualifizierter Datenschutzbeauftragter ist abhängig von den Einblicken und dem Entgegenkommen, die der Verantwortliche ihm gewährt. Fehlt es letzterem zudem selbst an vollständigem Verständnis über die bei ihm stattfindenden Prozesse und Datenflüsse[448], kann auch ein hinzukommender Datenschutzbeauftragter nur bedingt weiterhelfen.

Unter anderem auf dieses Problem zielt der in Art. 25 Abs. 1 DSGVO verankerte *privacy by design*-Grundsatz – zu dessen Verwirklichung der Datenschutzbeauftragte ebenfalls beitragen soll – ab, der Verantwortliche dazu verpflichtet, ihre Datenverarbeitungsumgebungen strukturell datenschutz-

444 Vgl. Art. 37 Abs. 7 DSGVO.

445 Im Rahmen der Informationspflichten in Art. 13, 14 DSGVO.

446 Vgl. Erwg. 97 der DSGVO sowie die Ausführungen von *Drewes*, in: Simitis u. a., DSGVO/BDSG, Art. 37 DSGVO Rn. 45 ff.

447 Vgl. *Art. 29-Datenschutzgruppe*, Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), S. 14.

448 Als Beispiele für solche Fälle sei hier nur der bereits erwähnte Einsatz von selbstlernenden Algorithmen sowie die ebenfalls bereits angesprochene Charakteristik agiler, sich spontan ändernder Verarbeitungspraktiken und Datenflüsse in Startup-Unternehmen genannt.

freundlich zu gestalten. Dazu gehört auch, bereits bei der anfänglichen Gestaltung der internen Verarbeitungsarchitektur Kriterien wie Nachvollziehbarkeit, Kontrollierbarkeit und Beweisbarkeit der tatsächlichen und möglichen Datenflüsse zu garantieren. Mit anderen Worten: Der Grundsatz verpflichtet den Verantwortlichen dazu, durch frühestmögliches Mitdenken des Datenschutzes schon zu verhindern, dass die eigenen Strukturen unnötige Komplexität gewinnen, sowohl hinsichtlich der tatsächlichen Datenschutzrisiken als auch der Möglichkeit, über die Gegebenheiten Rechenschaft abzulegen.[449]

Das Ziel des Managements fachlich-technischer Komplexität durch Wahl und Ausgestaltung des Verantwortlichen wird somit auf zwei Ebenen verfolgt: einerseits zugunsten der Behörde und in Bezug auf die faktische Komplexität (inklusive begrenzter finanzieller wie personeller Ressourcen) der von ihr auszuübenden Kontrolle, andererseits zugunsten des Verantwortlichen hinsichtlich des (idealerweise) proaktiven Hinwirkens auf eine weniger komplexe Systemarchitektur mit nachvollziehbaren Datenflüssen.[450]

cc) Management von Ungewissheit

Neben der Verringerung von Komplexität im Verhältnis zwischen Verantwortlichen und Aufsichtsbehörden sowie zwischen Verantwortlichen und ihren eigenen innerorganisatorischen Abläufen und Verarbeitungsumständen, könnte eine weitere Dimension der Komplexitätsreduktion durch Verantwortlichkeitszuschreibung darin bestehen, die dem Datenschutz inhärente Ungewissheit zu reduzieren. Diese Überlegung lässt sich auf zwei Ebenen anstellen und damit von zwei unterschiedlichen Enden denken.

(1) Risikobezogene Ungewissheit

Zunächst besteht eine grundlegende Ungewissheit hinsichtlich des Risikos durch den Einsatz von (insbesondere neuen) Verarbeitungstechnologien, die zu reduzieren bzw. zumindest handhabbar zu machen die Ausgestaltung des Verantwortlichen in der DSGVO bezwecken könnte.[451] Wie bereits beschrieben, sind die denkbaren mit der Verarbeitung personenbezogener Daten einhergehenden Gefahren zu dem Zeitpunkt, an dem das private Datenschutzrecht ansetzt,

---

[449] Vgl. die allgemeinen Rechenschafts- und Nachweispflichten in Art. 5 Abs. 2 und Art. 24 Abs. 1 S. 1 DSGVO sowie die konkreten Nachweispflichten, wie sie etwa Art. 7 Abs. 1 DSGVO für die Einwilligung des Betroffenen statuiert.

[450] Dabei versteht es sich von selbst, dass die zweite Ebene letztlich ebenso den Behörden zugutekommt, wenn der Verantwortliche seine Datenschutzkonformität erleichtert und leichter belegen kann.

[451] Für weitere Beispiele des gesetzlichen Umgangs mit Ungewissheit und Risiko, etwa im Atom- oder Gentechnikrecht, siehe *Hoffmann-Riem*, in: Röhl, Wissen – zur kognitiven Dimension des Rechts, S. 159 (174 ff.).

noch sehr abstrakt und ungewiss: einerseits, weil durchaus konkret benennbaren Gefahren auf temporaler Ebene sehr früh entgegengetreten wird durch Maßnahmen der Risikominimierung,[452] andererseits, weil noch gar nicht abschätzbaren Gefahren entgegengetreten werden muss, deren Ausmaß wie auch Eintrittswahrscheinlichkeit ungewiss sind. Vor allem in letzterem Fall ist zur Vorbeugung und Vorsorge von solcherlei Gefahren also vor dem Einsatz risikominimierender Maßnahmen zunächst die Ermittlung von Risikopotentialen, also die Verringerung von Unsicherheit über Existenz, Ausmaß und Eintrittswahrscheinlichkeit von Gefahren, nötig. Auch diesen regulatorischen Zweck verfolgt der Verordnungsgeber durch Inpflichtnahme des Verantwortlichen, der als unmittelbar beteiligter Akteur im Zweifel das bessere Verständnis und die besseren Einblicke in die mit seinem Handeln einhergehenden Gefahren und das Entwickeln denkbarer Gegenmaßnahmen hat. *Binns* bringt dies gut auf den Punkt, wenn er sagt:

„While Member State supervisory authorities may reasonably claim superior understanding of the data protection principles, they may not have a superior understanding of the latest personal data processing techniques, nor the most appropriate privacy-enhancing technologies."[453]

Dem Verantwortlichen wird diese Aufgabe etwa im Rahmen der von ihm durchzuführenden, oben bereits beschriebenen, Datenschutzfolgeabschätzung nach Art. 35 Abs. 1 DSGVO übertragen. Dieses Instrument verpflichtet ihn zu einer strukturierten Ergründung und Bewertung der mit seinem Verarbeitungsvorhaben einhergehenden Risiken sowie, soweit das Ergebnis dieser Schritte danach verlangt, zu der Erarbeitung, Implementation und Dokumentation von Maßnahmen, die zur Minimierung dieser Risiken führen. Davon umfasst sind nicht nur rechtliche Risiken, also die proaktive Beurteilung der Rechtmäßigkeit der geplanten Verarbeitungspraktik(en), sondern auch technische Risiken für Grundrechte und Interessen der Betroffenen. Durch den hier vorgesehenen Austausch zwischen Verantwortlichen und Aufsichtsbehörden ergibt sich ein Element der Wissensgenerierung[454], das über das Verhältnis zwischen diesen beiden Stellen hinausreicht: Durch Konsultation der Aufsichtsbehörde wird diese frühzeitig auf neu entstehende Risiken und – im Idealfall – erste vom betreffenden Verantwortlichen ersonnene Gegenmaßnahmen aufmerksam und kann dieses neugewonnene Wissen zukünftig generalisierend in ihre Kontroll-

[452] Beispielsweise im Bereich der Datensicherheit, wenn Art. 32 DSGVO dazu verpflichtet, risikoadäquate Maßnahmen zu ergreifen, die die Wahrscheinlichkeit des Eintreffens späterer Sicherheitsrisiken (sei es durch das, ggf. böswillige, Eingreifen Dritter oder durch interne, organisatorische Fehler) verringern.

[453] *Binns*, International Data Privacy Law 2017, 22 (32).

[454] Generell zu den Möglichkeiten der Wissensgenerierung zum Zwecke der Verringerung des Nichtwissens siehe *Dreyer*, Entscheidungen unter Ungewissheit im Jugendmedienschutz, S. 45 f.

wie auch Beratungsaufgaben[455] einfließen lassen. Dieses Wissen kann sowohl positiv genutzt werden, indem erfolgreiche Abschätzungen und Maßnahmen sich weiterverbreiten, aber auch negativ, indem neue Verarbeitungsvorgänge und Techniken, für die es zum jeweiligen Zeitpunkt schlicht noch keine hinreichenden Risikominimierungsmaßnahmen gibt, zunächst – für den konkreten Verantwortlichen und für die Allgemeinheit – verboten werden.[456] Diese Art der Steigerung von Handlungswissen ist dem Verwaltungsrecht insgesamt nicht fremd: Insbesondere der Einsatz von Instrumenten der regulierten Selbstregulierung[457] kann als Reaktion auf staatliche Wissensdefizite verstanden werden.[458]

Mit Blick auf den Wortlaut des Art. 35 DSGVO erscheint eine solche Wirkung zunächst kontraintuitiv: Die Durchführung einer Datenschutzfolgenabschätzung ist nach Abs. 1 S. 1 erst dann verpflichtend, wenn bereits ein „hohes Risiko für Rechte und Freiheiten natürlicher Personen" infolge der Verarbeitung feststeht. Als zentrale Anhaltspunkte, ob der Einsatz bestimmter Technologien und Verarbeitungspraktiken ein solches Risiko aufweist, stellen mit Abs. 4 und 5 der Norm die Aufsichtsbehörden sog. Blacklists und Whitelists zusammen, in die jene Praktiken aufgenommen werden, deren Einsatz auf jeden respektive gar keinen Fall die Durchführung einer Datenschutzfolgenabschätzung benötigen.[459] Beide Tatsachen lassen zunächst vermuten, dass Risiken notwendigerweise bereits (verantwortlichen- und bzw. oder behörden-) bekannt sein müssen, weil sonst schon keine Kenntnis des Verantwortlichen um seine Durchführungspflicht vorliegen und erst recht kein Tätigwerden der Behörde in Form der Aufnahme auf eine Blacklist geschehen sein kann. Ein solches Verständnis des Instruments verkennt aber, dass Sinn und Zweck der Norm nur dann erreicht werden können, wenn vor der eigentlichen Folgenabschätzung im engeren Sinne – also der Kalkulation der Risiken, der Abschätzung der Notwendigkeit von zu ergreifenden Maßnahmen und der Erfolgsabschätzung

---

[455] Gem. Art. 57 Abs. 1 lit. d DSGVO obliegt es den Aufsichtsbehörden nicht nur, die Einhaltung der DSGVO-Vorschriften zu überwachen und kontrollieren, sondern auch in Dialog mit Compliance-bereiten Verantwortlichen zu treten und diese bei ihren Anstrengungen zu beraten und unterstützen und für die Gefahren ihrer Verarbeitungsvorgänge zu sensibilisieren.

[456] Vgl. Art. 36 Abs. 2 S. 1 a. E., der auf die Befugnisse der Aufsichtsbehörden in Art. 58 DSGVO verweist.

[457] Siehe hierzu die Ausführungen *supra* bei 1. c).

[458] Vgl. *Eifert*, in: Hoffmann-Riem, Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, S. 137 (138 f.).

[459] Die DSK hat federführend für die deutschen Aufsichtsbehörden zumindest eine solche Liste von Verarbeitungstätigkeiten, für die die Durchführung einer DSFA zwingend nötig ist, aufgestellt (https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf) und dabei auf die in *Art. 29-Datenschutzgruppe*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679 aufgestellten Kriterien zurückgegriffen. Link zuletzt abgerufen am 14.01.2022.

ggf. gewählter Maßnahmen – von jedem Verantwortlichen bereits eine kleine Abschätzung dahingehend vorgenommen werden muss, zu ermitteln, ob das Risiko die von Art. 35 Abs. 1 S. 1 DSGVO gesetzte Schwelle zur Aktivierung einer Durchführungspflicht erreicht.[460]

Auch hier ließe sich zudem der oben bereits erwähnte Nachteil anbringen, wonach die Aufsichtsbehörden im Ergebnis wieder zu einem gewissen Grad auf die Richtigkeit der vom Verantwortlichen übermittelten Ergebnisse angewiesen sind. Wie groß das Ausmaß dieser Abhängigkeit ist, hängt davon ab, wie gut die jeweils betroffene Aufsichtsbehörde in der Lage ist, die vom Verantwortlichen überreichte Dokumentation seiner Folgenabschätzung inhaltlich zu durchdringen, nachzuvollziehen und damit letztlich bewerten und kontrollieren zu können.[461] Eine personelle und finanzielle Behördenausstattung, die garantiert, dass Mitarbeiter immer auf dem aktuellen (entwicklungs-)technischen Stand sind, wäre dafür unabdinglich. Eine wichtige Rolle kommt dabei auch dem EDSA als de-facto-Nachfolger der *Art. 29-Datenschutzgruppe* zu. Über diese Einrichtung, in der gem. Art. 68 Abs. 3 DSGVO neben dem EDSB ein Vertreter aus der Aufsichtsbehörde eines jeden Mitgliedstaats sitzt,[462] kann sichergestellt werden, dass von einzelnen Aufsichtsbehörden erlangtes Wissen breitflächig an die Aufsichtsbehörden der übrigen Mitgliedstaaten weitervermittelt wird. Der Erfolg dieses Instruments zur Ungewissheitsreduzierung hängt daher vom Finden eines idealen Ausgleichs ab: Haben die Behörden zu wenig eigenes Wissen und verlassen sich zu sehr auf die Eigenfähigkeiten der Verantwortlichen, geht ihnen die Fähigkeit einer wirksamen Kontrolle ab. Legen sie zu viel Fokus auf eigene innerbehördliche Wissensgenerierung, um möglichst wirksam kontrollieren zu können, bringen sie sich letztlich um den Vorteil der delegierten Wissensgenerierung, den das Instrument gerade mit sich bringen sollte.

(2) Compliancebezogene Ungewissheit

Weniger offensichtlich, aber ebenfalls von Bedeutung, ist die Ebene der Ungewissheitsbeseitigung durch den Verantwortlichen hinsichtlich der eigenen

---

460 Vgl. *Raso*, Innovating in uncertainty: effective compliance and the GDPR, S. 10, der von „mini-impact assessments" spricht.

461 So auch *Eifert*, in: Hoffmann-Riem, Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, S. 137 (138 f.): „Die verstärkte Einbeziehung privater Akteure und gesellschaftlicher Regulierungsmechanismen […] erschließt zwar prinzipiell auch deren Informationsverarbeitungskapazität und Wissensbestände für die Problembearbeitung, sie hinterläßt aber auf staatlicher Seite das Problem, trotz mangelnden Wissens geeignete Vorgaben zu formulieren, Rahmenbedingungen setzen oder Ergebnisse beurteilen zu müssen."

462 Dem deutschen föderalen Sonderweg mit einer eigenen Aufsichtsbehörde in jedem Bundesland wird durch Art. 68 Abs. 4 DSGVO Rechnung gezollt, nach welchem auch hier ein einzelner nationaler Vertreter bestimmt werden soll.

Ungewissheit über die konkrete Bedeutung von bestimmten DSGVO-Pflichten und die Frage, wann sie als erfüllt gelten, wann der Verantwortliche also *compliant*[463] ist und wann nicht. Wie bereits beschrieben, führt die grundlegende Offenheit und Abstraktheit vieler Pflichten und Prinzipien einerseits zu der gewollten Flexibilität und erhofften Zukunftsoffenheit, bringt gleichzeitig aber auch eine Rechtsunsicherheit für Normadressaten mit sich, solange keine klaren Maßstäbe und Kriterien existieren. Die Ausgestaltung der Verantwortlichkeit versucht dem zu begegnen, indem bspw., ganz in der Tradition der regulierten Selbstregulierung bzw. Co-Regulation,[464] unter anderem den Verantwortlichen selbst viel Spielraum bei ihrer Herangehensweise gelassen wird.[465]

Dieser Optionen- oder Möglichkeitsraum[466] eröffnet sich zunächst bei Pflichten, die ein gewisses Ziel vorgeben, dabei aber dem Verantwortlichen überlassen, wie genau er dieses erreicht. Paradebeispiele dafür sind die Art. 24 Abs. 1 S. 1, 25 Abs. 1 und 32 DSGVO, die hinsichtlich der Sicherstellung und Beweisbarkeit der verordnungsgemäßen Verarbeitung, hinsichtlich Umsetzung der *privacy by design*- und *privacy by default*-Prinzipien sowie hinsichtlich des Ziels der Datensicherheit schlicht „geeignete technische und organisatorische Maßnahmen" verlangen, ohne diese konkret zu benennen oder näher zu spezifizieren.

Interessanter mit Blick auf die ungewissheitsreduzierende Wirkung ist die zweite Ebene: Auch die Konkretisierung der Reichweite derartiger Pflichten, also die Frage, wie umfangreich und wirksam bspw. die ergriffenen Maßnahmen sein müssen oder welche Abwägungen zugunsten oder zulasten einer konkreten Verarbeitung ausgehen, kann vom Verantwortlichen mit vorgenommen werden, dieser also aktiv dazu beitragen, seine eigene Ungewissheit zu verringern. Eine solche Wirkung lässt sich zunächst am mehrmals in der DSGVO aufgeführten Begriff des „Stands der Technik"[467] festmachen. Dieser verweist dynamisch auf die zum jeweiligen Zeitpunkt bestmöglichen in der Praxis erprobten Praktiken und kann daher durch den Verantwortlichen selbst mitgeprägt werden. Verstärkt wird diese Möglichkeit zur eigenverantwortlichen Normkonkretisierung und damit Verringerung eigener Ungewissheit durch die von der DSGVO angebotenen Möglichkeiten kollektiver Standardisierung in Form von etablierten Verhaltensregeln (sog. Codes of Conduct) und Zertifizierungen der eigenen Maßnahmen und Verarbeitungstätigkeiten. Art. 40 und 42 DSGVO verfolgen neben dem Ziel der erhöhten Transparenz für Betroffene[468] nämlich auch zwei weitere Zwecke: einerseits eine gesteigerte Bereitschaft auf Verantwortlichenseite, die

[463] Zum Begriff der Compliance unter der DSGVO siehe *Thode*, CR 2016, 714 (714 ff.).

[464] Beides zu verstehen als Gegenbegriff zur bloßen Selbstregulierung dergestalt, dass die durch den Normadressaten selbst gewählten Regulierungsmaßnahmen zwingend, überprüfbar und sanktionierbar sind.

[465] Siehe dazu ausführlich *supra* bei B. I. 1. c.

[466] Vgl. *Hoffmann-Riem*, Innovation und Recht, Recht und Innovation, S. 368 ff.

[467] Siehe etwa Art. 25 Abs. 1 S. 1, 32 Abs. 1 und Erwägungsgründe 78 und 91 der DSGVO.

[468] Vgl. *Martini*, NVwZ-Extra 2016, 1 (9).

eigenen Verarbeitungsumstände erprobten und als sicher und in gewissem Ausmaß datenschutzkonform abgesegneten Standards anzupassen, indem in diesen Fällen Privilegierungen bei der Kontrolle durch Aufsichtsbehörden in Aussicht gestellt werden.[469] Andererseits können Verantwortliche insbesondere im Rahmen der Verhaltensregeln gem. Art. 40, vermittelt über eine Mitgliedschaft in Wirtschafts- und Branchenverbänden oder anderen Vereinigungen,[470] aktiv an der Standardisierung mitwirken und so selbst für Konkretisierung und Präzisierung unbestimmter und abstrakter Normen sorgen und eigene, innovative Schutzansätze und Verarbeitungstechniken für die breite Masse an Verantwortlichen etablieren.[471] Damit einher geht im Erfolgsfall eine (zumindest sektoral) gestiegene Rechtssicherheit und damit verringerte Ungewissheit nicht nur für den einzelnen Verantwortlichen, sondern für das Gros der Normadressaten.[472] Diese Rechtssicherheit kann sogar im gesamten Unionsgebiet eintreten, wenn gem. Abs. 9 der Norm die Kommission bestimmte Verhaltensregeln genehmigt und als Durchführungsrechtsakt mit allgemeiner Gültigkeit iSd Art. 291 AEUV beschließt.[473]

Der ambitionierte Ansatz der DSGVO, im Interesse technischer und innovativer Anpassungsfähigkeit[474] viele Pflichten und Bestimmungen abstrakt und ausfüllungsbedürftig zu gestalten, geht also notwendigerweise mit einem gewissen Grad an Rechtsunsicherheit einher.[475] Durch die Nutzung unter anderem der oben beschriebenen Instrumente regulierter Selbstregulierung überträgt der Verordnungsgeber die Verantwortung für die fortwährende Verringerung dieser Ungewissheit in Teilen den Verantwortlichen als Normadressaten selbst.[476] Der

---

[469] Art. 42 Abs. 4 DSGVO stellt zwar für den Fall der Zertifizierungen klar, dass eine solche nicht die Verantwortung des Verantwortlichen als solche mindert und ihn nicht von (auch nicht bloß manchen) seinen Pflichten befreit. Im Rahmen von etwa Art. 24 Abs. 3 und 32 Abs. 3 können übernommene Verhaltensregeln und genehmigte Zertifizierungsverfahren aber wichtige Faktoren bei der Beurteilung eines gelungenen Compliance-Nachweises sein. Vgl. *Martini*, in: Paal/Pauly, DSGVO/BDSG, Art. 24 DSGVO Rn. 45 zur Einordnung dieser Privilegierungen in die verwaltungsrechtliche Ermessensdogmatik.

[470] Für die Voraussetzungen der Anerkennung solcher Verbände und Vereinigungen siehe *European Data Protection Board*, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, S. 11 f. Vgl. ferner *Bergt/Pesch*, in: Kühling/Buchner, DSGVO/BDSG, Art. 40 DSGVO Rn. 11 ff.

[471] Vgl. *Roßnagel*, in: Simitis u. a., DSGVO/BDSG, Art. 40 DSGVO Rn. 2; siehe auch *Reifert*, ZD 2019, 305 (305), nach der Verhaltensregeln ein geeignetes Mittel darstellen, „die vielzähligen unbestimmten Vorschriften der DS-GVO in der Praxis handhabbar zu machen".

[472] Vgl. *Pohl*, PinG 2017, 85 (88).

[473] Vgl. hierzu die Ausführungen bei *Bergt/Pesch*, in: Kühling/Buchner, DSGVO/BDSG, Art. 40 DSGVO Rn. 49 ff.

[474] Vgl. *Martini*, NVwZ-Extra 2016, 1 (7 f.).

[475] Besonders kritisch *Roßnagel*, in: Simitis u. a., DSGVO/BDSG, Art. 40 DSGVO Rn. 1: „Viele Regelungen der DSGVO sind hochabstrakt und zu allgemein, um in einem rechtsstaatlichen Verfahren vollzogen und sanktioniert werden zu können."

[476] *Nolde*, PinG 2017, 114 (116) spricht bei solchen Möglichkeiten von Maßnahmen der „Eigensicherung". Einen Überblick über das komplexe Geflecht verschiedener Konkretisie-

Erfolg dieses Vorgehens hängt dabei, wie bei den meisten hier beschriebenen Erwartungen an die Steuerungswirkung der Verantwortlichkeitszuschreibung, nicht zuletzt davon ab, wie das Zusammenspiel zwischen Verantwortlichen, kollektiven Standardsetzungsinstanzen und Aufsichtsbehörden in der Praxis abläuft. Hier bedarf es zwingend gegenseitigen Vertrauens und Respekts und eines Vorgehens der Behörden, das im Zweifel die Beratung und konstruktive Unterstützung der Verantwortlichen bei seinen Anstrengungen eher in den Fokus stellt als das vorschnelle Sanktionieren.[477] Hinsichtlich der Anerkennung von Vereinigungen und ihren Verhaltensregeln sowie möglicher Zertifizierungsstellen bedarf es funktionierender, effizienter und unbürokratischer Mechanismen und Prozesse.[478]

b) Verantwortlichkeitszuschreibung als Form von Risikomanagement

Neben den beschriebenen Wirkungen der Verantwortlichkeitszuschreibung als Management von Komplexität liegt eine weitere erhoffte Wirkung im Management von (Verarbeitungs-)Risiken. Da im Kern des Datenschutzrechts das Ziel steht, die mit Datenverarbeitungen einhergehenden oder in Aussicht stehenden Gefahren einzudämmen und ihnen vorzusorgen, liegt hier eine zentrale Wirkung, deren Erreichung der Verordnungsgeber sich durch die Auswahl und Pflichtenbelegung des Verantwortlichen erhofft.

Insbesondere die Ausgestaltung der verschiedenen risikozentrierten Pflichten in Form ihrer Reichweite ist dabei von Bedeutung. Kurz gesagt: Aufgrund der bereits mehrfach beschriebenen Abstraktheit der Gefahren, denen vorgebeugt bzw. die eingedämmt werden sollen, und aufgrund der teilweise lange bestehenden Ungewissheit über ihre konkrete Erscheinung und Eintrittswahrscheinlichkeit, kann von Verantwortlichen nicht verlangt werden, Risiken gänzlich zu verhindern. In keinem Lebensbereich kann dem Einzelnen (weder privat noch von staatlicher Seite) garantiert werden, dass jegliche Risiken komplett ausgeräumt werden, ein gewisses Restrisiko gehört notwendigerweise zur Natur

---

rungsleistungen, das die DSGVO darüber hinaus von weiteren Akteuren verlangt, geben *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 253 ff. Vgl. auch *European Data Protection Board*, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, S. 9: „Codes can provide much needed confidence and legal certainty" und „could decrease the level of reliance that controllers and processors may sometimes place upon data protection supervisory authorities to provide more granular guidance for their specific processing activities."

[477] Vgl. *Binns*, International Data Privacy Law 2017, 22 (33): „This ought to create conditions in which responsibility is more fairly apportioned and trusting relationships between regulators and data controllers can be built." Ähnlich *Martini*, NVwZ-Extra 2016, 1 (9): „Datenschutzkontrolle vollzieht sich in diesem Leitbild nicht gegen, sondern mit den betroffenen Unternehmen."

[478] Kritisch gegenüber der Wirkung von Art. 40 DSGVO etwa *Wolff*, ZD 2017, 151 (154).

des Menschen als soziales Wesen.[479] So führt auch das BVerfG bzgl. Risiken der technologischen Entwicklungen im Bereich der Datenverarbeitungen aus: „Es ist nicht Aufgabe des Verfassungsrechts, solche Entwicklungen insgesamt aufzuhalten und alle Vor- und Nachteile der damit verbundenen Folgen zu neutralisieren."[480] Angestrebt wird daher auch im Datenschutzrecht allein die Eindämmung und Minimierung von Risiken, und dies auf unterschiedlichem Wege.

Eine Stellschraube betrifft die Frage, welches Maß der Verantwortliche leisten muss, um seiner Pflicht bzw. seinen Pflichten Genüge geleistet zu haben. Hat ein Verantwortlicher alles in seiner Macht Stehende getan und hat sich ein Risiko dennoch realisiert, so haftet er für dieses weder in Form eines Bußgeldes,[481] noch im Wege des Schadensersatzes[482]. Wie bspw. das bereits erwähnte Instrument der Datenschutzfolgenabschätzung aber zeigt, kommt es letztlich auf den Anknüpfungspunkt bzw. das konkret vorzuwerfende Fehlverhalten an und kann ihm dann möglicherweise vorgeworfen werden, eine Verarbeitung oder eine für diese notwendige Technologie eingesetzt zu haben, deren Risiken (zu diesem Zeitpunkt) schlicht zu hoch sind bzw. für deren Risiken er absehbar keine hinreichenden Gegenmaßnahmen aufweisen kann.[483] Ignoriert oder verkennt er das hohe Risiko von vornherein und unterlässt die Durchführung einer Datenschutzfolgenabschätzung, so kann auch das ihm vorgeworfen werden.[484]

Gleiches gilt, wenn er generell keine Anstrengungen zur Risikominimierung unternommen hat oder seine Anstrengungen nicht ausreichend waren. Hier kommt es zur steuerungslenkenden Wirkung entscheidend darauf an, die richtige Mitte zwischen zu weitreichenden Pflichten, die den Verantwortlichen überfordern und abschrecken, und zu „kurzen" Pflichten, die das risikominimierende Potential des Verantwortlichen nicht ausnutzen, der Bedeutung der gefährdeten Grundrechte und Interessen nicht gerecht werden, und somit eine Risikoeindämmung ausreichen lassen, die vermeidbar und unangemessen ist.

---

[479] Anders aber *Dammann*, ZD 2016, 307 (314 f.), der dem Datenschutzrecht, in Abgrenzung zu etwa Straßenverkehrs- und Lebensmittelrecht, den Anspruch unterstellt, den perfekten Schutz des Betroffenen zu gewährleisten.

[480] BVerfG, Beschluss v. 06.11.2019, 1 BvR 16/13 (Recht auf Vergessen I), Rn. 104.

[481] Ob hier das Verschulden materiell eine zwingende Voraussetzung ist und somit mindestens Fahrlässigkeit vorliegen muss, ist umstritten. Ablehnend dazu etwa *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 83 DSGVO Rn. 35. Überzeugender scheint es mit Blick auf den Wortlaut von lit. b der Norm aber, ein solches Verständnis anzunehmen. So auch *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 83 DSGVO Rn. 14; *Brodowski/Nowak*, in: BeckOK Datenschutzrecht, § 41 BDSG Rn. 17.

[482] Hier muss er aber gem. Art. 82 Abs. 3 DSGVO darlegen können, dass er alle ihn treffenden Sorgfaltspflichten erfüllt und in keiner Weise fahrlässig gehandelt hat. Vgl. *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 82 DSGVO Rn. 54. siehe auch *Wybitul* u. a., NJW 2018, 113 (116 f.); *Wybitul* u. a., ZD 2018, 202 (203); *Paal*, MMR 2020, 14 (17 f.).

[483] Vgl. die Kontroll- und Abhilfekompetenzen der Aufsichtsbehörde nach Art. 36 Abs. 2 S. 1 i. V. m. Art. 58 Abs. 2 lit. f DSGVO.

[484] Vgl. Art. 83 Abs. 4 lit. a DSGVO.

Auch hier lassen sich einige der oben genannten Normen nennen, um aufzuzeigen, wie die DSGVO versucht, diesen Mittelweg zu finden und beschreiten. Das bereits erwähnte Kriterium des „Stand(es) der Technik" etwa erhebt die jeweils aktuell der breiten Masse an Verantwortlichen in einem Bereich verfügbare und bewährte Technik zum entscheidenden Maßstab.[485] Gleichzeitig werden Überlegungen fruchtbar gemacht, die entfernt an polizeirechtliche Grundsetze angelehnt sind und etwa Risiken für Betroffene (berechnet auf Basis der Schwere und Eintrittswahrscheinlichkeit einer, häufig noch nicht konkret benennbaren, Gefahr)[486] mit einem durch Abhilfemaßnahmen erwarteten Ausmaß an Minimierung in Verhältnis setzen: Je schwerer die Verletzung von Betroffenengrundrechten bei Realisierung eines Risikos und je höher die Wahrscheinlichkeit eines solchen Umschlagens, desto erfolgsversprechender müssen die gewählten Abhilfemaßnahmen sein, um die entsprechende Verarbeitung datenschutzkonform durchzuführen.[487]

c) Verantwortlichkeitszuschreibung zur Überwindung von faktischen Rechtsdurchsetzungsdefiziten

Neben der dem Datenschutz aufgrund der technischen Komplexität und steten Entwicklung seiner Regelungsmaterie inhärenten Komplexität ist die Problematik der effektiven Durchsetzung seines Rechtsanspruchs eine der größten und meistdiskutierten.[488] Datenverarbeitungen sind allgegenwärtig, sie geschehen in jeder Sekunde und in jeglichen Lebenslagen, werden von Privatpersonen wie von Unternehmen vorgenommen. Gleichzeitig sind sie flüchtig und finden nahezu ausschließlich in der Sphäre der Verarbeitenden statt. Als zentrale Handlung, an die das Datenschutzrecht anknüpft, sind sie daher naturgemäß schwieriger zu regulieren als andere gefahrenemittierende Handlungen und Gegebenheiten wie bspw. der Betrieb von Atomkraftwerken und Gaststätten oder andere Bereiche

---

[485] Vgl. *Hartung*, in: Kühling/Buchner, DSGVO/BDSG, Art. 25 DSGVO Rn. 21. *Martini*, in: Paal/Pauly, DSGVO/BDSG, Art. 25 DSGVO Rn. 39 ff.; dabei ist der Begriff von den ebenfalls genutzten „allgemein anerkannten Regeln der Technik" sowie dem „Stand von Wissenschaft und Forschung" abzugrenzen. Vgl. *Bartels/Backer*, DuD 2018, 214 (215 f.); *Seibel*, NJW 2013, 3000 (3000 ff.).

[486] *Petri*, in: Simitis u. a., DSGVO/BDSG, Art. 24 DSGVO Rn. 3 weist hier zurecht darauf hin, dass die stets einhergehende Unsicherheit über wichtige Sachverhaltsumstände einen großen Unterschied zum polizeirechtlichen Risikobegriff darstellt. Die Begriffe werden bisweilen dennoch gleichgesetzt. Siehe etwa *Martini*, in: Paal/Pauly, DSGVO/BDSG, Art. 24 DSGVO Rn. 28 f.

[487] Vgl. Art. 24 Abs. 1 S. 1, 25 Abs. 1 und 32 Abs. 1 DSGVO, die jeweils die „unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen" als ein relevantes Kriterium für die zu treffenden organisatorischen und technischen Maßnahmen aufführen.

[488] Siehe speziell zur Schwierigkeit der Durchsetzung von Regulierungen der online stattfindenden Datenflüsse *Thierer*, Harv. J. Law Public Policy 2013, 410 (424 ff.). Empirische Erkenntnisse zum Vollzugsdefizit finden sich bei *Lepperhoff* u. a., DuD 2012, 195 (195 ff.).

des Wirtschaftsverwaltungsrechts. Anders als diese verfolgt das Datenschutzrecht zudem (nicht zuletzt aufgrund der im Vergleich zu den dortigen Materien weitaus abstrakteren Gefahren der Regelungsmaterie „Datenverarbeitung“[489]) einen Regulierungsansatz, der Datenverarbeitungen als regulierte Handlungen nicht von einer Behördenbeteiligung in Form einer Genehmigung oder anderen „wirtschaftsverwaltungsrechtlichen Eröffnungsinstrumenten“[490] abhängig macht.[491] Verantwortliche benötigen eine Rechtsgrundlage für ihre Datenverarbeitungen, sind aber nicht davon abhängig, diese behördenseitig legitimieren zu lassen – die Rechtmäßigkeit liegt bei Vorliegen und Beweisbarkeit einer Rechtsgrundlage *ipso jure* vor und wird nicht durch Verwaltungshandeln herbeigeführt. Wie bereits mehrfach angeklungen, erschwert dies auf faktischer Ebene die Kontrolle und Überprüfbarkeit der Einhaltung datenschutzrechtlicher Normen immens.[492] Mag dies zumindest teilweise auch daran liegen, dass sich eine gesamtgesellschaftliche und insbesondere unternehmerische Sensibilität für datenschutzrechtliche Grundprinzipien erst zu spät herausgebildet hat und sich daher viele heute klar als problematisch erkannte Praktiken bereits ungestört entwickelt und verfestigt hatten, so ist ein großer Teil doch auch der Materie selbst, insbesondere ihrer Durchdringung des Alltags, ihrer Flüchtigkeit und Abstraktheit geschuldet. Aufsichtsbehörden können – und sollen[493] – nicht jeden einzelnen Verstoß mitbekommen und verhindern, während Betroffene häufig kaum in der Lage sind, einen Verstoß überhaupt zu erkennen. Mit der Figur des Verantwortlichen und den bei ihrer Ausgestaltung gewählten Instrumenten geht daher auch die Erwartung an bzw. Hoffnung auf eine Abschwächung dieses inhärenten Rechtsdurchsetzungsdefizits einher.

Die nun schon mehrfach beschriebene Mischung an Regelungs- und Steuerungsinstrumenten, in der insbesondere Instrumente der regulierten Selbstregulierung und ähnliche die Innovationskräfte und Eigenmotivation der

---

[489] Hier zeigt sich einmal mehr die Bedeutung von Datenschutz als Vorfeldschutz. Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, S. 108 ff.; *Poscher*, in: Miller, Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, S. 129 (133 f.).

[490] *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (17 f.), der zudem prägnant ausführt: „Anders als beim gleichnamigen Institut des Wirtschaftsverwaltungsrechts geht es dabei aber nicht um eine behördliche Erlaubnis zur Aufhebung eines (dilatorischen) gesetzlichen Verbots nach einer Prüfung bestimmter Erlaubnisvoraussetzungen, sondern es wird ein Regel-Ausnahmeverhältnis beschrieben, das im Datenschutzrecht grundrechtlich durch Art. 8 GRCh influenziert und in Art. 6 DSGVO einfachrechtlich ausgestaltet ist.“

[491] Dies war unter der DSRL noch anders, da deren Art. 18 ff. allgemein geltende Meldepflichten statuierten, die jedoch nahezu keine praktische Wirkung zeigten. Vgl. *Karg*, in: Simitis u. a., DSGVO/BDSG, Art. 35 DSGVO Rn. 4.

[492] Vgl. *Schipper*, Neue Instrumente des Datenschutzrechts für das Verhältnis zwischen Privatperson und Unternehmen in der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika, S. 4 ff.; *Kosyra/Domurath*, in: Micklitz/Joost/Reisch/Zander-Hayat, Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt, S. 135 (135 ff.).

[493] Vgl. *Rademacher*, JZ 2019, 702 (710).

Verantwortlichen stimulierende Instrumente dominieren, adressiert diese Wirkrichtung, indem häufig einer indirekten, abgestuften Kontrolle der Vorzug gegenüber einer unmittelbaren Kontrolle und Überwachung der Verarbeitungstätigkeiten gegeben wird.[494] Insbesondere die Datenschutzfolgenabschätzung muss hier zum wiederholten Male als Paradebeispiel herangezogen werden: Als einzelne Pflicht, deren Einhaltung zunächst unmittelbar kontrolliert wird,[495] beinhaltet sie die Durchführung zahlreicher weiterer Pflichten, deren Erfüllung dem Verantwortlichen einigen Spielraum lässt, letztlich aber in Gänze dokumentiert und der Aufsichtsbehörde vorgelegt werden muss. Indem die Behörde nun nur noch die ihr vorgelegte, gebündelte und bereits aufbereitete, Selbstkontrolle und -evaluierung des Verantwortlichen überprüfen muss, wird die Kontrolldichte theoretisch um einiges erhöht.

Denkt man diesen Gedanken etwas weiter und abstrahiert ihn von den konkreten Pflichten, zeigt sich eine weitere grundlegende Methode, mit welcher die DSGVO der Allgegenwärtigkeit und Flüchtigkeit von einzelnen Datenverarbeitungen entgegenzuwirken versucht: eine Verschiebung des Regulierungs- und Kontrollfokus weg von der isolierten Verarbeitung als zentrales Handlungsobjekt und hin zu den Prozessen, Architekturen und anderweitigen Umgebungen, in welche sie eingebunden ist. Das ist zunächst kaum verwunderlich, ergeben sich doch die denkbaren Gefährdungen schon notwendiger Weise nicht (nur) aus der Verarbeitung als solcher, sondern (auch) aus ihrem Zusammenspiel mit Umwelt und Umgebung. So beispielsweise, wenn im Rahmen der Datensicherheit[496] Vorsorge gegen etwaige Angriffsszenarien durch Dritte oder anderweitigen unbefugten Zugriff durch Angestellte des Verantwortlichen, aber auch gegen ungewollten Datenverlust geleistet, kurz gesagt also mit Art. 32 Abs. 1 lit. b DSGVO die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der relevanten Systeme und Dienste garantiert werden muss.[497] Der Paradigmenwechsel innerhalb des Ansatzes der DSGVO geht jedoch darüber hinaus und nimmt das

---

[494] Zur begrenzten Wirksamkeit sog. „menschlicher Stichproben" zur Kontrolle von Rechtsunterworfenen siehe *Rademacher*, JZ 2019, 702 (703).

[495] Freilich besteht auch hier ein gewisses Durchsetzungsdefizit, weil die Aufsichtsbehörde zunächst Anlass haben muss, die Notwendigkeit der Durchführung einer solchen Abschätzung zu vermuten. Die Existenz eines unabhängigen Datenschutzbeauftragten beim Verantwortlichen soll dieses Problem abmildern, ist aber letztlich mit dem gleichen Makel belegt: Was, wenn der Verantwortliche *dieser* Pflicht, einen Datenschutzbeauftragten zu bestellen, ebenfalls nicht nachkommt? In diesem Teufelskreis zeigt sich, dass auch regulierte Selbstregulierung im Ausgang oder am Ende der Möglichkeit einer unmittelbaren Kontrolle und Sanktionsmöglichkeit bedarf, um wirken zu können.

[496] Vgl. Art. 32 DSGVO.

[497] Siehe zu diesen Schutzzielen *Jandt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 32 DSGVO Rn. 22 ff.; *Mantz*, in: Sydow, DSGVO, Art. 32 DSGVO Rn. 14 ff. ausführlicher zum Verhältnis zwischen den klassischen Schutzzielen der IT-Sicherheit und den Zielen der Datensicherheit im Datenschutzrecht *Petrlic/Sorge*, Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, S. 9 ff.

Verarbeitungsumfeld ganzheitlich in den Blick. Geht man davon aus, dass in den meisten (jedenfalls potenziell großflächig gefährdungsreichen und damit relevanten) Verarbeitungsszenarien die einzelne Verarbeitung in derselben Form und denselben Gesamtumständen replizierbar ist und nicht vom Einzelfall, sondern der Gestaltung der zu ihr hinführenden Strukturen und Prozesse abhängig ist, erscheint dies nur sachgemäß. Die Strukturen und Prozesse beim Verantwortlichen sind im Gegensatz zur Verarbeitung selbst weit weniger flüchtig, sondern grundsätzlich verstetigt,[498] und dadurch leichter der Kontrolle zugänglich. Dabei ist der ganzheitliche Fokus so zu verstehen, dass – ganz der Formulierung der „technischen und organisatorischen Maßnahmen" in bspw. Art. 24 Abs. 1 S. 1, 25 Abs. 1, 32 Abs. 1 DSGVO folgend – neben der technischen Verarbeitungs- und Unternehmensarchitektur auch die organisatorische und damit nicht zuletzt menschlich-soziale Ebene umfasst ist. So gehört neben der tatsächlichen Implementation von Maßnahmen etwa (unterstützt durch den ggf. verpflichtend, ansonsten immer auch freiwillig, zu bestellenden Datenschutzbeauftragten) auch die generelle wie auch fallbezogene Schulung und Sensibilisierung von Angestellten und Mitarbeitern, und damit die Steigerung der intrinsischen Motivation pro Datenschutz, speziell zur Verantwortung des Verantwortlichen. Eine bloß schematische Umsetzung von vermeintlichen Compliance-Maßnahmen *by the numbers* kann im Falle riskanter Verarbeitungstätigkeiten schon als nicht ausreichend erachtet werden, wenn nicht ein umfassendes und tatsächlich implementiertes Konzept bei allen Beteiligten beim Verantwortlichen dahintersteht.[499]

Dabei zeigt diese Methode der verantwortlicheninternen Bewusstseinsschärfung für den Datenschutz bereits, dass auch die eben beschriebenen „moderneren" Steuerungsinstrumente nur dann funktionieren können, wenn sie dem Verantwortlichen hinreichend Anreize zu ihrer Befolgung setzen. Auch in dieser Hinsicht bietet die DSGVO ein breites Portfolio. Der klassischste und vermeintlich weiterhin effektivste Anreiz sind die in Art. 83 DSGVO normierten Bußgelder – nicht nur in der ersten Zeit nach Wirksamwerden der Verordnung im Mai 2018 kam kaum eine Berichterstattung ohne Erwähnung des nun auf bis zu 20 Millionen Euro bzw. 4 % des weltweit erzielten Jahresumsatzes des Verantwortlichen angestiegenen Bußgeldrahmens aus.[500] Zweifel an der tat-

[498] Wenngleich sie in Zeiten zunehmend agiler Unternehmensführung und wandelnder Geschäftsmodelle ebenfalls an Stetigkeit verlieren. Zu dieser generellen Entwicklung und den resultierenden regulatorischen Herausforderungen siehe *Gürses/van Hoboken*, in: Selinger/Polonetsky/Tene, The Cambridge Handbook of Consumer Privacy, S. 579 (582 ff.).

[499] *Raso*, Innovating in uncertainty: effective compliance and the GDPR, S. 8: „Yet pro forma compliance programs belie the contempt of an organization for the protections of the GDPR."

[500] Die initiale Debatte um dieses Thema sehr gut einordnend *Malte Engeler*, Bußgelder bei Datenschutzverstößen: Angst vor einem Phantom, Netzpolitik vom 22.05.2018 (https://netzpolitik.org/2018/bussgelder-bei-datenschutzverstoessen-angst-vor-einem-phantom/). Zuletzt abgerufen am 14.01.2022.

sächlichen Effektivität ergeben sich aber aus den gerade beschriebenen Rechtsdurchsetzungsdefiziten (ist die Wahrscheinlichkeit einer Sanktionsverhängung eher gering, kann auch ein noch so hohes Sanktionsmaß keine große Anreizwirkung ausüben) sowie aus den Erkenntnissen, nach denen negative Anreize im Vergleich zu ihren positiven Pendants regelmäßig weniger effektiv sind[501] und bei dem Bestreben nach der Steigerung von Abschreckung durch Sanktionssteigerungen der erhoffte Effekt statistisch kaum belegt oder bereits früh ein Plateau zu beobachten ist.[502]

Erwähnenswert sind daher die von der DSGVO mittelbar geförderten positiven Anreizsysteme wie der eng mit dem Selbstdatenschutz und dem Transparenzprinzip verbundene Gedanke von Datenschutz als Wettbewerbsvorteil. Der Grundgedanke dabei ist, dass erkennbar datenschutzkonforme oder gar besonders (überobligatorisch) datenschutzfreundliche Verantwortliche in verschiedensten kommerziellen Bereichen sich aufgrund bewusster Präferenzen der Nutzer von ihren Wettbewerbern absetzen können und deshalb einen zusätzlichen Anreiz erlangen, möglichst datenschutzfreundlich zu agieren. Die Wirksamkeit eines solchen Anreizsystems hängt dabei primär von zwei Grundbedingungen ab: der Bedeutung von Datenschutz als tatsächliche Präferenz von Nutzern bei der Auswahl ihrer Dienste[503] und der hinreichenden Transparenz und Vergleichbarkeit der Datenschutzfreundlichkeit der jeweiligen Dienste. Zumindest der zweiten Voraussetzung leistet die DSGVO durch einige ihrer Verantwortlichenpflichten Vorschub. Die bereits erwähnten Möglichkeiten der Etablierung und Anwendung von Verhaltensregeln und Zertifizierungen nach Art. 40 und 42 DSGVO dienen insbesondere auch dieser erleichterten Erkennbarkeit und Vergleichbarkeit.[504] Fraglich erscheint aber, ob neben dem eher kleinen Kreis derer, für die Datenschutz einen besonderen Stellenwert einnimmt, auch die breite Masse der Gesellschaft (bereits) ein solches Bewusstsein entwickelt hat, um Datenschutz zu einer der Grundlagen ihrer Auswahlentscheidungen zu machen.[505] Jüngste Studien und nichtwissenschaftliche

[501] Vgl. *von Grafenstein*, The Principle of Purpose Limitation in Data Protection Laws, S. 78: „Since potential gains serve better than potential losses as incentive, the legislator should focus more, if it had to choose, on increasing legal certainty enabling entrepreneurs to exploit a competitive advantage than on penalties."

[502] Einen Überblick über die diesbezügliche empirische Studienlage liefert *Spirgath*, Zur Abschreckungswirkung des Strafrechts, S. 30 ff. Demgegenüber dürfte die Sanktionswahrscheinlichkeit den größeren Einfluss auf den Normbefolgungswillen haben als die Sanktionshöhe. Vgl. *Entorf*, in: Ott/Schäfer, Die Präventivwirkung zivil- und strafrechtlicher Sanktionen: Beiträge zum VI. Travemünder Symposium zur ökonomischen Analyse des Rechts vom 25. – 28. März 1998, S. 1 (4 ff.).

[503] Alternativ können hier auch andere Stakeholder wie Investoren relevant werden, deren Entscheidungen für oder gegen eine Beteiligung oder anderweitige Zusammenarbeit mit dem Verantwortlichen von dessen Einstellung zum Datenschutz beeinflusst werden.

[504] Vgl. *Scholz*, in: Simitis u. a., DSGVO/BDSG, Art. 42 DSGVO Rn. 4.

[505] Skeptisch und mit weiteren diese Skepsis untermauernden Nachweisen *Hornung/Hartl*, ZD 2014, 219 (221).

Erfahrungswerte zeigen, dass jedenfalls öffentlichkeitswirksame Datenpannen dazu führen können, dass betroffenen Diensten Nutzer[506] oder Investoren[507] abspringen.

3. Der Anknüpfungspunkt der Steuerung

Eine weitere Unterscheidung der verschiedenen Steuerungsinstrumente des Datenschutzrechts lässt sich dahingehend anstellen, welche unterschiedlichen Wirkrichtungen dabei in den Blick genommen werden. Hier lässt sich eine Unterscheidung heranziehen (und in der Folge erweitern), die *Hermstrüwer* in Bezug auf den objektiv-rechtlichen Schutz im privaten Datenschutzrecht aufgestellt hat.[508] Demnach gilt es, nach dem Anknüpfungspunkt des jeweiligen Instruments zu differenzieren.

a) Anknüpfungspunkt Informationsverwendung

Einige der datenschutzrechtlichen Instrumente knüpfen somit an die *Verwendung* von Daten und Informationen an und versuchen konkret, die Umstände solcher Verwendungen und Möglichkeiten der Datenverarbeiter zu regulieren. Gesteuert wird somit das *Verhalten* der Datenverarbeiter hinsichtlich verschiedener Aspekte der Datenverarbeitung: dem der zu verarbeitenden Daten selbst, und zwar sowohl hinsichtlich des *Ob* (darf überhaupt und in welchem Umfang darf verarbeitet werden?) als auch des *Wie* (welche Maßnahmen müssen für die Daten selbst und das Verarbeitungsumfeld ergriffen werden?), aber auch dem der daraus zu gewinnenden Informationen (und damit mittelbar auf darauf gestützte Folgehandlungen). Wie oben unter A. II. beschrieben, trifft dies zunächst auf grundlegende Datenschutzprinzipien wie das Rechtmäßigkeits- und Zweckbindungsprinzip gem. Art. 5 Abs. 1 DSGVO und die Rechenschaftspflicht in Art. 5 Abs. 2 DSGVO sowie die diese konkretisierenden spezielleren Pflichten zu. Indem beispielsweise von vornherein limitiert wird, zu welchen Zwecken Daten verarbeitet werden dürfen, verringert sich der Handlungsspielraum des Verarbeiters bei der späteren Verwendung dieser – wenn auch durch sein eigenes Handeln in Form der initialen Zweckfestlegung. Durch die vom EU-Verordnungsgeber (und nachgelagert teilweise von den Mitgliedstaaten) getroffene

---

[506] So war im Nachgang zum Cambridge Analytica-Skandal zwar kein Rückgang an Nutzerzahlen, zumindest aber ein spürbarer Rückgang an Nutzerinteraktion auf Facebook zu beobachten. Vgl. *Alex Hern*, Facebook usage falling after privacy scandals, study suggests, The Guardian vom 20.06.2019 (https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows). Zuletzt abgerufen am 14.01.2022.

[507] Siehe hierzu etwa *Nicole Lindsey*, Companies That Experience a Data Breach Will Underperform the Stock Market Over the Long Run, CPO Magazine vom 14.11.2019 (https://www.cpomagazine.com/cyber-security/companies-that-experience-a-data-breach-will-underperform-the-stock-market-over-the-long-run/). Zuletzt abgerufen am 14.01.2022.

[508] *Hermstrüwer*, Informationelle Selbstgefährdung, S. 63 ff.

Auswahl an und Ausgestaltung von Erlaubnistatbeständen und ihre Konkretisierung durch die Verwaltungs- und Urteilspraxis der Aufsichtsbehörden und Gerichte[509] sowie die mitgliedstaatliche Nutzung von Öffnungsklauseln[510] ist zudem limitiert, welche Verarbeitungszwecke in welchen Kontexten überhaupt erlaubt sind, wodurch (in der Theorie) ganze Geschäftszwecke und -zweige den Verarbeitern vorenthalten bleiben können – freilich mit der Einschränkung, dass in den meisten Fällen eine (ihrerseits situationsabhängig strengen Wirksamkeitsvoraussetzungen unterworfene) Einwilligung als Kompensation zum fehlenden gesetzlichen Erlaubnistatbestand eingeholt werden kann.

Neben dieser eher groben Verhaltenssteuerung führt die Vielzahl an Organisations- und Dokumentationspflichten dazu, dass das Verhalten des Verarbeitenden auch hinsichtlich der die Verarbeitung begleitenden Umstände, teilweise sehr detailliert, gesteuert wird. Wenn also mit Art. 30 Abs. 1 S. 1 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten geführt werden muss, wenn mit Art. 25 Abs. 1 und 32 Abs. 1 DSGVO technische und organisatorische Maßnahmen zur Absicherung der Datenschutzgrundsätze und zur Sicherung der Datensicherheit ergriffen werden müssen, dann betrifft das nicht nur den Umgang mit den Daten im engeren Sinne, sondern zwingt den Datenverarbeiter auch dazu, sein Verhalten in Bezug auf seine Unternehmensorganisation, die unternehmensinternen Zugriffsmöglichkeiten und vergleichbare Umstände anzupassen.

Ziel dieser Anknüpfung an die Informations- und Datenverwendung durch den Verarbeitenden ist einmal mehr die Verringerung von mit den Datenverarbeitungen einhergehenden Gefahren für Betroffene. Die Steuerung des Verantwortlichen hinsichtlich seiner Verwendung der betreffenden Daten dient daher einerseits der Verhinderung solcher Handlungen und Verwendungsmöglichkeiten, die von sich aus potenziell oder konkret gefährlich sind und die der Verarbeitende bewusst und willentlich tätigen würde. Darüber hinaus dienen einige der entsprechend ausgerichteten Instrumente – wie oben ausführlich beschrieben – der Komplexitätsreduzierung und somit dem besseren Verständnis und der Selbstreflektion des Datenverarbeiters, um so von ihm ausgehende gefährliche Handlungen und Verwendungen zu verhindern, die unbewusst und unwillentlich aufkommen könnten. In eine ähnliche Richtung zielen jene Instrumente, die dem Schutz vor durch die Informations- und Datenverwendung aufkommenden externen Gefahren wie Datenverlust oder Hacks dienen, insbesondere also die Pflichten zur Datensicherheit.

---

[509] Zu der besonderen Bedeutung dieser Praxis im Angesicht der außerordentlich abstrakten Bestimmungen der DSGVO siehe *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (334 f.).

[510] Siehe hierzu etwa die Regelungen zu Verbraucherkrediten, Scoring und Bonitätsauskünften in §§ 30, 31 BDSG.

b) Anknüpfungspunkt Informationspreisgabe

In eine zweite Kategorie lassen sich diejenigen Instrumente einordnen, die an die Daten- und Informations*preisgabe* und damit an das Betroffenenverhalten anknüpfen.[511] Gleichzeitig bedingen sich beide Kategorien in vielerlei Hinsicht gegenseitig, da etwa eine effiziente Steuerung des Verantwortlichen bzgl. seiner Informationsverwendung wichtige Grundvoraussetzung für die Steuerung der Informationspreisgabe ist: Nur wenn bspw. der Zweck einer Verarbeitung und Verwendung von Daten klar benannt und bekannt ist und die Verwendung nicht über ihn hinaus geht, hat der Betroffene überhaupt eine Chance, die ihn in den Mittelpunkt stellenden Instrumente bzgl. der Preisgabe und späteren Kontrolle von Daten und sich daraus ergebenden Informationen wirksam auszuüben.[512]

Paradebeispiel für ein Instrument dieser Wirkrichtung ist somit die Einwilligung mitsamt ihren Wirksamkeitsvoraussetzungen und den sie absichernden Grundprinzipien wie dem Transparenzprinzip. Zeitlich der Preisgabe selbst nachgelagert, aber trotzdem an sie anknüpfend, lassen sich hier zudem einige der Betroffenenrechte aus den Art. 13 ff. DSGVO anführen, die die nachträgliche Kontrolle der preisgegebenen Daten und Informationen ermöglichen sollen: Rechte auf Auskunft, Berichtigung, Widerspruch oder Löschung. Sie sind nicht zuletzt dort von Relevanz, wo Daten nicht beim Betroffenen selbst erhoben und damit „preisgegeben" wurden, wo also notwendigerweise keine Einwilligung, sondern einer der restlichen Erlaubnistatbestände vorlag. War ein solcher gar nicht einschlägig, waren die betreffenden Daten inkorrekt oder ist etwa die Notwendigkeit der Verarbeitung für den festgelegten Zweck entfallen, kann der Betroffene so nachträglich die ursprüngliche Preisgabe kontrollieren.

Die Schwierigkeit der Wirksamkeitsabsicherung solcher, in starkem Maße vom Willen und den Fähigkeiten der Betroffenen sowie von den diese negativ beeinflussenden externen Faktoren abhängigen, Instrumente durch ihre detaillierte und weitreichende Ausgestaltung wurde oben bereits geschildert. Auch auf die lauter werdenden Stimmen im Schrifttum, wonach die Einwilligung (und mit ihr der Selbstdatenschutz insgesamt) spätestens in der heutigen Zeit kein taugliches Instrument mehr darstellt,[513] wurde hingewiesen. Ihnen gegenüber stehen jedoch auch Stimmen, die mit Blick auf die ausufernde Verrechtlichung alltäglicher Datenverarbeitungen eine Erweiterung der Einwilligung zulasten gesetzlicher Erlaubnistatbestände fordern.[514] Will man der DSGVO eine Tendenz in die eine oder andere Richtung entnehmen, so deuten etwa Art. 9 Abs. 2 lit. a und (mit Abstrichen) Art. 21 Abs, 2 lit. c darauf hin, dass in be-

[511] *Hermstrüwer*, Informationelle Selbstgefährdung, S. 67 ff.

[512] Vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, S. 64.

[513] Vgl. etwa *Cate/Mayer-Schönberger*, IDPL 2013, 67 (68 ff.); *Hermstrüwer*, Informationelle Selbstgefährdung, S. 221 ff.; *Bietti*, Consent as a Free Pass; *Solove*, Pace. L. Rev. 2013, 307 (307 ff.); *Zanfir*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 237 (237 ff.).

[514] Siehe etwa *Buchner*, Informationelle Selbstbestimmung im Privatrecht, S. 255 f.

sonders sensiblen Bereichen die Einwilligung (mit wohlgemerkt verschärften Wirksamkeitsvoraussetzungen wie der Ausdrücklichkeit ihrer Erteilung) hinsichtlich ihrer Wirksamkeitserwartung als Instrument nach wie vor einen Vertrauensvorschuss gegenüber einigen der gesetzlichen Erlaubnistatbeständen genießen soll.

4. Zwischenergebnis

Als Abschluss der aufgeführten Differenzierungen nach Steuerungswirkungen und -richtungen der Verantwortlichkeit und der mit ihr verbundenen Instrumente lässt sich konstatieren, dass mit dem zunächst klassisch anmutenden Verbotsprinzip mit Erlaubnisvorbehalt für den Verantwortlichen eine heterogene Mischung unterschiedlichster verhaltenssteuernder und -regulierender Instrumente verknüpft ist.[515] Auf der obersten Ebene können als die wichtigsten von ihnen der Selbstdatenschutz (in Form der Betroffenenrechte in Art. 13 ff. DSGVO und dem Erlaubnistatbestand der Einwilligung in Art. 6 Abs. 1 DSGVO), der Systemdatenschutz (in Form der Bestimmungen zu *privacy by design* und *privacy by default* sowie zur Datensicherheit in Art. 25 und 32 DSGVO) sowie die Instrumente der (regulierten) Selbstregulierung (in Form der Privilegierungen bei umgesetzten Verhaltensregeln und Zertifizierungen nach Art. 40 und 42 DSGVO) herausgestellt werden. Auch in diese Reihe aufnehmen kann man die Kategorie der Handlungswissen und Reflektionsfähigkeit beim Verantwortlichen steigernden Regulierungsinstrumente,[516] die solche Instrumente umschreibt, die den Verantwortlichen selbst dazu bringen, seine Verhaltensweisen zu überwachen und reflektieren und eigenständig Risiken zu identifizieren und Verbesserungsmaßnahmen zu entwickeln und umzusetzen.[517] Diese Kategorie wird in der DSGVO vor allen Dingen durch die Datenschutzfolgenabschätzung in Art. 35–36, aber auch in den Vorschriften über den Datenschutzbeauftragten in Art. 37–39 umgesetzt.

---

[515] Die Notwendigkeit eines solch heterogenen Ansatzes im Lichte zunehmend häufiger und in kürzeren Abschnitten stattfindenden technologischen Innovationen betonend *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (317): „In dieser Situation dürfte nur eine Mischung verschiedener regulatorischer Mittel überhaupt eine Aussicht auf Erfolg versprechen."

[516] Dazu grundlegend *Binns*, International Data Privacy Law 2017, 22, der diese Instrumente unter dem Begriff der Meta-Regulation zusammenfasst.

[517] Siehe auch *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (21). Demzufolge ist der Verantwortliche „gezwungen, sich mit der Rechtskonformität seiner geplanten Datenverarbeitungsvorgänge auseinanderzusetzen" und Risiken zu „evaluieren und unter abwägender Berücksichtigung bestimmter, teilweise auch gegenläufiger Faktoren geeignete technische und organisatorische Schutzmaßnahmen [zu] treffen".

II. Die Grundprämissen der Verantwortlichkeit

Aus dem oben Hergeleiteten lassen sich einige Grundprämissen herausdestillieren, die erfüllt sein müssen und von deren Erfüllung die DSGVO implizit ausgeht, damit ihr Regelungskonzept mit dem datenschutzrechtlichen Verantwortlichen als zentraler Pflichtenadressat die von ihm erwartete Wirkung zeitigt. Diese Prämissen betreffen nicht die Tatbestandsebene der Verantwortlichkeit an sich, also die Frage, unter welchen Bedingungen die DSGVO die Verantwortlichkeit eines Akteurs annimmt, sondern die darüberliegende konzeptionelle Ebene: Sie stellen die Mindestvoraussetzungen dar, die realweltlich eingelöst werden müssen, damit das im Rahmen der DSGVO gewählte Regelungskonzept mit seinem starken Fokus auf den Verantwortlichen Wirkung zeigt. Vollständige Übereinstimmung mit der Tatbestandsebene liegt dann vor, wenn die Tatbestandsvoraussetzungen in ihrer jeweiligen Auslegung[518] solche Akteure zu Verantwortlichen erklären, in deren Person die Prämissen tatsächlich erfüllt sind.[519] Hier zeigt sich also, wie die Wirksamkeit der konkreten *Ausgestaltung* der Verantwortlichenfigur in Form eines bestimmten Instrumenten-, Pflichten- und Rechtsfolgenbündels – und damit die Wirksamkeit des gesamten Konzepts – durch die *Auswahl* des Verantwortlichen bedingt wird.

Die im Folgenden erläuterten Grundprämissen folgen den oben bei I. erlangten Erkenntnissen zu den Instrumenten des Gesamtkonzepts und den von ihnen erhofften Wirkungen. Sie sollen jeweils anhand ihrer besonderen Bedeutung für bestimmte, nicht immer exklusiv nur einer Prämisse zuordenbare, Verantwortlichenpflichten veranschaulicht werden.

1. Der Verantwortliche als zentrale, alle Umstände der Verarbeitung kennende und beeinflussende Figur

Die Notwendigkeit eines im jeweiligen Verarbeitungskontext zentralen, umfassend kenntnisreichen und handlungsfähigen Verantwortlichen für die erhoffte Wirkweise des soeben beschriebenen Regelungskonzepts zeigt sich bereits im Dualismus der ausgemachten Steuerungsrichtungen. Die Instrumente der DSGVO sind wahlweise auf die Informationsverwendung, also das Handeln des Verantwortlichen, oder die Informationspreisgabe, also das Handeln des Betroffenen gerichtet.[520] Dabei hängt die zweite Kategorie letztlich in fundamentaler Weise von der Wirksamkeit der ersten Kategorie ab: Das Handeln des Betroffenen setzt seine Kenntnis über die die Umstände, Grundlagen und Konsequenzen der konkreten Verarbeitung und ihr zugrundeliegenden Daten

[518] Zu den Tatbestandsvoraussetzungen und ihrem konkreten Verständnis siehe ausführlich *infra* bei C.

[519] Der ausführliche Abgleich zwischen diesen beiden Ebenen, für den die Herleitung und Konkretisierung der folgenden Prämissen den Boden bereitet, ist Thema von Kapitel 3.

[520] Vgl. die Ausführungen *supra* bei I. 3.

voraus. Die Wirksamkeit seines Handelns setzt voraus, dass seine geltend gemachten Rechte vom Verantwortlichen auch umgesetzt werden können.

Explizit lässt sich diese Prämisse, zumindest in Bezug auf die Fähigkeit zur Einflussnahme, auch bereits den Tatbestandsvoraussetzungen der Figur entnehmen – Art. 4 Nr. 7 definiert den Verantwortlichen als die Person, die die Entscheidungshoheit über die *Zwecke* und *Mittel* der jeweiligen Verarbeitung innehat.

Ähnlich gestaltet es sich mit Blick auf die erhofften Steuerungswirkungen. Der komplexitätsgeschuldeten Unwissenheit und Ungewissheit[521] nicht nur des Betroffenen, sondern insbesondere auch der Behörden – in Bezug sowohl auf die einzelnen Verarbeitungsvorgänge beim konkreten Verantwortlichen als auch im weiteren Sinne auf die gesellschaftlichen Implikationen und Risiken einer breiteren Nutzung bestimmter Verarbeitungsmethoden –, kann nur abgeholfen werden, wenn der Verantwortliche selbst möglichst weitgehende Kenntnis um die Umstände und möglichen Risiken seines Handelns hat. Das Ergreifen von Gegenmaßnahmen und das Anpassen von erkannten Zuwiderhandlungen oder Defiziten – sei es durch Eigenerkenntnis und Reflektion oder durch behördliche Anordnung, Sanktionsdruck oder den Anspruch eines Betroffenen – setzt die faktische Fähigkeit voraus, den entsprechenden Einfluss ausüben, die entsprechenden Praktiken anpassen zu können. Das gilt demnach einerseits für den Verantwortlichen und seine Fähigkeit zur Erfüllung elementarer Pflichten wie der zur Anfertigung eines Verzeichnisses von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 S. 1 DSGVO, zur Bereitstellung der in Art. 12 Abs. 1 S. 1 DSGVO aufgezählten und in weiteren Normen konkret behandelten Informationen und Mitteilungen an Betroffene, oder zur Vornahme konkreter technisch-organisatorischer Maßnahmen, wie sie Art. 24 Abs. 1 S. 1, 25 Abs. 1 und 32 Abs. 1 DSGVO vorsehen. Andererseits ermöglicht diese Kenntnis und Handlungsfähigkeit eine wirksame Interaktion zwischen Verantwortlichem und zuständiger Aufsichtsbehörde und schafft so eine der Grundvoraussetzungen für eine effektive Kontrolle und Durchsetzung.

Dabei muss dem Gesamtkonzept zugestanden werden, dass es durch entsprechende Pflichten bereits versucht, darauf hinzuarbeiten, dass ein Verantwortlicher diese Eigenschaften erlangt und beibehält. Die DSGVO sieht schließlich „eine ganze Reihe von prozeduralen und organisatorischen Instrumenten vor, mit denen die Verantwortlichen zu einer besseren ‚Compliance' im Hinblick auf das materielle Datenschutzrecht gebracht werden sollen, also die Rahmenbedingungen für die Befolgung des materiellen Rechts (hier durch weiteres Recht) verbessert werden sollen".[522] Einige der Pflichten wirken also darauf hin, die Grundvoraussetzungen für die effiziente Erfüllung anderer Pflichten zu

[521] Vgl. *supra* bei I. 2. a. bb) und cc).

[522] *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (19).

schaffen bzw. zu verbessern. Dies gilt vor allem für die oben beschriebenen Instrumente der zur Regulierung des Handlungswissens,[523] deren Ziel die eigenständige Sensibilisierung und Reflektion des Verantwortlichen hinsichtlich der Umstände der bei ihm durchgeführten Verarbeitungen und daraus potenziell erwachsenden Risiken für Betroffene ist, um stets die organisatorischen Fähigkeiten zu haben, die zahlreichen weiteren Pflichten erfüllen zu können. Dazu gehört bspw. auch die Fähigkeit, jederzeit einen umfassenden Überblick über unternehmensinterne, aber auch nach außen gehende Datenflüsse zu haben bzw. haben zu können. Auch diese geschickte Methode, Steuerungsinstrumente auf andere Steuerungsinstrumente innerhalb eines größeren Regelungskonzepts zu beziehen, hat aber ihre Grenzen. Ist ein Unternehmen, das den gesetzlich festgelegten Kriterien nach als Verantwortlicher zu qualifizieren ist, in der Realwelt schlicht nicht in der Lage, alle verarbeitungsrelevanten Umstände zu überblicken oder auf alle verarbeitungsrelevanten Umstände und beteiligten Akteure den notwendigen Einfluss auszuüben, um bestimmte Praktiken zu unterbinden oder zu ändern, so laufen auch solche Pflichten ins Leere, die den Verantwortlichen dazu zwingen sollen, stets in der Lage zur Erbringung solcher Dinge zu sein.

Eine Person, die die Tatbestandsvoraussetzungen der datenschutzrechtlichen Verantwortlichkeit im Rahmen der DSGVO erfüllt, muss daher, überspitzt beschrieben, im Rahmen des ihm unter dem Begriff der Datenverarbeitung übertragenen Lebenssachverhalts stets allwissend und allmächtig sein, damit das Regelungskonzept insgesamt seine Leistungsfähigkeit erreichen kann. Ist dies nicht der Fall, kommen zwei Optionen in Betracht. Ist die Diskrepanz ein Einzelfall und sind das Wissen und die Fähigkeit zur Einflussnahme durch Fehlverhalten des Verantwortlichen eingeschränkt und ist diese Einschränkung grundsätzlich behebbar, so liegt schlicht ein (ggf. systematisch) datenschutzwidriges Verhalten beim betreffenden Verantwortlichen – denkbar ist auch eine ganze Gruppe von Verantwortlichen – vor und ist die Prämisse an sich noch von der Realität getragen. Reine selbstverschuldete Ohnmacht kann die eigene Verantwortlichkeit nicht eliminieren, kann also nichts daran ändern, dass ein Akteur die ihn treffende(n) Pflicht(en) nicht erfüllt. Dieser Grundsatz ist aber aus einer Governance-Warte dann nur begrenzt sinnvoll, wenn die Pflichtigen auf breiter Ebene nicht in der Lage sind, die in sie gesetzten Erwartungen zu erfüllen. Die nachträgliche Sanktion von Pflichtverstößen ist keine ausreichende Kompensation für die Nichterreichung der mit dem eigentlichen Pflichtenkonzept verfolgten Ziele. Ist die Diskrepanz daher erkennbar großflächiger und liegen die Gründe dafür nicht (allein) bei den jeweiligen Verantwortlichen selbst, sondern, für diese nicht ohne weiteres zugänglich, im Missverhältnis zwischen gesetzgeberischer Vorstellung und Realwelt, so liegt in der Realität eines der Grund-

[523] Siehe *supra* bei I. 1. d).

prämissen des datenschutzrechtlichen Regelungskonzepts nicht mehr vor und wird dieses also nicht mehr von ihr getragen.

Die Unterscheidung zwischen diesen beiden Fällen gestaltet sich dabei jedoch, insbesondere bei zunehmender Anzahl betroffener Verantwortlicher, denkbar schwer. Ob verfestigte Strukturen und Geschäftspraktiken, durch die Verantwortliche den Überblick über relevante Verarbeitungsumstände verlieren oder durch eine Gemengelage an beteiligten Akteuren die Einflussnahmefähigkeit vermissen lassen, nun ihnen oder der fehlenden Tragfähigkeit des Regelungskonzepts angelastet werden können und sollten, gilt es dann im Einzelfall zu diskutieren.[524]

2. Der Verantwortliche als nach außen hin klar erkennbare Figur

Gleiches gilt auch für eine zweite Grundprämisse. Die Zentralität des Verantwortlichen muss sich nicht nur in seinem Wissen und seiner Fähigkeit zur Einflussnahme niederschlagen, sondern auch in seiner Sichtbarkeit und Erkennbarkeit. Dies ergibt sich zuvorderst aus seiner instrumentellen Rolle für das Instrument des Selbstdatenschutzes, wirkt sich aber zugleich auf die Erfolgsaussichten der Behördenaufsicht aus. Nur wenn der Betroffene weiß, wer seine Daten in welchem Kontext verarbeitet und wie betreffende Person zu erreichen ist, ist er in der Lage, seine Rechte zu adressieren und auszuüben.[525] Nur wenn die Aufsichtsbehörde weiß, welche Unternehmen in welchem Ausmaß und zu welchen Zwecken Daten verarbeiten, kann sie ihren Überwachungs- und Durchsetzungsaufgaben, aber auch ihren Pflichten zur Sensibilisierung und Unterstützung kooperationswilliger Verantwortlicher[526] nachkommen. Dabei genügt es nicht, dass der jeweilige Verantwortliche insgesamt und abstrakt, etwa auf seiner Website durch Bereithaltung einer Datenschutzerklärung, zu erkennen gibt, dass er bestimmte Datenverarbeitungen vornimmt. Es bedarf vielmehr einer Kenntlichmachung und Offenbarung im jeweiligen Moment ganz konkreter Verarbeitungskontexte. Nicht nur, aber in besonderem Maße dann, wenn es augenblicklich von Relevanz ist, also im Moment des jeweiligen Verarbeitungsvorgangs, müssen Betroffene in der Lage sein, den Verantwortlichen zu identifizieren und ggf. zu reagieren. Nicht umsonst verlangt Art. 13 Abs. 1 DSGVO die Erbringung der Informationspflicht (inklusive Nennung des Namens und der Kontaktdaten des Verantwortlichen) *zum Zeitpunkt* der Erhebung der Daten und stellt auch Art. 14 Abs. 3 DSGVO strenge Voraussetzungen an die nachträgliche Informierung bei nicht direkt beim Betroffenen erhobenen Daten. Auch dann, wenn es auf das Treffen einer verarbeitungserheblichen Entscheidung wie die

[524] Siehe zu dem akteursübergreifenden Verlust von Einflussnahmefähigkeit in verteilten Verarbeitungsszenarien *supra* bei Kapitel 2 B. I. und zur Bestandsaufnahme der Prämissen unter diesem Eindruck *infra* bei Kapitel 3 A. I.

[525] Vgl. *Petri*, in: Simitis u. a., DSGVO/BDSG, Art. 4 Nr. 7 DSGVO Rn. 1.

[526] Vgl. Art. 57 Abs. 1 lit. a, b und c DSGVO.

Erteilung einer Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO ankommt, ist es insbesondere bei der in der heutigen digitalen Welt üblichen Pluralität beteiligter Akteure vonnöten, dass Betroffene Transparenz darüber haben, welche Akteure beteiligt sind und wer von ihnen die Rolle eines Verantwortlichen innehat. Gleiches gilt für die Ausübung der Betroffenenrechte in Art. 16–22 DSGVO, die zwingend ein Minimum an Vorkenntnis über den Verantwortlichen und die Verarbeitungsumstände voraussetzt.

Die hohe Bedeutung der kontextsituativen Identitätsoffenlegung zeigt sich zudem für das Verhältnis zwischen Verantwortlichen und Aufsichtsbehörde. Mit Blick auf das oben angesprochene[527] zweifache Risikowissen, das sich die Aufsichtsbehörden aneignen müssen – zum einen in Bezug auf konkrete Verarbeitungsvorhaben konkreter Verantwortlicher, zum anderen in Bezug auf die gesellschaftlichen Risiken der breiteren Etablierung neuer Verarbeitungspraktiken und Technologien –, benötigen sie in besonders sensiblen Verarbeitungskontexten die selbständige Vorlage durch den Verantwortlichen, etwa im Rahmen der Datenschutzfolgenabschätzung nach Art. 36 Abs. 1 DSGVO. Diese Abhängigkeit von der Erkennbarkeit des Verantwortlichen ist aufgrund des Wegfalls der in der DSRL noch vorhandenen Anmeldepflichten[528] nun besonders hoch. Auch die Funktionsfähigkeit des Selbstdatenschutzes wird hier abermals virulent, da insbesondere wenig kooperationswillige „schwarze Schafe" unter den Verantwortlichen häufig erst durch die Beschwerden von Betroffenen gem. Art. 77 DSGVO bekannt werden. Auch diese können ihre Erfahrungen mit ggf. datenschutzwidrig handelnden Verantwortlichen nur teilen, wenn sie um deren Identität und Verarbeitungspläne wissen.

Ein weiteres Mal zeigt sich also auch hier das besondere Ausmaß der gegenseitigen (Erfolgs-)Abhängigkeit der verschiedenen Regulierungsinstrumente voneinander.

3. Der Verantwortliche als einfach zuordenbare Rolle

Zuletzt gilt eine Prämisse, auf der letztlich alle bisher genannten Prämissen aufbauen und die zunächst zu offensichtlich erscheint, um überhaupt erwähnt zu werden, in der heutigen Realität arbeitsteiliger und ausgelagerter Verarbeitungsvorgänge und hinsichtlich der rollenbezogenen Abgrenzung zu anderen verwaltungsrechtlichen Pflichtigkeiten aber durchaus wert ist, näher betrachtet zu werden. Knapp formuliert lautet sie: Die Zuschreibung von Verantwortlichkeit als zentrales Element des Regelungskonzepts hinter dem (privaten) Datenschutzrecht kann nur den von ihr erhofften Erfolg zeitigen, wenn Unternehmen stets und möglichst frühzeitig wissen, *dass*, *wann* und in Bezug auf *welche Verarbeitungen* sie als Verantwortliche im Sinne der DSGVO agieren. Besteht

[527] Siehe *supra* bei B. I. 2. b.
[528] Etwa im dortigen Art. 20.

hier eine zu große Unsicherheit oder ist Akteuren überhaupt nicht klar, dass sie datenschutzrechtlich relevante Handlungen vornehmen, besteht ein fundamentales Regulierungsdefizit.[529] Hier zeigt sich die Unterscheidung der datenschutzrechtlichen Verantwortlichkeit von anderen verwaltungsrechtlichen Verantwortlichkeitsmodellen. Weder ist der Anknüpfungspunkt für die Verantwortlichkeit hinreichend konkret oder bezieht sich auf eindeutige und homogene Handlungen oder Lebenssachverhalte, noch bedarf es im Vorfeld der Einholung einer Genehmigung oder eines anderen Aktes, der durch Herstellung von Kontakt zur zuständigen Behörde auch aufklärenden und hinweisenden Charakter hätte. Ist einem Rundfunkbetreiber, einem Betreiber einer Gaststätte oder eines Atomkraftwerks aufgrund der Eindeutigkeit des Bezugsobjekts und bzw. oder der Genehmigungsbedürftigkeit ohne weiteres klar, dass er diese mit Pflichten belegte Rolle innehat, ist dies beim datenschutzrechtlichen Verantwortlichen daher nicht ohne weiteres der Fall. Die soziale Konstruktion,[530] die nötig ist, um die abstrakte Norm der Verantwortlichkeit gem. Art. 4 Nr. 7 DSGVO auf den eigenen konkreten Lebenssachverhalt anzuwenden, ist, nicht zuletzt durch die heute vorherrschende Alltäglichkeit von Datenverarbeitungen mit ihren zunehmend heterogenen Ausgestaltungen und Beteiligungsmodellen, ungleich schwerer zu erreichen.

Auch hier gilt das bereits im vorangegangenen Abschnitt Gesagte: Versäumen es Verantwortliche, sich ihrer Rolle bewusst zu werden, und verstoßen deshalb gegen datenschutzrechtliche Pflichten, so befreit sie das naturgemäß nicht von besagter Verantwortlichkeit und führt Rechtsfolgen herbei, die sanktionieren, aber auch eine zukünftig erhöhte Normbefolgung erreichen sollen.[531] Nichtsdestotrotz liegt es im ureigenen Interesse des Verordnungsgebers, solche Fälle fehlender Kenntnis um die eigene Verantwortlichkeit möglichst gering zu halten oder gar gänzlich zu eliminieren. Auch dies lässt sich durch einen Vergleich mit einem anderen Rollenmodell gut verdeutlichen: Während der polizeirechtliche Störer als ebenfalls situativ und durch soziale Konstruktion bestimmbarer Pflichtiger sich überhaupt erst durch die Inanspruchnahme seitens der Behörde seiner Rolle gewahr wird, ist dies vollkommen in Einklang mit der Zielsetzung des Polizeirechts, das die momentane Abwehr von Gefahr (sowie nachgelagert ggf. die Erstattung der verursachten Kosten) bezweckt. Anders verhält es sich aber mit dem Datenschutzrecht, dem es gerade um die dauerhafte, geordnete Strukturierung des Datenumgangs[532] und damit um das Erreichen

[529] So auch bereits zu Zeiten der DSRL *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 9: „Hinsichtlich der Ziele der Richtlinie ist es äußerst wichtig, dass die Verantwortung für die Datenverarbeitung klar festgelegt ist und praktisch zum Tragen kommen kann."

[530] Vgl. *Hoffmann-Riem*, AöR 2017, 1 (34).

[531] Siehe die die Ausführungen zur Rechtsdurchsetzungsinstrumente *supra* bei B. I. 1. e).

[532] Siehe *Marsch*, Das europäische Datenschutzgrundrecht, S. 265.

einer möglichst breitflächigen dauerhaften Normbefolgung geht,[533] die schon im Ansatz[534] voraussetzt, dass die Pflichtigen sich regelmäßig ihrer Pflichtigkeit bewusst sind. Die reine nachträgliche Sanktionierung oder Ergreifung anderer Maßnahmen ist hier kein taugliches Äquivalent zu der Regulierungswirkung möglichst breitflächiger Normbefolgung. Dass die Klarheit über die Rollenverteilung möglichst früh vorhanden sein muss, verdeutlichen die zahlreichen Pflichten, die vor der eigentlichen Verarbeitungstätigkeit anknüpfen und Einfluss auf die planerischen und organisatorischen Abläufe des Verantwortlichen ausüben sollen. Zu nennen sind hier etwa die Pflichten zum Ergreifen von *privacy by design*-Maßnahmen gem. Art. 25 Abs. 1 oder zur Durchführung einer Datenschutzfolgenabschätzung gem. Art. 35 Abs. 1 S. 1.

Diese Prämisse der einfachen (Eigen-)Zuordenbarkeit der Verantwortlichkeit kann aus zweierlei Gründen nicht (mehr) erfüllt sein: Einerseits dann, wenn die Zuordnungskriterien (in Form der Tatbestandsmerkmale) für sich bereits zu unbestimmt sind, andererseits dann, wenn die Entwicklung der Verarbeitungsrealität neue Beitragskonstellationen und Ausprägungen von Verarbeitungshandlungen geschaffen hat, die eine Einordnung unter die an sich verfestigten und konkretisierten Kriterien erschweren.

Zur Vermeidung beider genannten Fälle besteht daher über das unionrechtliche Bestimmtheitsgebot[535] hinaus ein großes Interesse an hinreichender Rechtssicherheit und -klarheit in Bezug auf die Tatbestandsvoraussetzungen der Verantwortlichkeit und ihre situative Einschlägigkeit. Die Aufgabe, diese Rechtssicherheit herzustellen, liegt neben dem Verordnungsgeber vor allen Dingen beim EuGH sowie bei den Aufsichtsbehörden[536] und weiteren relevanten Institutionen und Einrichtungen wie insbesondere dem EDSA.[537] Ihnen obliegt es, Konkretisierungsleistungen sowohl für entwicklungsunabhängige Grundsatzrechtsfragen als auch für akute, neu auftretende Phänomene zu leisten. Es ist daher bereits seit längerem üblich, dass Aufsichtsbehörden für

---

533 Vgl. *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (22), der in der Mischung an gewählten Instrumenten einen Weg zur „Sicherstellung der Rechtsbeachtungskontrolle durch den Rechtsunterworfenen bei möglichst geringem staatlichem Ressourceneinsatz“ sieht.

534 Das heißt: schon vor der nachgelagerten Frage der Effektivität der Rechtsdurchsetzung.

535 Dieses ist einerseits Ausfluss des Erfordernisses einer gesetzlichen Grundlage gem. Art. 52 Abs. 2 S. 2 GRCh und hat andererseits bereits Gültigkeit als allgemeiner Rechtsgrundsatz. Vgl. *Jarass*, in: Jarass, Grundrechtecharta, Einleitung Rn. 46 und Art. 52 Rn. 27.

536 Vgl. die expliziten Aufgaben in Art. 57 Abs. 1 lit. d und i DSGVO.

537 Zu dessen in Art. 70 Abs. 1 DSGVO normierten Aufgaben gehört auch das Ausarbeiten von Leitlinien und Empfehlungen als Orientierungshilfe für Verantwortliche. Vgl. hierzu auch *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (335): „[…] spricht aber viel dafür, dass die entscheidenden Weichenstellungen für das europäische Datenschutzrecht künftig im Ausschuss gefällt werden.“

konkrete Branchen und Verarbeitungsszenarien und -kontexte Anleitungen und Leitfäden veröffentlichen – insbesondere dort, wo eine Mehrzahl von Akteuren beteiligt und die Zuordnung von Einflusssphären und Bestimmung hinreichender Einflussschwellen daher besonders schwierig ist.[538]

Von besonderer Kritikalität sind hier zwei Problemfelder, die an dieser Stelle nur kurz angesprochen und im folgenden Abschnitt dieser Arbeit ausführlich analysiert werden sollen: zum einen die Abgrenzungen zwischen den Rollen des Verantwortlichen und des Auftragsverarbeiters, wenn Datenverarbeitungen arbeitsteilig von unterschiedlichen Akteuren vorgenommen werden.[539] Zum anderen die durch inzwischen gefestigte EuGH-Rechtsprechung seit 2018 erfolgte Etablierung der bis dahin in der Praxis irrelevanten gemeinsamen Verantwortlichkeit, die einer weitreichenden Absenkung der Tatbestandsvoraussetzungen des Art. 4 Nr. 7 DSGVO gleichkam, ohne diese jedoch mit klaren Kriterien zu versehen.[540] Die Folge ist eine kaum überschaubare Breite an unterschiedlichen Literaturansichten und in der Folge eine bis heute anhaltende Rechtsunsicherheit bei potenziell betroffenen, privaten wie unternehmerisch tätigen, Akteuren.[541]

4. Annex: Notwendigkeit eines Minimums an Rechtsdurchsetzung

Keine eigenständige Prämisse, aber gleichermaßen von ihrer Erfüllung abhängig und gewissermaßen quer über ihnen liegend ist der Gedanke, dass mit Blick auf die Wirksamkeit der einzelnen Regulierungsinstrumente und des Konzepts der Verantwortlichkeit insgesamt stets ein Mindestmaß an Rechtsdurchsetzung erreicht werden muss, mit dem eine gewisse kritische Schwelle überschritten wird. Wie bereits erläutert, hat der Datenschutz grundlegende, seiner Materie inhärente Rechtsdurchsetzungsdefizite,[542] denen das Regelungskonzept der DSGVO punktuell entgegenzuwirken versucht. Gleichzeitig setzen viele der das Regelungskonzept ausmachenden Instrumente ihrerseits ein Mindestmaß an grundlegender, tatsächlicher Normbefolgung[543] voraus, um überhaupt wirksam sein zu können. Mit anderen Worten: Viele Instrumente des privaten Datenschutzrechts setzen einen handlungs- und in Teilen kooperationsbereiten Verantwortlichen voraus. Macht ein Verantwortlicher seine Verarbeitungsvorgänge gar nicht kenntlich, laufen der Selbstdatenschutz, aber auch die Kontrolle durch

---

538 Vgl. etwa *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter".

539 Siehe hierzu die Ausführungen zur Rolle des Auftragsverarbeiters *infra* bei C. II. 4. a).

540 Siehe hierzu ausführlich die Ausführungen *infra* bei C. II. 4. b).

541 Hierzu ausführlich *infra* bei C. II. 4. c).

542 Vgl. *Thierer*, Harv. J. Law Public Policy 2013, 410 (424 ff.); *Lepperhoff* u. a., DuD 2012, 195 (195 ff.).

543 Grundlegend zur Normbefolgung als Voraussetzung der Normwirkung *Hoffmann-Riem*, Innovation und Recht, Recht und Innovation, S. 142 ff.

die Aufsichtsbehörden schlicht ins Leere, solange nicht durch Zufall oder journalistische Recherche (meist im Falle eines größeren Skandals, also dann, wenn es bereits zu Datenpannen oder anderen Schäden gekommen ist) Details über individuelle oder kollektive Praktiken ans Licht kommen.

Den beiden bereits aufgeführten Prämissen, die das „Können" des Verantwortlichen in den Mittelpunkt stellen, ist daher eine Ebene des faktischen „Müssens" zur Seite zu stellen: Nur, wenn erreicht wird, dass Verantwortliche – sei es aus eigener (etwa auf Marktmechanismen und Wettbewerb zurückzuführender) Motivation oder aus regulatorischem Druck – effektiv dazu angehalten werden, dem Grunde nach Rechenschaft über ihre Verarbeitungsvorgänge und zusammenhängende Praktiken abzulegen und ihr eigenes Handlungswissen durch organisatorische Ausrichtung und Reflektion zu steigern[544], können nachgelagerte Instrumente wie die Einbindung eines Datenschutzbeauftragten oder die Kontrolle durch Aufsichtsbehörden greifen. Daran mangelt es, wenn sie faktisch überhaupt nicht befürchten müssen, als Verantwortliche erkannt oder bzgl. ihrer Verarbeitungsvorgänge kontrolliert und belangt zu werden, aber auch dann, wenn sie sich, wie eben beschrieben, nicht in der Lage sehen, ihre Rolle als Verantwortlicher zu erkennen.

Dass die Effektivität (und damit letztlich auch die verfassungsrechtliche Legitimität) des Rechts von seiner erfolgreichen Durchsetzung abhängt, betrifft nicht nur das Datenschutzrecht.[545] Doch wie das eben Beschriebene zeigt, gilt es für das private Datenschutzrecht in besonderem Maße.

Das latente Rechtsdurchsetzungsdefizit des Datenschutzes zu beheben war eines der explizit erwähnten Ziele, die mit der Konzeption der DSGVO verfolgt wurden.[546] Jedenfalls einige der deshalb gewählten Änderungen im Vergleich zur Rechtslage unter der DSRL betreffen auch die hier relevante grundlegende Bereitschaft zur Beschäftigung und zum ernsthaften Umgang mit Datenschutz. Dazu gehören bspw. der in der Hoffnung auf erfolgreiche Abschreckungseffekte massiv erhöhte Bußgeldrahmen,[547] die erstmalige Kodifizierung von zivilrechtlichen Ansprüchen auf Schadensersatz für immateriellen Schaden,[548] die erweiterten Möglichkeiten des kollektiven Rechtsschutzes durch Verbandsklagerechte[549] oder die – allerdings nach wie vor umstrittene – Möglichkeit der

[544] Siehe die Ausführungen zu den Instrumenten zur prozeduralen Steigerung von Handlungswissen bei B. I. 1. d).

[545] Die verfassungsrechtlichen Implikationen ineffektiver Steuerungsinstrumente aufzeigend *Baehr*, Verhaltenssteuerung durch Ordnungsrecht, S. 84 ff.

[546] So insbesondere hinsichtlich der Defizite bei der grenzüberschreitenden Rechtsdurchsetzung im Lichte eines bis dato heterogenen europäischen Rechtsrahmens, siehe Erwg. 9 DSGVO. Siehe zudem *Bergt*, DuD 2017, 555 (555); vgl. auch *Golla*, jipitec 2017, 70 (70 ff.).

[547] Vgl. Art. 83 Abs. 4 – Abs. 6 DSGVO. Je nach Norm, gegen die verstoßen wurde, liegt die Obergrenze bei bis zu 20 Mio. Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes.

[548] Vgl. Art. 82 Abs. 1 DSGVO sowie die ausführliche Behandlung bei I. 1. e) bb) (1).

[549] Vgl. Art. 80 Abs. 1 DSGVO. Hiermit soll insbesondere die fehlende Klagefreudigkeit

Abmahnung von Datenschutzverstößen durch Wettbewerber[550]. Als „weicheres" Gegenstück zum letztgenannten Aspekt sind zudem die intensivierten Bemühungen um eine Sensibilisierung der Bevölkerung als Versuch zu erwähnen, datenschutzfreundliches Vorgehen von Unternehmen als erstrebenswerten Wettbewerbsvorteil zu etablieren.[551]

Auch die Einführung des Kohärenzverfahrens zwischen den mitgliedstaatlichen Aufsichtsbehörden nach Art. 63 DSGVO, das eine einheitliche Anwendung und Durchsetzung der Verordnung im gesamten Anwendungsbereich erreichen will, kann in diese Reihe gestellt werden; durch stark divergierende Rechtsauffassungen und Vorstellungen von der angemessenen Durchsetzungshärte[552] wirkte sich insbesondere die Zuständigkeit der irischen und luxemburgischen Aufsichtsbehörden für dort ansässige große Konzerne wie Facebook, Google oder Amazon negativ auf das Datenschutzniveau aus.[553] Das Kohärenzverfahren soll daher insbesondere in solchen Fällen, die Daten Betroffener aus dem gesamten EU-Raum betreffen, einen Konsens zwischen allen Aufsichtsbehörden erreichen und „Datenschutz-Oasen" verhindern.

Wenngleich also das Datenschutzrecht qua seiner Natur schon rein faktisch keinen Vollvollzug gewährleisten kann und in seiner Rolle als Vorfeldschutz wohl auch gar nicht soll,[554] ist ein Mindestmaß an Durchsetzung doch die Grundvoraussetzung für die großflächige Grundeffektivität seines Regelungskonzepts. Dies ist im Grunde zwar ein Allgemeinplatz, der für jede (regulierende) Norm gilt,[555] hat aber für die DSGVO aufgrund ihres besonderen Ensembles an Instrumenten und deren gegenseitiger Abhängigkeiten eine eigenständige Bedeutung. Defizitäre Rechtsdurchsetzung bedeutet hier nicht nur, dass nicht jeder Normverstoß geahndet, nicht jeder Schaden ausgeglichen wird. Stattdessen führt die Interdependenz der einzelnen Regelungsinstrumente dazu, dass sich die Nichtbefolgung einzelner Pflichten schnell unmittelbar auf die grundlegende Wirksamkeit ganzer Instrumente durchschlägt. Ein zu hohes Rechtsdurchsetzungsdefizit sorgt so dafür, dass die einzelnen Akteure die mit ihren Rollen verbundenen Erwartungen nicht mehr erfüllen können und trägt letztlich mit dazu bei, dass zentrale Grundprämissen nicht mehr tragen.

---

der Betroffenen kompensiert werden. Eingeschränkt wird der Umfang dieses Instruments jedoch dadurch, dass Verbände zunächst nur auf Auftrag individueller Betroffener tätig werden dürfen. Abs. 2 der Norm erlaubt Mitgliedstaaten, durch nationales Recht auch initiatives Tätigwerden zu statuieren. Ob die deutsche Norm des § 2 Abs. 2 S. 1 Nr. 11 UKlaG eine (europarechtskonforme) Umsetzung dieses Spielraums darstellt, ist umstritten. Siehe dazu ausführlich *supra* bei I. 1. e) bb) (2).

[550] Siehe dazu *supra* bei I. 1. e) bb) (3).

[551] Vgl. *Schröder*, ZD 2012, 193 (193 f.).

[552] Vgl. *Dünkel*, DuD 2019, 483 (483).

[553] Vgl. *Caspar*, in: Kühling/Buchner, DSGVO/BDSG, Art. 63 DSGVO Rn. 11 m. w. N.

[554] Siehe *Rademacher*, JZ 2019, 702 (707 ff., 710) m. w. N. sowie tiefergehenden Gedanken zum denkbaren Eigenwert eines gewissen Vollzugsdefizits.

[555] Siehe abermals *Hoffmann-Riem*, Innovation und Recht, Recht und Innovation, S. 142 ff.

5. Zwischenergebnis

Zusammenfassend lässt sich festhalten, dass die hier vorgestellten Prämissen also – aus ihren jeweils eigenen Gründen und in unterschiedlichem Ausmaß – konstituierend für die Wirksamkeit der Verantwortlichkeit als Herzstück des Regelungskonzepts der DSGVO sind. Diese Bedeutung lässt sich paradigmatisch an bestimmten Pflichten festmachen, bei denen es besonders auf die jeweiligen Eigenschaften der Rolle des Verantwortlichen ankommt. Die folgende Tabelle fasst die wichtigsten Eigenschaften jeder Prämisse zusammen.

Tabelle 2: Die einzelnen Grundprämissen und ihre Charakteristika.

Prämisse	*Bedeutung bzgl. des Verantwortlichen*	*Besonders betroffene Pflichten*
(1.) Zentralität, Kenntnis und Einflussfähigkeit	Muss den ihm zugewiesenen Lebensabschnitt weitreichend überblicken, beeinflussen und kontrollieren können	Art. 25 Abs. 1, 30 Abs. 1, 32 Abs. 1 DSGVO
(2.) Äußere Erkennbarkeit	Muss für andere Akteure (insb. Betroffene und ASB) leicht erkennbar und erreichbar sein	Art. 6 Abs. 1 lit. a, 16–22 DSGVO
(3.) Einfache Zuordenbarkeit	Muss frühzeitig und leicht seine Pflichtigkeit erkennen können	Art. 25 Abs. 1, 35 Abs. 1 S. 1 DSGVO
(4.) Annex: Minimum an Rechtsdurchsetzung	Aufeinander aufbauende Instrumente setzen gegenseitig ihre Durchsetzung voraus	–

Ist eine der Prämissen oder sind mehrere von ihnen in der Praxis großflächig nicht mehr erfüllt, droht damit die Untauglichkeit des gesamten Konzepts.

Der Frage, ob die beschriebenen Prämissen derzeit und auch unter der in Kapitel 2 beschriebenen Verarbeitungsrealität noch tragen, und ob ein erforderliches Mindestmaß an Rechtsdurchsetzung noch anzunehmen ist, soll im nächsten Kapitel nachgegangen werden. Bereits jetzt lässt sich aber mit den oben angestellten Überlegungen sagen, dass sich hinsichtlich jeder der Prämissen zumindest berechtigte Zweifel dahingehend äußern lassen, inwieweit sie von der Realität moderner Verarbeitungsszenarien noch getragen werden. Liegt ein solcher Fall defizitärer Prämissen vor, stellt sich die Frage, was sich am Gesamtkonzept ändern lässt und wo die richtigen Stellschrauben für eine solche Änderung liegen, um den defizitären Prämissen wieder zur Wirksamkeit zu verhelfen.

Hier hilft – zumindest für eine grobe Systematisierung – die oben aufgestellte Trennung der Verantwortlichkeitszuschreibung in zwei zentrale Elemente: die der *Auswahl* des Verantwortlichen und die der *Ausgestaltung* seiner Stellung und seines Pflichtenkatalogs.

Ein Ansatzpunkt wäre daher die Modifizierung der Ausgestaltung der datenschutzrechtlichen Verantwortlichkeit dergestalt, dass die gewählten Instrumente

nicht mehr oder jedenfalls in nur noch geringerem Ausmaß von der bzw. den jeweils defizitären Prämisse(n) abhängig ist oder von gänzlich anderen Prämissen lebt.[556] Ein solcher Ansatz wäre gleichwohl eher umfangreich und aufwändig. Die derzeitige Kombination an Verantwortlichenpflichten, Betroffenenrechten und Aufsichtsbehördenbefugnissen ist in großen Teilen ein gewachsenes Konstrukt jahrzehntelanger Datenschutzpraxis, das zwar durch die DSGVO einige Modernisierungen und Änderungen erfuhr, aber im Großen und Ganzen noch denselben Überlegungen und Grundsätzen verschrieben ist, die zum Zeitpunkt des Erlasses der DSRL im Jahr 1997 vorherrschten.

Der Weg des geringeren Widerstandes scheint daher darin zu liegen, sich der Auswahl des Verantwortlichen anzunehmen. Käme man zu dem Ergebnis, dass die Erfüllung aller notwendigen Prämissen in einer die Tatbestandsvoraussetzungen der Verantwortlichkeit erfüllenden Person in heutigen Verarbeitungsszenarien regelmäßig oder häufig nicht mehr möglich ist, müssten dann also die Tatbestandsvoraussetzungen entsprechend geändert werden, um dafür zu sorgen, dass (wieder) eine Kongruenz zwischen der erfüllten Qualifikation als Verantwortlichem und dem Vorliegen aller damit erhofften Prämissen vorliegt. Dies muss nicht zwingend heißen, dass dadurch stets alle Prämissen in jeder als Verantwortlicher eingestuften Person in vollem Ausmaß verwirklicht sein müssen. Dort, wo dies nicht möglich erscheint, kann ein Weg auch darin liegen, zusätzliche Verantwortlichkeiten zu begründen, beispielsweise also bisher noch nicht von Pflichten belegte Akteure in die Pflicht zu nehmen, um so bestehende Defizite auszugleichen. In diese Richtung gehend könnte man auch die oben bereits erwähnte neuere EuGH-Rechtsprechung zur gemeinsamen Verantwortlichkeit interpretieren, die für eine sehr weitreichendere Öffnung des bis dato relativ engen Verantwortlichenbegriffs gesorgt hat. Nicht umsonst begründet der EuGH, beginnend mit seinem Urteil in der Sache Google Spain[557], die Notwendigkeit für seine Öffnung der Verantwortlichkeit regelmäßig mit der Bedeutung einer solch weiten Auslegung der Kriterien für den „wirksamen und umfassenden Schutz der betroffenen Personen".[558] Gleichzeitig demonstriert ebenjene Rechtsprechung jedoch auch die Probleme, die mit einer solchen Anpassung schnell einhergehen. Wo vorschnell über Tatbestandsvoraussetzungen disponiert wird, die über die Pflichtigkeit eines Akteurs entscheiden, ohne die Änderungen hinreichend zu schärfen und sich ausreichend Gedanken über die Konsequenzen zu machen, droht Rechtsunsicherheit und damit – ironischerweise – eine (weitere) Schwächung bereits defizitärer Prämissen.

---

[556] Siehe etwa *Hoffmann-Riem*, in: Hoffmann-Riem, Big Data: regulative Herausforderungen, S. 11 (55) m. w. N. für den Ansatz einer Neubestimmung des Begriffs personenbezogener Daten.

[557] EuGH Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317.

[558] EuGH Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317 Rn. 34.

Hinsichtlich der gemeinsamen Verantwortlichkeit – der sich Abschnitt C. in diesem Kapitel widmen wird – nach derzeitigem Verständnis des EuGH bedeutet dies große Unsicherheit darüber, wer nun zum Kreis der Verantwortlichen gehört oder nicht. Damit einher gehen, je nach Interpretation der Reichweite der Verantwortlichkeit, auch Defizite der ersten Prämisse, also der tatsächlichen Fähigkeit Verantwortlicher, die von ihnen erwarteten Dinge zu leisten, den von ihnen erwarteten Einfluss zu erbringen. Den derzeit besonders aktuellen und öffentlichkeitswirksamen Fall, der die Problematik in all ihren Facetten verdeutlicht, stellt die Entscheidung des Baden-Württembergischen Landesdatenschutzbeauftragten dar, den von ihm betriebenen und bis dato sehr aktiven und um Beantwortung von Fragen der Bevölkerung und von Verantwortlichen bemühten Twitter-Account aufzugeben.[559] Seine Begründung: Er sei infolge der EuGH-Rechtsprechung gemeinsam mit Twitter für deren Verarbeitung von Besucherdaten zu Analysezwecken verantwortlich und könne mangels hinreichender Informationen von Seiten Twitters seinen Pflichten gegenüber Besuchern seines Accounts nicht nachkommen. Der Betrieb seines Accounts sei somit datenschutzwidrig.[560] Jede der Ansichten, auf die sich seine Entscheidung stützt (Übertragung der Wertung aus den EuGH-Urteilen auf andere soziale Netzwerke, Reichweite der Pflichten der jeweiligen Verantwortlichen in solchen Fällen, Haftung des einen Verantwortlichen für mögliche Verstöße des anderen) ist höchst umstritten, doch die negativen Folgen dieser Ungewissheit bleiben zunächst bestehen.

Bevor nun die Voraussetzungen der Verantwortlichkeit – und damit insbesondere die Weite dieser Figur unter Zugrundelegung der jüngsten EuGH-Rechtsprechung – in Abschnitt C. erläutert werden, widmet sich der folgende Abschnitt zunächst der Frage, welche Grenzen dem Verordnungsgeber durch Unionsprimärrecht und andere Quellen hinsichtlich der Ausgestaltung des Konzepts der Verantwortlichkeit gesetzt werden.

III. Ausmaß legislativer Gestaltungsfreiheit zwischen verfassungsrechtlicher Determinierung und rechtspolitischer Gebotenheit

Nach dem Ergebnis der in Abschnitt A dieses Kapitels vorgenommenen Untersuchung von Regelungszweck und grundrechtlichem Schutzgut besteht nur eine geringe grundrechtliche Determinierung des privaten Datenschutzrechts. Die Ausgestaltung einer (private Datenverarbeitungen) strukturierenden Regulierung und die konkrete Wahl der dieser zugrundeliegenden Regelungskonzepte liegt damit größtenteils in der freien Hand des europäischen Verord-

[559] Siehe *Hoffmann* u. a., ZD 2013, 122 (125) zur generellen Frage der Zulässigkeit der behördlichen Nutzung sozialer Medien.

[560] Siehe dazu auch *Stadler*, Kann man noch datenschutzkonform twittern?

nungsgebers.[561] Fraglich ist aber, gerade mit Blick auf die soeben identifizierten Grundprämissen der Verantwortlichenfigur, wo dieser grundsätzlich weite Einschätzungs- und Gestaltungsspielraum in Bezug auf das gewählte Regelungskonzept seine Grenzen findet. Diese Erkenntnis ist nötig, um im Rahmen des in Kapitel 3 folgenden Abgleichs zwischen den Prämissen des Verantwortlichkeitskonzepts und der in Kapitel 1 beschriebenen heutigen Verarbeitungsrealität ggf. festgestellte Dysfunktionalitäten und Wirkungsdefizite des Verantwortlichkeitskonzept als mögliche Verstöße gegen diese Grenzen einordnen und damit eine Pflicht zum Handeln herleiten zu können.

1. Kohärentes Gesamtkonzept/Nachbesserungspflicht

Wie bereits festgestellt, ist der von der DSGVO und bereits der DSRL verfolgte Weg eines umfassenden Verbots aller privaten Datenverarbeitungen in Verbindung mit einem (zugegeben durchaus weitreichende Erlaubnistatbestände bereitstellendem) Erlaubnisvorbehalt[562] nicht zwingend. Hat der Gesetzgeber sich aber für ein solches als Grundkonzept entschieden, so könnte es naheliegen, die Existenz eines Gewährleistungsgebots anzuerkennen, das den Gesetzgeber verpflichtet, im Rahmen dieses Konzepts gewisse Mindeststandards einzuhalten. Auch ein weiter Gestaltungs- und Regulierungsspielraum ermächtigt nicht zum Erlass eines willkürlichen oder zur Erfüllung seines selbst formulierten Zwecks gänzlich ungeeigneten, in seiner Gesamtheit und Einbettung in sein mittelbares und unmittelbares Regelungsumfeld inkohärenten, Gesetzes. Dies lässt sich aus zwei Richtungen denken: einerseits aus Perspektive der Datenverarbeiter hinsichtlich der Verhinderung einer übermäßigen, unnötigen (im Sinne von: nicht zum Ziel der Regelung beitragenden) und bei Vollzugsdefiziten auch unfairen (im Sinne von: nicht alle grundsätzlich gleichen Verarbeitenden gleichmäßig betreffenden) Belastung, andererseits aus Perspektive der Betroffenen hinsichtlich der Optimierung ineffizienter oder gar nicht funktionierender Schutzkonzepte.[563] Insbesondere die letztgenannte, betroffenenzentrierte Perspektive lässt sich als Ausprägung der von *Marsch* beschriebenen Ausgestaltungsdimension von Art. 8 GrCh verstehen.[564] Ein effizientes Gesetz ist nach diesen beiden Perspektiven also eines, das seinen Schutzzweck bei möglichst geringer Eingriffsintensität möglichst weitgehend erfüllt.

---

[561] Vgl. *Reinhardt*, AöR 2017, 528 (556): „Art. 8 GRCh gebietet kein spezifisches Datenschutzkonzept, sondern enthält deutungsoffene Prinzipien."

[562] Aufgrund der weitreichenden Erlaubnistatbestände wird die Bezeichnung zuweilen als irreführend kritisiert, siehe etwa *Albers/Veit*, in: BeckOK Datenschutzrecht Art. 6 DSGVO Rn. 12. *Roßnagel*, NJW 2019, 1 (5); zu den verschiedenen Formen von Verboten mit Erlaubnisvorbehalten außerdem *Grabitz*, AöR 1973, 568 (612 f.).

[563] Als möglicher dritter Blickwinkel ließe sich die Perspektive der Verwaltung unter der Prämisse einer möglichst effizienten und günstigen Aufgabenerfüllung hinzunehmen.

[564] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, S. 130 f. sowie die Ausführungen *supra* bei A. I. 1. a) bb).

Diskutiert werden sollen im Folgenden daher mögliche Grenzen, die sich auf dem Zusammenspiel zwischen Gesetzeszweck und vom Gesetzgeber gewähltem Gesamtkonzept zur Erfüllung des Zwecks begründen. Die eine, insbesondere, aber nicht nur bei Erlass des Gesetzes relevante Frage betrifft die Verhältnismäßigkeit des Gesetzes, *in concreto* seine Geeignetheit zur Erfüllung des Gesetzeszwecks. Die zweite denkbare Grenze könnte sich anhand der Rechtsfigur der Nachbesserungspflicht des Gesetzgebers[565] diskutieren lassen.

a) Bei Erlass des Gesetzes – Untergrenze „Verhältnismäßigkeit"

So frei der Gesetzgeber bei der Wahl seines Regelungskonzepts auch ist, muss er doch im Rahmen dieser von ihm selbst gesetzten Parameter dafür Sorge tragen, dass das Konzept seiner Wahl in sich schlüssig ist. Unionsprimärrechtlich lässt sich diese Grenze dogmatisch an das in Art. 52 Abs. 1 S. 2 GRCh verankerte[566] und darüber hinaus im Rahmen allgemeiner Rechtsgrundsätze anerkannte[567] Verhältnismäßigkeitsprinzip[568] und insbesondere das darin enthaltene Gebot der Geeignetheit und Erforderlichkeit andocken.[569] Eine legislative Maßnahme muss, jedenfalls dort, wo sie (Unions-)Grundrechte tangiert, stets

[565] Ausführlich zu dieser Rechtsfigur im deutschen Verfassungsrecht, unter anderem *Mayer*, Die Nachbesserungspflicht des Gesetzgebers; *Choi*, Die Pflicht des Gesetzgebers zur Beseitigung von Gesetzesmängeln; *Murswiek*, Die staatliche Verantwortung für die Risiken der Technik; *Ossenbühl*, in: Starck/Drath, Bundesverfassungsgericht und Grundgesetz: Festgabe aus Anlaß des 25-jährigen Bestehens des Bundesverfassungsgerichts, S. 458; *Badura*, in: Müller/Eichenberger, Staatsorganisation und Staatsfunktionen im Wandel: Festschrift für Kurt Eichenberger zum 60. Geburtstag, S. 481; *Steinberg*, Der Staat 1987, 161; für die eher spärliche, aber zumindest vorhandene Existenz der Figur im Unionsrecht siehe *Schwerdtfeger*, in: Meyer/Hölscheidt, GRCH, Art. 52 Rn. 43 mit Verweis auf EuGH Rs. C-101/12 (Schaible), ECLI:EU:C:2013:661 Rn. 94 und EuGH Rs. C-127/07 (Arcelor Atlantique und Lorraine u. a.), ECLI:EU:C:2008:728 Rn. 62.

[566] Der in Art. 5 Abs. 4 AEUV normierte Verhältnismäßigkeitsgrundsatz ist kompetenzbezogen, regelt also das Verhältnis zwischen Union und Mitgliedstaaten. Vgl. *Trstenjak/Beysen*, EuR 2012, 265 (274 ff.).

[567] Siehe die Ausführungen in EuGH Rs. C-184/02 (Spanien/P), Slg. 2004, I-7789 Rn. 52; EuGH Rs. C-453/03 (Fratelli), Slg. 2005, I-10423 Rn. 87; EuGH Rs. C-28/05 (Dokter), Slg. 2006, I-5421 Rn. 75; EuGH Rs. C-120/06 (Montecchio), Slg. 2008, I-6513 Rn. 183. Vgl. auch *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 159.

[568] Instruktiv hierzu insgesamt *Riedel*, Die Grundrechtsprüfung durch den EuGH.

[569] Das Ausmaß an (In-)Kongruenz zwischen deutschem und unionsrechtlichem Verhältnismäßigkeitsprinzip ist umstritten. Die wohl hM sieht aber einen inhaltlichen nahezu Gleichlauf, auch wenn die systematische Trennung der drei Prüfungsstufen nicht immer klar ersichtlich ist. *Kischel*, EuR 2000, 380 (390 ff.) etwa sieht die einzelnen nach deutscher Tradition „konstituierenden Merkmale" sowie die Grundstruktur der Verhältnismäßigkeit auch in der Rechtsprechung des EuGH durscheinen. Ähnlich *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 211 f.; a. A. *Stein*, EuZW 1998, 261 (262), der eine Verkürzung auf das Merkmal der Geeignetheit moniert.

einen legitimen Zweck verfolgen.[570] Unionsrechtlich ergibt sich dies unmittelbar aus Art. 52 Abs. 1 S. 2 GRCh, der konkret und abschließend das Gemeinwohl und den Schutz von Individualpositionen als legitime Interessenkategorien benennt.[571] Hat der Unionsgesetzgeber eine darunter passende Zielsetzung definiert bzw. die entsprechende Kompetenzgrundlage ausgewählt, muss die von ihm gewählte Ausgestaltung des Gesetzes und das gewählte Konzept darin zudem geeignet sein, dieses Ziel zwar nicht zwingend gänzlich zu erreichen, sich ihm aber jedenfalls anzunähern bzw. die Wahrscheinlichkeit eines Erfolgseintritts erhöhen.[572] Ist das Gesetz dafür offensichtlich ungeeignet, so kann es schon nicht verhältnismäßig sein.[573] Darüber hinaus verlangt der EuGH, jedenfalls bei der Prüfung der speziellen Gleichheitsgrundrechte, dass die infrage stehende Regelung versucht, das Ziel „in kohärenter und systematischer Weise“[574] zu erreichen.[575] Auch geprüft wird inhaltlich die – praktisch meist relevantere[576] – Frage nach der Erforderlichkeit der gesetzlichen Maßnahme, also die Prüfung hin auf ein mögliches alternatives milderes Mittel.[577] Aufgrund der fehlenden Trennschärfe bei der Bezeichnung der Prüfungsabschnitte finden sich hier häufig[578] außerdem Elemente einer Angemessenheitsprüfung.[579]

---

[570] Die Bedeutung dieses Merkmals im Vergleich zum deutschen Recht dürfte jedoch eher gering sein, da die von Art. 5 EUV und insbesondere dem dort verankerten Prinzip der begrenzten Einzelermächtigung aufgestellte Kompetenzordnung sowieso für jeden Unionsrechtsakt eine ausdrückliche Kompetenzgrundlage innerhalb der Verträge fordert, ein Tätigwerden ohne Verfolgung eines legitimen Zwecks also schwer vorstellbar ist. Entsprechend ist das Merkmal auch praktisch kein Prüfungsteil im (zugegeben unsystematischen) Prüfungsaufbau des EuGH. Vgl. *Calliess*, in: Calliess/Ruffert, EUV/AEUV, Art. 5 EUV Rn. 9; vgl. Bast, in: Grabitz u. a., Das Recht der Europäischen Union, Art. 5 EUV Rn. 14a; ausführlich zu der interessenbezogenen Prüfungspraxis des EuGH *Riedel*, Die Grundrechtsprüfung durch den EuGH, S. 149 ff.

[571] Vgl. *Riedel*, Die Grundrechtsprüfung durch den EuGH, S. 152.

[572] Vgl. in Bezug auf das deutsche Verfassungsrecht *Grzeszick*, in: Dürig u. a., GG, Art. 20 Rn. 112; *Huster/Rux*, in: BeckOK Grundgesetz, Art. 20 Rn. 194 ff.; auch im Rahmen der GRCh genügt bereits ein Beitrag zur Zielerreichung, siehe *Jarass*, in: Jarass, Grundrechtecharta, Art. 52 Rn. 37 f.

[573] Siehe etwa EuGH Rs. 40/72 (Schroeder/Deutschland), Slg. 1973, 125 Rn. 14 sowie *Calliess*, in: Calliess/Ruffert, EUV/AEUV, Art. 5 AEUV Rn. 45 m. w. N. Vgl. auch *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 200 f.

[574] EuGH Rs. C-159/10 (Fuchs), Slg. 2011, I-6919 Rn. 85; EuGH C-123/10 (Brachner), Slg. 2011, I-10003 Rn. 71.

[575] Vgl. *Riedel*, Die Grundrechtsprüfung durch den EuGH, S. 156 f.

[576] Vgl. *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 209 ff. m. w. N., wobei es in den meisten vom EuGH entschiedenen Fällen um mitgliedstaatliche Maßnahmen und nicht, wie hier, um solche von EU-Institutionen geht.

[577] Vgl. EuGH Rs. C-180/96 R (Großbritannien/Kommission), Slg. 1998, I-3903.

[578] Nämlich immer dann, wenn der EuGH keine explizite, eigens geprüfte Angemessenheitsprüfung vornimmt. Vgl. EuG Rs. T390/94 R (Schröder).

[579] Siehe insbesondere EuG, verb. Rs. T-125, 152/96 (Boehringer), Slg. 1999, II-3427.

Für die von der DSGVO (jedenfalls hinsichtlich ihrer Anwendung auf private Datenverarbeitungen) primär betroffenen Grundrechte in Art. 7 und 8 GRCh einerseits und Art. 16 GRCh[580] andererseits lässt sich dies so formulieren: Ein gänzlich zur grundsätzlichen Strukturierung privater Datenverarbeitungen ungeeignetes Gesetz hegt die für Betroffene entstehenden abstrakten Gefahren nicht ein und belastet gleichzeitig unverhältnismäßig stark die unternehmerische Freiheit von Verantwortlichen. Da die Regelung privater Datenverarbeitungen in jedem Fall eine Beschränkung der Unionsgrundrechte von Datenverarbeitern darstellt, musste hier zudem darauf geachtet werden, dass es kein weniger belastendes als das eingesetzte Regelungskonzept mit vergleichbarer Wirksamkeitsprognose zum Zeitpunkt der Gesetzgebung gab,[581] und dass der verfolgte Zweck in einem angemessenen Verhältnis zu dem gewählten Regelungskonzept stand. Besondere Berücksichtigung im Rahmen der Abwägung muss hier aber Art. 8 Abs. 1 GRCh zuteil kommen, aus dem eine gewisse Vorprägung folgt: „Der Korridor, der sich dem Gesetzgeber eröffnet, […] wird durch die Strukturierungsermächtigung des Art. 8 Abs. 1 GRC zugunsten der Betroffenen und damit zu Lasten der Datenverarbeiter verschoben."[582] Damit ist also zu konstatieren, dass das Unionsprimärrecht den Interessen derer, deren Daten verarbeitet werden, die grundsätzliche Vermutung eines gewissen Vorrangs einräumt und dem Gesetzgeber hinsichtlich der Angemessenheit der Maßnahme einen vergleichsweise weiten Gestaltungsspielraum einräumt. Von größerer Bedeutung sind hier daher die Merkmale der Geeignetheit und der Erforderlichkeit.

In welchem Umfang dabei die gesetzgeberische Geeignetheitseinschätzung gerichtlich überprüft werden darf, ist strittig. Hinsichtlich der Frage der eigenen Prüfungskompetenz hat auf Ebene des deutschen Verfassungsrechts das BVerfG hierzu die sogenannte Drei-Stufen-Lehre entwickelt, nach der vom Gesetzgeber getroffene Tatsachenfeststellungen und Prognoseentscheidungen durch das Gericht, je nach konkreten Umständen des Einzelfalls,[583] einem abgestuften Prüfungsumfang unterworfen werden dürfen. Dieser reicht von einer bloßen Evidenzkontrolle[584] (offensichtlich unhaltbare Einschätzungen) über eine Vertretbarkeitskontrolle[585] bis hin zu einer intensivierten inhaltlichen

---

[580] Siehe zum Schutz der unternehmerischen Freiheit von Datenverarbeitern am Beispiel von Google BVerfG, Beschluss v. 06.11.2019, 1 BvR 276/17 Rn. 103 ff.

[581] Vgl. *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 208.

[582] *Marsch*, Das europäische Datenschutzgrundrecht, S. 269.

[583] Diese sollen abhängig sein „im Besonderen von der Eigenart des in Rede stehenden Sachbereichs, den Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden, und der Bedeutung der auf dem Spiele stehenden Rechtsgüter", BVerfGE 106, 62 (152).

[584] Siehe die Entscheidungen zum Grundlagenvertrag und zum Stabilisierungsfonds, BVerfGE 36, 1 (17) und BVerfGE 37, 1 (20).

[585] Zuletzt etwa BVerfG, 18.07.2019 – 1 BvL 1/18, BvL 4/18, 1 BvR 1595/18 Rn. 117 =

Kontrolle.[586] Hinter dieser abgestuften Zurückhaltung steht die grundsätzlich anzuerkennende Gestaltungsfreiheit des Gesetzgebers und letztlich die Gewaltenteilung zwischen Legislative und Judikative: Nur dort, wo es aus verfassungsrechtlichen Gründen zwingend nötig ist, darf das Gericht in die gesetzgeberische Wahlfreiheit bzgl. der Erfüllung der von einem Gesetz verfolgten Ziele eingreifen.[587]

Eine ähnliche Linie verfolgt der EuGH, wenn er im Rahmen von Geeignetheit und Erforderlichkeit einer Maßnahme letztlich gesetzgeberische Prognoseentscheidungen über den Kausalverlauf des gewählten Konzepts bzw. über hypothetische Kausalverlaufe alternativer Konzepte, die nicht gewählt wurden, überprüft.[588] Auch hier hängt die Kontrolldichte von Faktoren wie dem betroffenen Sachbereich, Art und Schwere des Eingriffs und der Natur der betroffenen Grundrechte ab.[589] Während insbesondere bei personalen Grundrechten (wie denen auf Leben oder körperliche Unversehrtheit) ob ihrer herausgehobenen Bedeutung eine hohe Kontrolldichte vorliegt[590], nimmt sich der EuGH bei „wirtschaftspolitischen" Maßnahmen und ihren häufig komplexen Materien,[591] die zudem in erster Linie Wirtschaftsgrundrechte oder Grundfreiheiten betreffen, stark zurück.[592] Eine solche thematisch bedingt eingeschränkte Kontrolldichte ist nach bisheriger Rechtsprechung umso mehr anzunehmen, wenn es nicht um mitgliedstaatliche, sondern um Gemeinschaftsmaßnahmen geht. Effektiv prüft der EuGH hier allein die etwaige Offensichtlichkeit einer fehlerhaften Prognose zum Zeitpunkt des Gesetzeserlasses und konstatiert, dass eine Unverhältnismäßigkeit der Maßnahme erst dann vorliegt, „wenn diese Maßnahme zur Erreichung des Zieles, das das zuständige Organ verfolgt, offensichtlich ungeeignet ist."[593]

NZM 2019, 676 (687) zur Frage der Verfassungsmäßigkeit von Bundesregelung und Berliner Landesregelung in Sachen „Mietpreisbremse".

[586] Siehe etwa BVerfGE 7, 377, BVerfGE 39, 1, BVerfGE 45, 187, BVerfGE 71, 364 (397) und BVerfGE 88, 87 (97).

[587] Dies gilt umso mehr infolge immer differenzierender Rechtsfolgen von BVerfG-Entscheidungen mit zunehmend starker eigener Gestaltungswirkung, vgl. *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 96 f.

[588] Vgl. *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 207 ff.

[589] Vgl. EuGH C-293/12 (Digital Rights), ECLI:EU:C:2014:238 Rn. 47.

[590] Vgl. *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 529.

[591] Vgl. EuGH C-296/93 (Frankreich/K), Slg. 1996, I-795 Rn. 31; EuGH C-368/96 (Generics), Slg. 1998, I-7967 Rn. 67; EuGH C-58/08 (Vodafone), Slg. 2010, I-4999 Rn. 52.

[592] *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, S. 527 f.; *Riedel*, Die Grundrechtsprüfung durch den EuGH, S. 156.

[593] Vgl. EuGH Rs. C-280/93 (Deutschland/Kommission), Slg. 1994, I-4973 Rn. 89. Siehe auch *Koch*, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs

Da es sich beim in der DSGVO verkörperten privaten Datenschutzrecht um eine komplexe wirtschaftspolitische (im weiteren Sinne) Materie handelt, die in erster Linie Wirtschaftsgrundrechte betrifft, ist daher auch hier davon auszugehen, dass die gesetzgeberische Prognoseentscheidung bzgl. Geeignetheit und Erforderlichkeit des gewählten Regelungskonzepts nur sehr eingeschränkt anhand des Maßstabs einer offensichtlichen Fehlerhaftigkeit verfassungsrechtlich bzw. -gerichtlich überprüft werden kann.[594] Auch die Berücksichtigung der Tatsache, dass aufgrund des umfassenden Verbots mit Erlaubnisvorbehalt neben Unternehmensfreiheiten durchaus auch private Kommunikation und damit Kommunikationsgrundrechte betroffen sein könnten[595], ändert nichts an den weiteren Faktoren wie der Komplexität der Materie und der historisch generell geringen Kontrolldichte bei Rechtsvorschriften der Unionsorgane. Eine nennenswerte Einschränkung der unionsgesetzgeberischen Gestaltungsfreiheit durch Geeignetheits- und Erforderlichkeitserwägungen ist daher nicht anzunehmen.

b) Nach Erlass des Gesetzes – verfassungsrechtliche Nachbesserungspflicht

Eine Grenze der gesetzgeberischen Einschätzungsprärogative kommt aber nicht nur bei Erlass des Gesetzes in Betracht, sondern kann sich auch danach stetig aktualisieren und unter Umständen dazu verpflichten, die getroffenen Überlegungen in regelmäßigen Abständen mit möglicherweise veränderten Gegebenheiten abzugleichen und das gewählte Konzept ggf. daran anzupassen.[596] Auf EU-Ebene zeugen kurze, nüchterne Feststellungen in zwei Entscheidungen des EuGH davon, dass eine Pflicht zur Nachbesserung von EU-Rechtsakten jedenfalls möglich ist.[597] Da es aber auch hier an weitergehenden dogmatischen Ausarbeitungen mangelt und das Verhältnis zwischen deutschem Verfassungsrecht und einfachem Gesetzesrecht jedenfalls[598] im Grundsatz vergleichbar zu

---

der Europäischen Gemeinschaften, S. 531 m. w. N. *Riedel*, Die Grundrechtsprüfung durch den EuGH, S. 155.

[594] A. A. aber *Reinhardt*, AöR 2017, 528 (549), der insbesondere mit Blick auf das Google Spain-Urteil konstatiert, dass der EuGH „hingegen gerade im Bereich des Daten- und Privatheitsschutzes recht weitgehende Beurteilungskompetenzen wahr[nehme]".

[595] Diesem Einwurf ließe sich zudem mit Art. 85 DSGVO entgegenhalten, dass der (abschließende) Ausgleich mit Kommunikationsgrundrechten durch die DSGVO selbst gar nicht vorgenommen wird, sondern auf die Mitgliedstaaten mit ihren jeweils eigenen diesbezüglichen Maßstäben delegiert wird.

[596] Vgl. BVerfGE 65, 1 (55) und BVerfGE 93, 37 (74).

[597] Siehe die (als solche betitelten) „Hinweise" in EuGH Rs. C-101/12 (Schaible), ECLI:EU:C:2013:661 Rn. 94 und EuGH Rs. C-127/07 (Arcelor At-lantique und Lorraine u. a.), ECLI:EU:C:2008:728 Rn. 62, nach denen der Gemeinschaftsgesetzgeber verpflichtet ist, „insbesondere im Hinblick auf die Ziele der Richtlinie […] und der Gemeinschaftspolitik […] die eingeführten Maßnahmen […] in angemessenen Zeitabständen zu überprüfen". Im zweiten genannten Urteil wurde eine solche Pflicht sekundärrechtlich auch in Art. 30 der überprüften Richtlinie (2003/87) verankert, wie es auch Art. 97 im Rahmen der DSGVO tut.

[598] Trotz aller offensichtlicher Unterschiede, etwa auf Ebene des Gesetzgebungsprozesses.

dem zwischen unionalem Primär- und Sekundärrecht erscheint, sollen die folgenden Überlegungen vor dem Hintergrund der jedenfalls grundsätzlich ausdifferenzierten und durchdachten deutschen Dogmatik, die sich aus jahrelanger Behandlung in Rechtsprechung und Literatur speist, angestellt werden. In diesem Rahmen werden derartige legislative Überwachungs- und Anpassungspflichten – in Literatur und BVerfG-Rechtsprechung bisweilen uneinheitlich – unter dem Topos der Nachbesserungspflicht des Gesetzgebers diskutiert. Verstanden wird darunter meist eine (echte und damit verfassungsrechtliche) Rechtspflicht des Gesetzgebers zur Nachbesserung bzw. Anpassung eines bereits erlassenen Gesetzes. Ob eine solche Rechtspflicht stets eine nachträglich eintretende Verfassungswidrigkeit des betroffenen Gesetzes voraussetzt, wird größtenteils bejaht[599], teils aber auch verneint[600] oder nicht endgültig entschieden[601]. Da die Frage aber die nach einer echten, verbindlichen Rechtspflicht ist, die sich in Bezug auf den Gesetzgeber als Verfassungsorgan bzw. den EU-Gesetzgeber als EU-Organ nur aus der Normenebene des Verfassungs- bzw. Primärrechts ergeben kann, muss im Kern notwendigerweise eine Verfassungswidrigkeit vorliegen. Über die Grundrechte und andere verfassungsrechtlich anerkannte, positiv normierte Prinzipien[602] hinausgehende verfassungsrechtliche Pflichten, etwa zum Erlass eines möglichst „guten", möglichst effizienten Gesetzes, deren Verletzung beachtlich sein könnte, gibt es aber richtigerweise schon zum Zeitpunkt des Gesetzgebungsprozesses nicht[603]: „Der Gesetzgeber schuldet gar nichts anderes als das Gesetz."[604] Nicht anders kann es sich daher bzgl. einer Nachbesserungspflicht verhalten. Ebenfalls nicht anders lässt sich im Ergebnis auch die Erkenntnis aus den betreffenden BVerfG-Entscheidungen der letzten Jahrzehnte beschreiben[605] – stets wurden Verpflichtungen zur Nachbesserungen mit dem erklärten Ziel ausgesprochen, die Rechtslage mit der

---

599 So etwa *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 48 ff., der dies – durchaus überzeugend – darauf zurückführt, dass eine solche Rechtspflicht den Gesetzgeber schon aus Gründen der Normkonkurrenz nur auf der (insofern höheren) Verfassungsebene treffen kann.

600 Siehe *Badura*, in: Müller/Eichenberger, Staatsorganisation und Staatsfunktionen im Wandel: Festschrift für Kurt Eichenberger zum 60. Geburtstag, S. 481 (487); *Ossenbühl*, in: Starck/Drath, Bundesverfassungsgericht und Grundgesetz: Festgabe aus Anlaß des 25-jährigen Bestehens des Bundesverfassungsgerichts, S. 458 (518).

601 Siehe *Steinberg*, Der Staat 1987, 161 (169 ff.).

602 Bspw. das aus Art. 20 Abs. 3 GG bzw. Art. 52 Abs. 1 S. 2 GRCh abgeleitete Bestimmtheitsgebot.

603 Vgl. *Schuppert*, Governance und Rechtsetzung, S. 27 ff.

604 *Schlaich*, in: Die Verfassungsgerichtsbarkeit im Gefüge der Staatsfunktionen. Besteuerung und Eigentum, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer zu Innsbruck vom 01. bis 04. Oktober 1980, S. 103 (109).

605 Ausführlich zur rechtsdogmatischen Herleitung der Bindungswirkung unter Differenzierung zwischen ihrer Aussprache in der Urteilsbegründung und im Tenor des Urteils, siehe *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 75 ff.

Verfassung in Einklang zu bringen[606] oder wurde gar eine konkrete Frist zur Nachbesserung gesetzt[607] (teilweise mit Verweis auf eine sonst bevorstehende Verfassungswidrigkeit der Norm[608]). Die Aussprache einer solchen Pflicht geht dabei regelmäßig Hand in Hand mit der verfassungsgerichtlichen Unvereinbarerklärung des betreffenden Gesetzes in Abgrenzung zur direkten Nichtigerklärung.[609] Verzichtet das BVerfG also auf die Nichtigerklärung eines verfassungswidrigen Gesetzes[610] und erklärt nur die Unvereinbarkeit, dann regelmäßig deshalb, weil die kurzfristige Aufrechterhaltung des verfassungswidrigen Zustandes mit der Aussicht auf baldige Nachbesserung vorzugswürdig gegenüber einer Nichtigkeit mitsamt eines übergangsweisen Regelungsvakuums erscheint. Gleichzeitig stellt das BVerfG klar, dass ein Verfahren mit dem Ergebnis einer solchen Aussprache nicht konstitutiv für das Entstehen einer Nachbesserungspflicht ist, sondern sich diese unmittelbar aus der Verfassung selbst ergibt, sofern die veränderten Umstände eine Nachbesserung verfassungsrechtlich erforderlich machen[611] und dieser Umstand zumindest klar erkennbar ist[612], wobei letzteres im direkten Zusammenhang mit einer Pflicht zur fortlaufenden gesetzgeberischen Kontrolle zu sehen ist.[613]

Einigkeit besteht quer durch alle Literaturansichten im Grundsatz darüber, dass das Auslösen einer solchen Pflicht eine Änderung der „maßgeblichen Umstände“[614] seit dem Zeitpunkt des Gesetzeserlasses voraussetzt. Fraglich ist dabei zweierlei: Welche Art von Umständen spielt dafür eine Rolle? Und wie muss das Ausmaß der Änderung aussehen, um als „maßgeblich“ verstanden zu werden und eine Pflicht zu bedingen? Differenzieren lässt sich hier zunächst zur ersten Frage zwischen Änderungen auf Ebene des Gesetzes selbst bzw. seinem Zusammenspiel mit anderen Gesetzen und Änderungen im Wirkbereich des Gesetzes – in anderen Worten: Veränderungen im Normprogramm und im Normbereich.[615] Beide können eine Nachbesserungspflicht grundsätzlich auslösen.

Auf Ebene des *Normprogramms* können sich veränderte Umstände etwa daraus ergeben, dass sich die Norm selbst oder die Verfassung bzw. das Primärrecht verändern. Auch möglich sind veränderte Umstände, die sich erst aus der

606 Vgl. BVerfGE 82, 60 (97); 82, 126 (155); 87, 153 (178); 90, 263 (276).
607 Vgl. BVerfGE 78, 249 (251).
608 Vgl. BVerfGE 22, 349 (363).
609 *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 77 spricht diesbezüglich anschaulich von der Unvereinbarerklärung als „das Surrogat der Nichtigerklärung“.
610 Etwa aus Gründen der Rechtssicherheit oder weil der Wegfall des Gesetzes die Rechtslage noch weiter von der Verfassung entfernen würde.
611 Vgl. BVerfGE 56, 54 (81).
612 Vgl. BVerfGE 88, 203 (310).
613 Vgl. BVerfGE 65, 1 (66).
614 BVerfGE 59, 336 (357).
615 Vgl. *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 113 ff.; zur Bedeutung der beiden Begriffe siehe *Müller/Christensen*, Juristische Methodik, Band I: Grundlagen Öffentliches Recht, S. 217 ff.

Zusammenschau mehrerer Gesetze ergeben und bewerten lassen, etwa, weil nicht das infrage stehende Gesetz, sondern ein anderes novelliert oder gänzlich neu erlassen wurde und das Zusammenspiel aus beiden eine nunmehr verfassungsrechtlich problematische Lage kreiert.[616] Auch im Datenschutzrecht lässt sich eine nach dieser Kategorie potenziell problematische Lage finden, namentlich das nach Erlass der DSGVO bis dato entstandene Regelungsvakuum in Bezug auf den Schutz von auf Nutzerendgeräten gespeicherten (nicht notwendig personenbezogenen[617]) Daten im Zusammenhang mit Diensten der Informationsgesellschaft. Das bis Mai 2018 bestehende Zusammenspiel zwischen DSRL und ePrivacy-RL fand mit Wirksamwerden der DSGVO sein (vermeintliches) Ende, da die ursprünglich auf einen zeitgleichen Erlass hin geplante ePrivacy-VO[618] nicht rechtzeitig fertig wurde und aufgrund zäher Verhandlungen bis heute in einer Art „Gesetzesentwicklungslimbo" steckt.[619] Da die DSGVO – wie der Name bereits sagt – nur als *Grund*verordnung gedacht ist und von bereichsspezifischen Spezialgesetzen flankiert werden soll[620], wäre es durchaus denkbar, hier eine Pflicht des EU-Gesetzgebers zum baldigen Erlass der ePrivacy-VO anzunehmen, da sonst bei Gesamtschau eine Primärrechtswidrigkeit (hier wohlgemerkt infolge eines *unterlassenen* Gesetzgebungsakts) drohte. Dem wurde durch Art. 95 DSGVO, der einstweilen das Konkurrenzverhältnis der beiden Rechtsakte zugunsten eines Fortgeltens der ePrivacy-RL qua Spezialität auflöst, jedoch bereits präventiv Abhilfe geschaffen. Eine zusätzliche Problematik droht in Deutschland aufgrund der wohl unzureichenden Umsetzung einiger Normen der Richtlinie ins nationale Recht, so etwa bei Art. 5 Abs. 3 ePrivacy-RL respektive § 15 Abs. 3 TMG. Um den Wertungen der Richtliniennorm innerhalb der DSGVO auch in Deutschland zu Wirksamkeit zu verhelfen, wird deshalb vertreten, das Einwilligungserfordernis von Art. 5 Abs. 3 der Richtlinie durch „hereinlesen" in die Abwägung des Art. 6 Abs. 1 lit. f DSGVO zu bewahren.[621]

Änderungen im *Normbereich* kommen dort in Betracht, wo normrelevante Tatsachen sich nach Gesetzeserlass ändern. Dies können mit Blick auf das Prinzip Gewaltenteilung, aber auch auf faktische Grenzen der Überprüfbarkeit,

---

616 So etwa beim Zusammenspiel zwischen Gerichtsorganisation und Besoldungsrecht, vgl. BVerfGE 26, 116 (139) oder zwischen Einkommenssteuerrecht und Bundeskindergeldgesetz bzgl. der Steuerfreiheit des familiären Existenzminimums, vgl. BVerfGE 83, 60 (97).

617 Vgl. Art. 5 Abs. 3 ePrivacy-RL. Wo die DSGVO einen generellen Schutz Betroffener in Bezug auf die Verarbeitung der sie betreffenden personenbezogenen Daten bezweckt, erfassen die (bisherigen und zukünftigen) ePrivacy-Rechtsakte jegliche Daten unabhängig von ihrem Personenbezug und stellen – insofern den Privatsphärenschutz aus Art. 7 GRCh in den Mittelpunkt rückend – zentral auf ihre Belegenheit auf einem Nutzerendgerät ab.

618 Siehe etwa den Normierungsauftrag in Erwg. 173 der DSGVO.

619 Siehe *Hemmert-Halswick*, MMR-Aktuell 2019, 422777.

620 Vgl. die Ausführung von *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 218 ff.

621 *Kremer*, CR 2019, 676, Rn. 50 ff.

nur Tatsachen sein, die sich außerhalb der sog. Einschätzungsprärogative des Gesetzgebers befanden bzw. befinden.[622] Umstände innerhalb dieser Einschätzungsprärogative sind der Bewertung durch das BVerfG entzogen und können somit auch keine Verfassungswidrigkeit begründen. Um die Relevanzschwelle zu überschreiten, müssen grundsätzlich überprüfbare Tatsachen zudem geeignet sein, die verfassungsrechtliche Beurteilung der infrage stehenden Norm so zu beeinflussen, dass das Gesetz auch bei anfänglicher Existenz der Tatsache bzw. anfänglicher Kenntnis des Gesetzgebers um diese als nicht mit der Verfassung in Einklang bewertet worden wäre. Dem gleichgestellt werden Fälle, in denen verfassungsrelevante Umstände bereits von Anfang an vorlagen, aber erst später bekannt wurden.[623] Das BVerfG unterscheidet zudem teilweise danach, ob die verfassungsrelevante Tatsachenänderung für den Gesetzgeber *ex ante* absehbar war oder nicht.[624] Dabei entbindet eine fehlende Absehbarkeit den Gesetzgeber jedoch nicht von einer etwaigen Nachbesserungspflicht, sondern „rettet" ihn vielmehr vor einer automatischen Nichtigkeit des betreffenden Gesetzes.[625] Ein typisches Beispiel für veränderte normrelevante Umstände, das das BVerfG in seiner Entscheidungshistorie mehrfach beschäftigt hat[626], ist die Berechnung von Grundsteuer auf Basis sog. Einheitswerte, die aus Praktikabilitätserwägungen in regelmäßigen Abständen festgesetzt werden, um die Berechnung von Steuersummen auf Kosten realitätsnaher Bewertungen zu vereinfachen. Je länger die letzte periodische Hauptfeststellung zurück liegt, desto mehr führt die Diskrepanz zwischen typisierter Einheitsbewertung und tatsächlichem Wert zu „Ungleichbehandlungen durch Wertverzerrungen"[627]. Ein weiteres Beispiel sind die vom BVerfG festgestellten Verstöße gegen den Gleichbehandlungsgrundsatz in Form der Besteuerungsgleichheit aus Art. 3 Abs. 1 GG durch strukturelle Vollzugsdefizite von Besteuerungstatbeständen.[628]

In Bezug auf die DSGVO könnten solche normrelevanten Umstände beispielsweise darin liegen, dass sich infolge technischer Entwicklungen neue Szenarien ergeben, die zum Zeitpunkt des Gesetzeserlasses noch nicht existierten bzw. absehbar waren. Im Bereich des Datenschutzes, der im Zentrum einer jeden technischen Entwicklung steht und somit in regelmäßigen (gefühlt immer kürzer werdenden) Abständen wieder auf den Prüfstand gestellt wird, ist dies besonders virulent. So verwundert es nicht, dass die DSGVO explizit dem

622 Vgl. *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 117 f.
623 *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 121 f.
624 Vgl. BVerfGE 83, 1 (17) und BVerfGE 25, 1 (12 f.).
625 *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 119.
626 Vgl. BVerfGE 23, 22 (252 ff.); 41, 269 (282 f.) sowie erst kürzlich BVerfGE 148, 147.
627 BVerfGE 148, 147, Leitsatz 3.
628 BVerfGE 84, 239 und 110, 94. Für eine tiefergehende Behandlung der Urteile und der Frage ihrer Übertragbarkeit siehe *Funke*, AöR 2007, 168.

Ideal eines entwicklungsoffenen[629] und risikosensiblen[630] Gesetzes verpflichtet ist. Zahlreiche Normen – insbesondere Verantwortlichenpflichten – sind bewusst abstrakt und offen formuliert und knüpfen nicht an konkret benannte, besonders gefährliche Verarbeitungsarten oder Szenarien an[631], um im Idealfall gerade solche zukünftigen, noch nicht absehbaren technischen Entwicklungen erfassen zu können und so die kaum zu stemmende Notwendigkeit zu verhindern, in regelmäßigen Abständen nachzubessern. Durch die Risikosensibilität werden zudem etwa viele Pflichten in ihrer Reichweite abhängig gemacht von den Umständen des Einzelfalls und dem Risiko, das konkret für Betroffene droht.[632] Gute Beispiele hierfür sind Art. 23 und 24 DSGVO, die die vom Verantwortlichen zu einzusetzenden technischen und organisatorischen Maßnahmen abhängig machen von unter anderem der „unterschiedlichen Eintrittswahrscheinlichkeit" und von der „Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen". Manche Normen finden überhaupt nur Anwendung, sobald ein gewisses Mindestrisiko vorliegt, so etwa die Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung nach Art. 35 DSGVO oder die Pflichten zur Benachrichtigung von Aufsichtsbehörde und Betroffenen bei Datenpannen (sog. *data breaches*) gem. Art. 33 und 34 DSGVO. Das Zusammenspiel dieser beiden Ansätze soll – im Idealfall – dazu führen, dass die DSGVO auf zwei Ebenen für technische Entwicklungen gewappnet ist: Einerseits sollen durch das auf Verantwortlichenseite, aber auch durch die Aufsichtsbehörden[633] stetig wieder neu zu bemessende Risiko auch solche Gefahren pflichtenseitig mit dem bestehenden gesetzlichen Instrumentarium abgedeckt werden, die erst durch zukünftige technische Entwicklungen entstehen. Andererseits sind die Verantwortlichenpflichten oftmals dynamisch daran gekoppelt, was technisch maßnahmenseitig möglich ist (die DSGVO verwendet hier häufig den Begriff des „Stands der Technik", etwa in Art. 25 Abs. 1) und streben so Entwicklungsoffenheit an – Maßnahmen, die heute noch genug für Compliance sind, können

[629] Erwg. Nr. 15 spricht insoweit von der Technologieneutralität des Schutzes natürlicher Personen. Siehe *Albers/Veit*, in: BeckOK Datenschutzrecht, Art. 6 DSGVO Rn. 14 zu diesem Regulierungsansatz und der damit auch einhergehenden Rechtsunsicherheit. Noch kritischer die übermäßige Abstraktion solcher Regelungern betonend *Sydow/Kring*, ZD 2014, 271 (272 f.); ähnlich bzgl. Rechtsunsicherheit durch zu hohe Abstrahierung *Richter*, DuD 2016, 89 (91 f.).

[630] Für eine Bestandsaufnahme dieses Konzepts siehe *Schröder*, ZD 2019, 503 (503 ff.) m. w. N. Für Beispiele risikobasierter Normen siehe *Buchner*, DuD 2016, 155 (157).

[631] Eine Ausnahme von dieser der DSGVO sehr weitgehend zugrundeliegenden Regelungstechnik ist der bereits erwähnte Art. 22, der konkret das Phänomen algorithmenbasierter Entscheidungen adressiert.

[632] Vgl. *Veil*, ZD 2015, 347 (348 ff.) für eine weitere Auflistung und kritische Bewertung der verschiedenen risikosensiblen DSGVO-Normen und Pflichten und eine Systematisierung anhand der Konsequenzen unterschiedlicher Risiken.

[633] Etwa in Form sog. Blacklists, auf denen besonders riskante Verarbeitungsvorgänge verzeichnet werden, die stets die Durchführung einer Datenschutzfolgenabschätzung nötig machen, vgl. Art. 35 Abs. 4 S. 1.

in einem Jahr bereits zu wenig sein. Diesen zukunftsoffenen und dynamischen Ansätzen zum Trotz erscheint es denkbar, dass die DSGVO hinsichtlich der Wirksamkeit ihres Gesamtkonzepts von der technischen Entwicklung überholt wird; dies belegt nicht zuletzt die zahlreich vorhandene Kritik an den eben beschriebenen Ansätzen.[634]

Denkbar ist aber auch eine Überholung bzw. eine fehlende Tragfähigkeit des gesetzgeberischen Gesamtkonzepts dergestalt, dass ursprünglich getroffene Grundannahmen über das Verhalten der vom Konzept betroffenen Akteure, ihre Beziehungsgeflechte, ihre Handlungsmöglichkeiten und grundsätzlichen Fähigkeiten sich im Nachhinein als von Beginn an falsch herausstellen oder aufgrund infolge gesellschaftlicher Entwicklung veränderter Bezugsobjekte jedenfalls nachträglich nicht mehr mit der Realität übereinstimmen. Sobald elementare Prämissen eines Schutz- und Regulierungskonzepts wie das der DSGVO zugrundliegende nicht mehr zutreffen, fehlt es dem gesamten Gesetz bereits grundlegend an der Geeignetheit zur Erfüllung seines Zwecks.[635] Ein weit verbreitetes Beispiel für eine möglicherweise fehlgeleitete, aber für das derzeitige Datenschutzrecht elementare Grundannahme ist die sich im Kern des von der DSGVO stark verfolgten Konzepts des Selbstdatenschutzes befindliche (unterstellte) Möglichkeit des Individuums, rational und selbstbestimmt in die Verarbeitung der ihn betreffenden Daten einzuwilligen. Zwar ist die Einwilligung – entgegen mancher Ansichten[636] und dem gefühlten Rechtsempfinden großer Teile der Öffentlichkeit[637] – weder der einzige[638], noch ein von der DSGVO in der Hierarchie über die anderen Erlaubnistatbestände gestellte[639] „Rechtfertigungsgrund" für Datenverarbeitungen.[640] Dennoch spielt sie in der Praxis faktisch die bedeutendste Rolle[641] und erfährt regelmäßig wiederkeh-

---

634 Vgl. *Veil*, ZD 2015, 347; *Sydow/Kring*, ZD 2014, 271.

635 Vgl. BVerfGE 56, 54 (80 ff.); BVerfGE 77, 170 (215); BVerfGE 79, 174 (202; BVerfGE 85, 191 (212 f.); BVerfGE 92, 26 (46); BVerfGE 121, 317 (360).

636 Differenzierend und die relevanten Stimmen zur Frage eines etwaigen Vorrangs der Einwilligung gegenüber den anderen Rechtsgrundlagen aufzeigend *Schantz*, in: Simitis u. a., DSGVO/BDSG, Art. 6 Abs. 1 DSGVO Rn. 11.

637 Auch hier zeigt sich der nach wie vor große Einfluss des Konzepts der informationellen Selbstbestimmung, das sich durch nichts so stark verkörpern lässt wie durch die individuelle Einwilligung in Datenverarbeitungen.

638 Art. 6 Abs. 1 DSGVO kennt derer nämlich explizit sechs.

639 Im Gegenteil geht die Tendenz eher hin zu einem Zurückdrängen der Einwilligung zugunsten zwingender staatlicher Vorgaben, wie etwa *Hermstrüwer*, Informationelle Selbstgefährdung, S. 69 schön ausführt. In diese Richtung argumentierend auch *Zanfir*, in: Gutwirth/Leenes/de Hert, Reloading Data Protection, S. 237.

640 Vgl. *Frenzel*, in: Paal/Pauly, DSGVO/BDSG, Art. 6 DSGVO, Rn. 10, wonach der Einwilligung „keine eigenständige, die Verarbeitung besser legitimierende, aufwertende Wirkung" gegenüber den anderen Erlaubnistatbeständen zukomme.

641 Vgl. *Reinhardt*, AöR 2017, 528 (557): „Im Fall der Datenverarbeitung durch private Unternehmen hingegen hängt regelmäßig von der Zustimmung ab, in welchem Maß und zu welchen Zwecken auf personenbezogene Daten zugegriffen werden kann."

rende und weitreichende Kritik, die sich teilweise auf Marktgegebenheiten[642], teilweise auf Fehlannahmen hinsichtlich Verhalten und Rationalität der Einwilligenden[643] bezieht.[644] Auch hier kommen demnach defizitäre Bereiche des vom Gesetzgeber gewählten Gesamtkonzepts in Betracht, zu deren Beseitigung er verpflichtet ist bzw. sich durch die insofern noch freie Wahl seines Konzeptes selbst verpflichtet hat. Sein zunächst noch sehr weiter Spielraum verengt sich also durch die von ihm selbst vorgenommene Entscheidung für ein bestimmtes Konzept.[645] Bezogen auf den Selbstdatenschutz der Betroffenen heißt das etwa, dass er grundlegend nachvollziehbare Prämissen hinsichtlich der Rationalität und Handlungsfähigkeit der Betroffenen zugrunde legt.[646] Es heißt aber auch, dass er das Gesamtkonzept auf Basis dieser Prämissen legislativ mit Leben füllt und „den Rahmen der Informationsordnung so gestaltet, daß Selbstschutz effektiv möglich ist“[647]. Ein Konzept, das den Einzelnen bei der Wahrnehmung und Ausübung seines Selbstdatenschutzes völlig allein lässt, kann seinen Zweck nicht erfüllen.[648]

Denkbar wäre auch, in Tradition der oben angesprochenen BVerfG-Rechtsprechung[649], das chronische Vollzugsdefizit des Datenschutzrechts[650] als Anknüpfungspunkt für eine Nachbesserungspflicht zu nehmen. Neben der zweifelhaften Tauglichkeit dieser Urteile zur Verallgemeinerung über das Steuerrecht

---

642 Siehe etwa *Kamp/Rost*, DuD 2013, 80 (82 ff.), die auf regelmäßig bestehende Ungleichgewichte zwischen Unternehmen und Einwilligungen erteilenden Betroffenen sowie auf falsche Annahmen bzw. Freiwilligkeit und Informiertheit hinweisen. Ähnlich auch *Becker*, JZ 2017, 170 (174 f.); zu den Grenzen der Freiwilligkeit im Rahmen der DSGVO siehe auch *Borgesius* u. a., EDPL 2017, 353.

643 Ausführlich dazu *Hermstrüwer*, Informationelle Selbstgefährdung, S. 227 ff., 319 ff., 383 ff., der die fehlende Rationalität auf strategische und kognitive Einwilligungsrestriktionen zurückführt. Für empirische Untersuchungen zur rationalen Verarbeitung von Informationen, etwa durch Datenschutzerklärungen, siehe weiter *Ben-Shahar/Schneider*, More than you wanted to know; *Vila* u. a., in: Camp/Lewis, Economics of information security, S. 143; *Adams*, J. L. Inf. & Sci. 2014, 158 (159 ff.); *Solove*, Harv. L. Rev. 2013, 1880 (1883 ff.).

644 Siehe *Bunnenberg*, Privates Datenschutzrecht, S. 85 ff. für einen Überblick über die mannigfaltigen Regulierungsherausforderungen im Zusammenhang mit der Einwilligung.

645 Ähnlich auch *Mayer*, Die Nachbesserungspflicht des Gesetzgebers, S. 47, der davon spricht, dass in Fällen von gesetzgeberischen Nachbesserungspflichten „dieser Zwang erst indirekt durch die Legislative selbst hervorgerufen wird“.

646 Ob diese in Anbetracht der *supra* genannten mannigfaltigen wissenschaftlichen Kritik noch als gegeben hingenommen werden kann, soll hier dahinstehen.

647 *Hoffmann-Riem*, AöR 1998, 513 (534); dazu gehört bspw. auch die hinreichende Bildung der Bevölkerung in Sachen Selbstschutzmöglichkeiten und Sensibilität für Risiken und Gefahren, vgl. *Wagner*, DuD 2012, 83 (84 f.).

648 Vgl. *Richter*, DuD 2016, 89 (92); In eine ähnliche Richtung gehend *Hermstrüwer*, Informationelle Selbstgefährdung, S. 33, der – bezogen auf das Recht auf informationelle Selbstbestimmung – eine dynamische Anpassung der rechtlichen Schutzvoraussetzungen an den tatsächlichen Umgang mit und die Wertschätzung für Daten bzw. Privatheit fordert. Siehe ferner *Bäcker*, Der Staat 2012, 91 (105 f.); *Grimm*, JZ 2013, 585 (588).

649 BVerfGE 84, 239 und 110, 94.

650 Siehe hier etwa *Lepperhoff* u. a., DuD 2012, 195 (195 ff.).

hinaus,[651] ist aber sehr fraglich, ob dieses Defizit bereits das Ausmaß eines *strukturellen* Defizits angenommen hat.[652]

Der materielle Bezugspunkt für die Beurteilung, ob veränderte (und nicht in die Einschätzungsprärogative des Gesetzgebers fallende) Umstände eine verfassungsrechtliche bzw. unionsprimärrechtliche Neubeurteilung und Pflicht zur Nachbesserung auslösen, ist, wie bereits beschrieben, die Vereinbarkeit des Gesetzes unter Berücksichtigung der neuen oder neu bekannt gewordenen Umstände mit der Verfassung bzw. dem Unionsprimärrecht. Die Existenz und Anerkennung einer Beobachtungs- und Nachbesserungspflicht des Gesetzgebers auch nach Erlass eines Unionsrechtsakts wie der DSGVO grenzt diesen daher materiell nicht weiter ein, als es das Unionsprimärrecht (insbesondere in Form von Grundrechte und Grundfreiheiten) ohnehin schon tut.[653] Es erweitert diese (wie eingangs beschrieben geringe) primärrechtliche Determinierung aber um eine zeitliche Dimension, die im von technischen und ökonomischen Entwicklungen wie auch gesellschaftlichen Veränderungen und Anpassungstendenzen so stark wie kaum ein anderes Regelungsgebiet geprägten Datenschutzrecht von besonders großer Bedeutung ist. Der Regelungsansatz des EU-Verordnungsgebers, die DSGVO einer risikosensiblen und technologieoffenen Systematik zu unterworfen, darf als Versuch verstanden werden, diesen Entwicklungstendenzen ein Instrument entgegenzusetzen, das im Idealfall in der Lage ist, die auf Dauer zwingend notwendigen Anpassungen organisch vorzunehmen. Ob dies (vollends) gelingt, bleibt abzuwarten – und wird bereits zuweilen angezweifelt.[654] Dass auch von gesetzgeberischer Seite nicht davon ausgegangen wird, damit gänzlich frei von zukünftigen Nachbesserungen zu sein, zeigt der Mechanismus des Art. 97 DSGVO.

2. Schutz vor höheren Gefahrenpotentialen

Eine tatsächlich inhaltliche Grenze erfährt die, wie beschrieben grundsätzlich sehr geringe, verfassungsrechtliche Determinierung des privaten Datenschutzes dort, wo in einzelnen seiner Regelungsgebiete höhere Gefahrenpotentiale bestehen. Die Tatsache, dass auf der untersten Ebene des Schutzzwecks „nur" die aus Art. 8 Abs. 1 GRCh abgeleitete Strukturierungsermächtigung des Gesetzgebers steht, darf nicht darüber hinwegtäuschen, dass im Rahmen privater Datenver-

---

[651] Einen guten Überblick über den entsprechenden Streitstand liefert *Funke*, AöR 2007, 168 (168).

[652] Siehe zur Differenzierung der beiden Begriffe *Funke*, AöR 2007, 168 (172 ff.).

[653] Es ließe sich, wenn überhaupt, genau andersherum argumentieren, dass in Fällen von Prognoseentscheidungen und komplexen Sachzusammenhängen die Existenz bzw. das Zugestehen einer Beobachtungs- und Nachbesserungspflicht den ursprünglichen Spielraum des Gesetzgebers bei Erlass des Gesetzes *vergrößert*, indem ihm zugebilligt wird, trotz unklarer Tatsachenbasis tätig zu werden, *sofern* er die Tauglichkeit des gewählten Konzeptes fortlaufend evaluiert und ggf. nachbessert. Vgl. BVerfGE 88, 203 ff. (254, 263, 310).

[654] Vgl. etwa *Veil*, ZD 2015, 347 (348 ff.); *Schröder*, ZD 2019, 503 (503 ff.).

arbeitungen auch Gefahrenlagen denkbar sind, die die freiheitsakzessorische Dimension des europäischen Datenschutzgrundrechts betreffen und somit gesetzgeberische Schutzpflichten aktivieren.

Die in der deutschen Grundrechtsdogmatik in Rechtsprechung und Literatur breit anerkannte Schutzpflichtendimension der Grundrechte[655] als Ausdruck der objektiven Werteordnung der Grundrechte bzw. Elemente objektiver Ordnung[656] findet inzwischen auch auf Unionsebene eine grundsätzliche Anerkennungsbasis in Literatur[657] und EuGH-Rechtsprechung.[658] Da es aber „bislang an einer dezidierten Entfaltung des Schutzpflichtenkonzepts auf Unionsebene“[659] und somit einer hinreichend ausdifferenzierten Dogmatik fehlt, sollen dennoch auch hier für die inhaltlichen Details primär die Ausführungen in der deutschen Dogmatik und Literatur näher untersucht werden.[660]

Grundlegend soll die Schutzpflichtenebene der Grundrechte den Staat im Privatrecht dort zum gesetzgeberischen Handeln verpflichten, wo das Individuum vor Übergriffen anderer Privater geschützt werden muss.[661] Wann eine derartige Notwendigkeit besteht, hängt vom infrage stehenden Grundrecht und der im konkreten Gefahrenszenario bestehenden Möglichkeit zu privatautonomem Selbstschutz ab.[662] Nach gängiger Dogmatik ist von einer solchen Aktivierung der Schutzpflichtendimension im privatrechtlichen Bereich beispielsweise dann

---

655 Ein grundlegender chronologischer Aufriss findet sich bei *Stern*, DÖV 2010, 241; instruktiv auch *Bumke*, AöR 2019, 1 (3 ff.).

656 So explizit etwa in BVerfGE 53, 30 (57); 56, 54 (73); 73, 261 (269); 77, 170 (214); 92, 26 (46).

657 Siehe *Suerbaum*, EuR 2003, 390 (392 f.); *Gersdorf*, AöR 1994, 400 (402 ff.); *Stoppel*, Grundfreiheitliche Schutzpflichten der Mitgliedstaaten im Europäischen Gemeinschaftsrecht; außerdem *Calliess*, in: Calliess/Ruffert, EUV/AEUV, Art. 1 GRCh Rn. 5 m. w. N. zu impliziter Anerkennung im Rahmen der Beeinträchtigung positiver Pflichten; weiter *Jarass*, in: Jarass, Grundrechtecharta, Art. 52 Rn. 17; allgemeiner zur mittelbaren Drittwirkung von Grundrechten im Unionsrecht *Walkila*, Horizontal effect of fundamental rights in EU law; *Unseld*, Zur Bedeutung der Horizontalwirkung von EU-Grundrechten; *Kühling*, in: von Bogdandy/Bast Europäisches Verfassungsrecht, S. 675 ff.; speziell zu Art. 7 und 8 GRCh *Roßnagel*, NJW 2019, 1 (3).

658 Siehe bspw. EuGH, Rs. C-13/94 (P/S and Cornwall County Council), Slg. 1996, I-2143 Rn. 22 und EuGH, Rs. C-265/95 (Kommission/Frankreich), Slg. 1997, I-6959 Rn. 32.

659 *Greve*, in: Franzius/Lejeune/von Lewinski/Meßerschmidt/Michael/Rossi/Schilling/Wysk, Beharren. Bewegen: Festschrift für Michael Kloepfer zum 70. Geburtstag, S. 665 (676).

660 So etwa auch *Calliess*, in: Calliess/Ruffert, EUV/AEUV, Art. 3 GRCh Rn. 11, der für ein Heranziehen des deutschen Untermaßverbots plädiert. Auch an anderer Stelle, etwa bei *Frenz*, Handbuch Europarecht Band 4, S. 108 ff., wird bei der eigentlich dezidierten Behandlung der grundrechtlichen Schutzpflichten auf europäischer Ebene regelmäßig auf die deutsche Grundrechtsdogmatik zurückgegriffen. Für einen Versuch der Erfassung und Weiterbildung genuin europarechtlicher dogmatischer Grundlagen siehe *Stoppel*, Grundfreiheitliche Schutzpflichten der Mitgliedstaaten im Europäischen Gemeinschaftsrecht, S. 114 ff.

661 Vgl. *Dreier*, in: Dreier, GG Band I, Vorb. Rn. 101. Die nähere Entfaltung der Schutzpflichtendimension geht primär auf das BVerfG zurück, siehe etwa BVerfGE 106, 28 (36 f.); 115, 320 (358 f.); 121, 317 (356 f.); 125, 39 (78 f.); 88, 203 (254 ff.); 96, 409 (412).

662 Vgl. *Canaris*, AcP 1984, 201 (228).

auszugehen, wenn – entgegen dem von der Privatautonomie vorausgesetzten Ideal der grundsätzlichen Gleichordnung der sich gegenüberstehenden Privaten – die strukturelle Unterlegenheit einer Partei, etwa aufgrund einer Kräfte- und Informationsasymmetrie, infrage steht, und dieses Ungleichgewicht nicht bereits durch rechtliche Rahmung, etwa die Bereitstellung von Selbstschutzmöglichkeiten, ausgeglichen wird.[663] Entscheidende Kriterien können insbesondere „die Unausweichlichkeit von Situationen, das Ungleichgewicht zwischen sich gegenüberstehenden Parteien, die gesellschaftliche Bedeutung bestimmter Leistungen oder die soziale Mächtigkeit einer Seite“[664] sein, die dazu führen, dass aus Selbstbestimmung Fremdbestimmung wird.[665] Dabei ist je nach konkreter Gefährdungslage zu bestimmen, ob die im jeweiligen Fall relevante Schwelle überschritten wurde.[666] So führte das BVerfG in Bezug auf das Recht auf informationelle Selbstbestimmung prägnant aus:

„Die aus dem Recht auf informationelle Selbstbestimmung folgende Schutzpflicht gebietet es, dafür Sorge zu tragen, dass informationeller Selbstschutz für Einzelne tatsächlich möglich ist. […] Hat aber in einem Vertragsverhältnis ein Partner ein solches Gewicht, dass er den Vertragsinhalt faktisch einseitig bestimmen kann, so ist es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen der beteiligten Parteien hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt.“[667]

Das vom Gesetzgeber gewählte Grundkonzept – insbesondere ein solch breites wie das der DSGVO – muss daher in der Lage sein, entsprechend der tatsächlich vorliegenden Gefahrenlage hinreichend zu skalieren, um neben den alltäglichen, bloß abstrakten Verarbeitungsgefahren auch größere, konkrete Gefährdungen einzuhegen. Unstrittig ist, dass Einzelfallumstände wie besonders dominante Positionen Privater oder besonders essenzielle von ihnen bereitgestellte Güter zu einer dem Bürger-Staat-Verhältnis vergleichbaren Lage und damit einer entsprechenden privaten Grundrechtsbindung führen können.[668] Auch das BVerfG betont demnach die Möglichkeit einer verfassungs-

---

663 Vgl. *Bäcker*, Der Staat 2012, 91 (105 ff.); siehe zum Vorrang des Selbstschutzes im Rahmen des Rechts auf informationelle Selbstbestimmung auch *Schipper*, Neue Instrumente des Datenschutzrechts für das Verhältnis zwischen Privatperson und Unternehmen in der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika, S. 16 f. Ausführlich zu diesem Thema auch *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, S. 15 ff.; siehe auch *Roßnagel*, NJW 2019, 1 (3): „Diese Verpflichtung ist umso stärker, je weniger der Einzelne die Möglichkeit hat, für einen solchen Schutz selbst zu sorgen.“

664 Vgl. BVerfGE 89, 214 (232 ff.); BVerfGE 128, 226 (249 f.); BVerfGE 148, 267 (280 f. Rn. 33).

665 *Greve*, in: Franzius/Lejeune/von Lewinski/Meßerschmidt/Michael/Rossi/Schilling/Wysk, Beharren. Bewegen: Festschrift für Michael Kloepfer zum 70. Geburtstag, S. 665 (673).

666 Vgl. *Hermstrüwer*, Informationelle Selbstgefährdung, S. 57 m. w. N.

667 BVerfG, Beschluss v. 17.07.2013, 1 BvR 3167/08, Rn. 20.

668 Vgl. BVerfGE 128, 226 (249 f.).

rechtlichen Gebotenheit einer grundlegenden gesetzlichen Ausgestaltung solcher Beziehungen:

„Insoweit können auch hier strenge Strukturierungsanforderungen an die Datenverarbeitung und die Anknüpfung an Zweck und Zweckbindungen – insbesondere etwa in Wechselwirkung mit Einwilligungserfordernissen – geeignete und möglicherweise verfassungsrechtlich gebotene Mittel zum Schutz der informationellen Selbstbestimmung sein."[669]

Bei seiner Entscheidung, auf welche Weise er den Gefährdungen entgegenzuwirken gedenkt, steht dem Gesetzgeber dann jedoch, nicht zuletzt begründet durch Aspekte der Gewaltenteilung,[670] ein grundsätzlich sehr weiter Gestaltungs- und Einschätzungsspielraum zu.[671] So bedingt die aktivierte Schutzpflicht eines Grundrechts regelmäßig allein das „Ob" eines Tätigwerdens zum Schutze der Bürger, nicht aber auch ein konkretes „Wie":[672] „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."[673] Auch hier urteilt das BVerfG in Bezug auf das Recht auf informationelle Selbstbestimmung: „Das Grundgesetz gibt eine konkrete Ausgestaltung des Schutzes der informationellen Selbstbestimmung nicht vor."[674] Nichtsdestotrotz kann nicht jedes beliebige gesetzgeberische Handeln ausreichen, um eine grundrechtliche Schutzpflicht zu erfüllen: Der mit dem entsprechenden Gesetz bezweckte Schutz muss auch *wirksam* sein.[675] Ob man diesen Gedanken nun (von der Schutzrichtung her gedacht) dogmatisch in Form des häufig zitierten Untermaßverbots ausformuliert oder (von der Abwehrrichtung her gedacht) als gänzlich im Rahmen der oben bereits erörterten Verhältnismäßigkeitsprüfung als etwaige Ungeeignetheit und damit fehlende Rechtfertigung des mit einem solchen Gesetz verbundenen Eingriffs in andere Grundrechte verortet aufgehen

669 BVerfG, Beschluss v. 06.11.2019, 1 BvR 16/13, Rn. 88.

670 Vgl. *Reinhardt*, AöR 2017, 528 (548): „Angesichts der Vielzahl an Möglichkeiten, der grundrechtlichen Gewährleistungsverantwortung nachzukommen, müssen dem politischen Gesetzgeber weitreichende Gestaltungsspielräume zukommen."

671 Siehe BVerfGE 77, 170 (214); 79, 174 (202); 96, 56 (64); 121, 317 (356); 125, 39 (78); 133, 59 (76 Rn. 45); 142, 313 (337 Rn. 70). Vgl. auch *Dreier*, in: Dreier, GG Band I, Vorb. Rn. 103; *Stern*, DÖV 2010, 241 (245).

672 Siehe die prägnanten Ausführungen von *Canaris*, AcP 1984, 201 (231 f.) zur Frage der Ausgestaltung des zivilrechtlichen Persönlichkeitsrechtsschutzes am Beispiel von BVerfGE 54, 208.

673 BVerfGE 77, 170 (214 f.); 79, 174 (201 f.).

674 BVerfG, Beschluss v. 17.07.2013, 1 BvR 3167/08, Rn. 21.

675 Vgl. BVerfGE 56, 54 (80 ff.); 77, 170 (215); 79, 174 (202; 85, 191 (212 f.); 92, 26 (46); 121, 317 (360). Das ist demnach nicht der Fall, wenn „die öffentliche Gewalt Schutzvorkehrungen entweder überhaupt nicht getroffen hat oder offensichtlich die getroffenen Regelungen und Maßnahmen gänzlich ungeeignet oder völlig unzulänglich sind, das Schutzziel zu erreichen, oder erheblich dahinter zurückbleiben".

sieht,[676] sei dahingestellt. In jedem Fall bewegt sich die gesetzgeberische Einschätzungsprärogative im breiten[677] Korridor zwischen (richtigerweise über das Untermaßverbot vermitteltem[678]) Mindestschutz[679] und über andere betroffene Grundrechte und das Verhältnismäßigkeitsprinzip vermitteltem Obermaßverbot.[680] In prägnante Worte fasst dies *Reinhardt*:

„Die Charta-Grundrechte beschränken den gesetzgeberischen Entscheidungsspielraum in zweifacher Hinsicht. Als positive Schutz- und Handlungspflichten verlangen sie nach einem Datenschutzkonzept, das die Grenzen des Untermaßverbotes beachtet, also hinreichend effektiv ist. Als negative Pflichten verlangen sie die Berücksichtigung der widerstreitenden Grundrechte derjenigen, die von den Maßnahmen in der Ausübung ihrer Freiheiten beschränkt werden.“[681]

Durch die – insofern sehr frei – durch den EU-Gesetzgeber getroffene Wahl eines *one size fits all*-Konzepts, wie es die DSGVO in Bezug auf private Datenverarbeitungen verfolgt, besteht nun die Besonderheit, dass gleichzeitig eine generelle Strukturierung gefahrentechnisch niedrigschwelliger alltäglicher Datenverarbeitungen *und* ein Schutz vor konkreten Gefahren erreicht werden soll, die sich in bestimmten Szenarien im Zusammenhang mit solchen Verarbeitungen ergeben. Es vermischen sich also innerhalb eines Regelwerks Elemente der Ausgestaltung einer freien, nur durch das Obermaßverbot begrenzten Förderung bestimmter Grundrechte einerseits und der Ausgestaltung eines schutzpflichtenadäquaten Mindestschutzes (wiederum begrenzt durch das Übermaßverbot) dort, wo eine Aktivierung von Schutzpflichten infrage kommt, andererseits. Während also die oben bei B. IV. 1. beschriebene Grenze aufgrund Untauglichkeit bzw. Ungeeignetheit des selbst gewählten Gesamtkonzepts erst erreicht ist, wenn sich (anfängliche) Fehlannahmen und/oder die (häufig aufgrund von gesellschaftlichen oder technischen Entwicklungen nachträglich) fehlende Tragfähigkeit von Grundprämissen auf struktureller Ebene zeigt, kommt die Aktivierung einer grundrechtlichen Schutzpflicht auch (aber nicht nur[682]) gerade in

---

676 So etwa, und damit dem Untermaßverbot letztlich die Daseinsberechtigung absprechend *Hain*, DVBl 1993, 982 (983).

677 Vgl. *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, S. 217.

678 Vgl. *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, S. 216 f., der die Inkongruenz zwischen Übermaßverbot und Untermaßverbot schön aufzeigt.

679 Kritisch zur Operationalisierbarkeit eines solchen Mindestschutzes *Dreier*, in: Dreier, GG Band I, Vorb. Rn. 103.

680 Vgl. *Jarass*, AöR 1985, 363 (384).

681 *Reinhardt*, AöR 2017, 528 (554), der zudem die Einbettung in das komplexe Geflecht gesellschaftlicher Beziehungen und Entwicklungen betont: „Ein kohärentes Regelungskonzept wird dabei nicht nur die verschiedenen Grundrechtspositionen kompatibilisieren, sondern auch der Eigenlogik von Medien und der Sogkraft von Technikentwicklungen Rechnung tragen müssen.“

682 So würde die *supra* bei IV.1.b) beschriebene fehlende gesetzliche Ausgestaltung und Absicherung der (informierten und freiwilligen) Einwilligung auch im Rahmen einer den materiellen Kern von Art. 7 GRCh treffenden Schutzpflicht virulent werden.

isolierten Bereichen in Betracht, solange diese eine hinreichend konkrete Gefährdung für eines der von Art. 8 GRCh akzessorisch flankierten Freiheitsgrundrechte mit sich bringen.[683] Die erste Grenze bezieht sich somit eher auf die Makroebene des Gesamtkonstrukts der datenschutzbezogenen Gesetzgebung, die zweite auf die Mikroebene des grundrechtsadäquaten Umgangs mit konkreten Gefahrenszenarien *innerhalb* des Gesamtkonstrukts. Aus dieser Unterscheidung lässt sich zudem ableiten, dass ein Defizit auf Gesamtkonzeptsebene regelmäßig auch die Aktivierung einer (oder mehrerer) Schutzpflicht(en) bedingen und ein adäquates Umsetzen dieser infrage stellen wird.

Die Schwelle für eine dergestalt hergeleitete Einschränkung der gesetzgeberischen Gestaltungsfreiheit dürfte dabei insgesamt aber immer noch vergleichsweise hoch sein. Zum einen müssten im dem betroffenen Bereich hinreichend konkrete Gefahren für eines oder mehrere der Unionsgrundfreiheiten drohen. Zum anderen müsste der auch hier relevante risikosensible Ansatz der DSGVO insofern „versagen", als die generellen Pflichten und Schutzmaßnahmen nicht ausreichen, um die Selbstschutzmöglichkeiten des Individuums hinreichend zu aktivieren bzw. abzusichern und die sich außerhalb seiner Einflusssphäre abspielenden Verarbeitendenhandlungen und -prozesse hinreichend zu lenken. Auch dürfte es keine bereichsspezifische rechtliche Rahmung außerhalb der DSGVO geben, die, da es schließlich im Kern um (wenn auch datenverarbeitungsspezifische) Schutzpflichten anderer Freiheitsgrundrechte geht, in erkennbar sensiblen Bereichen häufig bereits im Rahmen der dortigen Regularien existiert.[684]

In Betracht kommt eine solch extreme Schieflage ohne anderweitige rechtliche Rahmung aber möglicherweise im Verhältnis zwischen dem Individuum und den großen, global agierenden Plattformen wie Facebook und Google, deren Sammlung, Speicherung und Verwendung von Nutzerdaten in kaum abschätzbarem Ausmaß kombiniert mit einer fast schon zwingenden Angewiesenheit (sei es aus Gründen der Praktikabilität, des sozialen Zwangs oder der quasimonopolistischen Stellung) vieler Nutzer auf die entsprechenden Dienste. Die Frage, ob das Datenschutzrecht hier (noch) in der Lage ist, den Selbstschutz der Nutzer hinreichend zu gewährleisten bzw. die Handlungsmacht der Plattformen durch materielle Verbote, objektiv wirkende Pflichten und Behördenkontrollen hinreichend einzuschränken, oder ob die hier besonders virulente Überforderung des Einzelnen sowie die fehlende Durchsetzung auf dem Papier womög-

---

683 Vgl. *Reinhardt*, AöR 2017, 528 (558): „Allerdings kann die Beobachtung eines systematischen Versagens von Schutzmechanismen weitergehende Eingriffe rechtfertigen."

684 Hier kommen beispielsweise das VVG im Bereich der Offenlegung von sensiblen (Gesundheits-)Daten im Versicherungswesen oder das TKG hinsichtlich des Telekommunikationsdatenschutzrechts in den Sinn.

lich tauglicher Pflichten und Rechte zu einem großflächigen Versagen des potenziell notwendigen Schutzes führt, darf durchaus aufgeworfen werden.[685]

3. Prozedurale Pflichten als Kehrseite der Medaille: Beobachtungspflicht, Wirksamkeitskontrolle und Zweckmäßigkeitserwägungen

Nachdem nun festgestellt wurde, dass weitergehende primäre bzw. materielle verfassungsrechtliche Grenzen der gesetzgeberischen Gestaltungsfreiheit nicht bestehen bzw. im Ergebnis zu denselben Überlegungen und damit demselben Ausmaß an Eingrenzung zurückführen, die bereits eingangs unter der Frage des grundrechtlichen Schutzguts diskutiert wurden,[686] verbleibt eine Betrachtung möglicher prozeduraler Sekundärpflichten, die zumindest als Leitplanke des Handeln des Verordnungsgebers fungieren und dafür sorgen, dass dieser – insbesondere in einem dynamischen Gebiet wie dem Datenschutzrecht – Vorkehrungen dafür trifft, dass relevante Realweltänderungen oder neue Erkenntnisse über die Wirksamkeit des Gesetzgebungsakts auch zeitnah erkannt werden. Solche prozeduralen Leitplanken wären dann als Kehrseite[687] der grundsätzlich die Freiheit und den Prognosespielraum des Verordnungsgebers betonenden Einschätzungsprärogative bei komplexen und unsicheren Materien sowie der eben beschriebenen hohen Hürden für die Aktivierung einer tatsächlichen Nachbesserungspflicht anzusehen.[688] Anders gesagt: Die bei Erlass eines Gesetzesakts vorliegende Freiheit des Verordnungs- und Gesetzgebers, auch bei bestehender Ungewissheit über die Wirkung eines Akts der Gesetzgebung und die eigene Interpretation sowie etwaige Weiterentwicklung der Realwelt (kurz gesagt: über *Normprogramm* und *Normbereich*) bestimmte Entscheidungen treffen zu dürfen, die sich im Nachhinein als falsch herausstellen,[689] würde dann nur soweit reichen, wie er gleichzeitig genügend Vorkehrungen zur Sicherstellung aktiver Evaluationen getroffen hat. Kommt er dieser Pflicht nicht nach, ist der Gesetzesakt bereits von vornherein, und nicht erst dann, wenn die veränderten Bedingungen eine Nachbesserung erfordert hätten, verfassungswidrig.

---

685 Die Grenzen individueller Kontrolle am Beispiel sozialer Netzwerke und unter Rückgriff auf informationsethische und psychologische Theorien aufzeigend *Adams*, J. L. Inf. & Sci. 2014, 158 (167 f.).

686 Siehe *supra* A. I.

687 Oder mit *Bickenbach*, Die Einschätzungsprärogative des Gesetzgebers, S. 364 als „objektiv-rechtliche[s] Pfand des Bürgers".

688 Vgl. *Bickenbach*, RW 2019, 243 (252 f.): „Das Postulat einer Beobachtungspflicht folgt in der Regel einer der Gesetzgebung zugestandenen Einschätzungsprärogative. Sie ist das Instrument des Bundesverfassungsgerichts, um eine vorzeitige bzw. rückschauende Korrektur gesetzgeberischer Prognosen vermeiden zu können."

689 Vgl. *Steinberg*, Der Staat 1987, 161 (164 f.): „Die Diskrepanz zwischen gesetzgeberischer Erwartung und tatsächlicher Entwicklung kann darin in Erscheinung treten, daß der angestrebte Zweck nicht oder nicht vollständig erreicht wird oder daß das Gesetz wider Erwarten oder stärker als erwartet Rechte Dritter oder Interessen der Allgemeinheit beeinträchtigt."

Das BVerfG betont eine Pflicht, ungewissen Auswirkungen eines Gesetzes Rechnung zu tragen, in ständiger Rechtsprechung im Zusammenhang mit dem sog. Prozess gestufter Anforderungen. Dessen erste Stufe ist demnach ein Prüfauftrag, der darauf gerichtet sein soll, „zu überprüfen, ob die ursprüngliche Entscheidung auch unter den veränderten Umständen aufrechtzuerhalten ist“[690]. Dabei hat der Gesetzgeber grundsätzlich alle zugänglichen Erkenntnisquellen auszuschöpfen, um die Auswirkungen so zuverlässig wie möglich abschätzen zu können.[691] Zwar nimmt das BVerfG derartige Beobachtungspflichten erst bei Vorliegen konkreter Anhaltspunkte für tatsächlich veränderte Umstände, und damit letztlich im Verbund mit und nicht als Kehrseite von einer etwaigen Nachbesserungspflicht, an, doch darf der Gesetzgeber sich „der Kenntnisnahme entsprechender Umstände doch nicht bewusst verschließen.“[692] Taugliche und bei sichtbar gewordenen Zweifeln zwingend geforderte Maßnahmen können dann etwa die Form von Evaluationen[693] oder wissenschaftlichen Begleitungen des Gesetzesvollzugs, aber auch von öffentlichen Ausschussanhörungen oder staatlichen oder staatlich geförderten Forschungs- und Entwicklungsprogrammen annehmen.[694]

Doch auch eine generelle und dauerhafte, bereits vor akut aufkommenden Zweifeln an der Beständigkeit der ursprünglichen Prognoseentscheidung aufkommende Beobachtungspflicht wird diskutiert.[695] Begründet wird die Notwendigkeit einer solchen etwa mit der durch zunehmende Datafizierung ausgelösten besseren und leichteren Überprüfbarkeit von Wirksamkeit und Erfolgen von

---

690 BVerfGE 49, 89 (130); 56, 54 (79); 65, 1 (55); 88, 203 (309 f.); 90, 145 (194).

691 *Steinberg*, Der Staat 1987, 161 (166). Vgl. etwa im Volkszählungsurteil BVerfGE 61, 1 (55): „Die Methoden der amtlichen Statistik und Sozialforschung entwickeln sich stetig weiter. Diese Entwicklung darf der Gesetzgeber nicht unberücksichtigt lassen.“ Eine ähnlich klare Formulierung findet sich im Cannabisurteil, BVerfGE 90, 145 (194): „Angesichts der dargestellten offenen kriminalpolitischen und wissenschaftlichen Diskussion […] hat der Gesetzgeber die Auswirkungen des geltenden Rechts unter Einschluß der Erfahrungen des Auslandes zu beobachten und zu überprüfen.“

692 BVerfGE 150, 1 (90).

693 Zur grundlegenden Erläuterung und Einordnung der Natur von Gesetzesevaluationen und ihrem prospektiven Gegenstück, der Gesetzesfolgenabschätzung, siehe *Sicko*, in: Dalibor/Fröhlich/Rodi/Schächterle/Scharrer, Risiko im Recht – Recht im Risiko: 50. Assistententagung Öffentliches Recht, Greifswald 2010, S. 199 (204 ff.). Vgl. auch *Bickenbach*, Die Einschätzungsprärogative des Gesetzgebers, S. 415 ff.

694 Vgl. *Steinberg*, Der Staat 1987, 161 (166) sowie BVerfGE 56, 54 (82 f.) und 150, 1 (90); generell gesprochen geht es um das Sammeln von Erfahrungen und Verbessern der existierenden Wissensbasis, also das Erheben und Auswerten von Daten, vgl. *Albers*, VerwArch 2008, 481 (485). Zu den Anforderungen an die Informationsbeschaffungsbemühungen des Gesetzgebers und die empirischen Instrumente, die ihm zur Verfügung stehen, siehe *Steinbach*, Der Staat 2015, 267.

695 Vgl. *Bickenbach*, RW 2019, 243 (250): „Die Gesetzgebung ist daher verpflichtet, gesellschaftliche Entwicklungen auf ihre rechtliche Relevanz hin zu beobachten.“ Grundlegend zudem *Bickenbach*, Die Einschätzungsprärogative des Gesetzgebers, S. 361 ff.; siehe auch *Hoffmann-Riem*, AöR 2005, 5 (22).

Gesetzen,[696] eingeordnet als Vorstufe einer später ggf. sich realisierenden verfassungsrechtlichen Nachbesserungspflicht.[697] Dieser Ansatz vermag zu überzeugen und ist auf den zweiten Blick auch weniger weit von dem des BVerfG entfernt, als es zunächst den Anschein hat. Nimmt man dessen Relativierung, der Gesetzgeber dürfe auch schon vor sichtbar gewordenen Zweifeln die Augen vor der Kenntnisnahme veränderter Umstände nicht verschließen, beim Wort, liegt die Existenz einer durchgehend existierenden Beobachtungspflicht, die sich bei den ersten Anzeichen von veränderten Bedingungen und Zweifeln an der (andauernden) Richtigkeit der bisherigen Einschätzung verstärkt und zu einer tiefergehenden Nachforschungspflicht konkretisiert, nicht fern. Bei einem solch fließenden Übergang ändert sich dann nicht nur die Intensität der geforderten Beobachtung und Prüfung, sondern auch (freilich ebenso fließend) dessen Prüfobjekt: Auf der ersten Stufe steht die Beobachtung der gesellschaftlichen Entwicklungen oder veränderten Wissensbasis, auf der zweiten die Prüfung der ursprünglichen Einschätzung oder Prognoseentscheidung im Abgleich mit den Feststellungen der ersten Stufe.

Denkbar ist darüber hinaus auch, dass die praktische gesetzgeberische Umsetzung solcher prozeduralen Pflichten ein Evaluationsprogramm aufweist, das über die Feststellung bloßer verfassungsrechtlich relevanter Entwicklungen und Erkenntnisse hinausgeht. Nicht nur Verfassungsverstöße sollen dann vorhergesehen werden, sondern niedrigschwellige Gesetzesdefizite auf Ebene von Wirkung, Ergebnissen und unbeabsichtigten Nebeneffekten – kurz gesagt: Zweckmäßigkeits- und Effektivitätsgesichtspunkte[698] – ermittelt und ggf. behoben werden. Solche Überlegungen sind in Rechtstheorie und -soziologie üblich; Rechtsnormen sollten stets richtig[699], aber auch effektiv sein[700] – ganze Bereiche wie der der Gesetzgebungslehre beschäftigen sich mit der Verbesserung von Gesetzen und ihrer Wirkung.[701] Auch die Erfüllung rechtspolitischer Ziele steht und fällt damit, dass bestehende Gesetze in regelmäßigen Abständen auf die beschriebenen Zweckmäßigkeitserwägungen hin überprüft und bei Bedarf angepasst werden. Dabei wächst die Bedeutung der Erfolgskontrolle analog mit dem Ausmaß, in dem ein Gesetz darauf abzielt, die gesellschaftliche Wirklich-

---

696 Siehe mit zahlreichen weiteren Nachweisen *Karpen*, Gesetzgebungslehre – neu evaluiert, S. 75, der hier von der Programmwirkung als eine der fünf Phasen der Gesetzesentstehung und -anwendung spricht.

697 Vgl. *Choi*, Die Pflicht des Gesetzgebers zur Beseitigung von Gesetzesmängeln, S. 76 f.; ebenso *Bickenbach*, Die Einschätzungsprärogative des Gesetzgebers, S. 363 f.: „[…] ist die Beobachtungspflicht zeitlich und inhaltlich eine Vorpflicht zur Nachbesserungspflicht."

698 Vgl. *Schröder*, in: Rehbinder/Schelsky, Zur Effektivität des Rechts, S. 271 (273).

699 Die Überprüfung der Richtigkeit einer Norm schließt die *supra* dargelegte Kontrolle der Rechtmäßigkeit und insbesondere Verfassungsmäßigkeit mit ein.

700 Vgl. *Karpen*, Gesetzgebungslehre – neu evaluiert, S. 38 ff.

701 Siehe grundlegend *Karpen*, Gesetzgebungslehre – neu evaluiert; *Noll*, Gesetzgebungslehre.

keit zu gestalten.[702] Nicht zuletzt kann das damit verfolgte Ziel der Effektivierung eines Gesetzes und seiner Folgen dazu führen, dass überkomplexe Gesetze simplifiziert oder die geregelte Materie in Teilen dereguliert wird und damit die betroffenen Akteure bei gleichbleibender oder gar verbesserter Wirkung des Gesetzes entlastet.[703] Weitere treibende Faktoren können sein: die Eindämmung der – gerade auf EU-Ebene kritisierten – „Normenflut"[704] und das Ideal größerer Kosteneffizienz.[705] Liegt der Fokus dabei größtenteils auf den Phasen der Gesetzesplanung und des Gesetzgebungsprozesses – häufig unter dem Schlagwort der Gesetzesfolgenabschätzung[706] – so ist auch die nachträgliche Überprüfung eines bereits wirkenden Gesetzes nicht minder wichtig: „Evaluation ist ein Gebot des Rechtsstaats."[707]

Hinsichtlich der DSGVO und seinem Regelungskonzept als Ergebnis einer gesetz- bzw. verordnungsgeberischen Einschätzungs- und Prognoseentscheidung lassen sich diesen theoretischen Vorüberlegungen konkrete Beispiele von Selbstbindungen und prozeduralen Pflichten gegenüberstellen: Zielsetzung der DSGVO ist ausweislich Erwg. 6 die Aufrechterhaltung eines hohen Datenschutzniveaus auch in Zeiten regelmäßiger technologischer Entwicklungen und, damit einhergehend, stetiger Erleichterung des Verkehrs personenbezogener Daten. Ein ähnliches Bekenntnis zur stetigen Evaluierung und Fortentwicklung des Regelungskonzepts der DSGVO lässt sich der ständigen Rechtsprechung des EuGH seit der Entscheidung in der Sache Google Spain[708] entnehmen. So betont der EuGH in nahezu jedem seiner in den letzten Jahren im Bereich des Datenschutzes ergangenen Urteile die Notwendigkeit der dauerhaften Gewährleistung eines „wirksamen und umfassenden Schutzes" des Betroffenen und begründet damit unter anderem seine weite Auslegung des Verantwortlichenbegriffs,[709] welche als Fortentwicklung ihrerseits ein Beispiel der externen (weil außerhalb des Gesetzgebers stattfindenden) Erfolgskontrolle darstellt.[710] Noch expliziter ordnet Art. 97 der Verordnung an, dass im Rahmen

---

[702] In Abkehr zur bloßen Kodifizierung bestehender gesellschaftlicher und sozialer Normen, vgl. *Schröder*, in: Rehbinder/Schelsky, Zur Effektivität des Rechts, S. 271 (273 f.).

[703] Vgl. *Böhret/Konzendorf*, Ko-Evolution von Gesellschaft und funktionalem Staat, S. 183 f.

[704] Siehe *Roman Herzog*, Europa befasst sich mit zu vielen kleinen Dingen, Deutschlandfunk vom 12.05.2014 (https://www.deutschlandfunk.de/roman-herzog-europa-befasst-sich-mit-zu-vielen-kleinen-100.html). Zuletzt abgerufen am 14.01.2022.

[705] Vgl. *Karpen*, Gesetzgebungslehre – neu evaluiert, S. 89.

[706] Siehe etwa *Grimm*, ZRP 2000, 87; *Böhret/Konzendorf*, Handbuch Gesetzesfolgenabschätzung (GFA); ebenso den Überblick in *Smeddinck*, DÖV 2004, S. 103 (104 ff.).

[707] *Karpen*, Gesetzgebungslehre – neu evaluiert, S. 90.

[708] EuGH, Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317.

[709] Siehe EuGH, Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317 Rn. 34; Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 28; Rs. C-25/17 (Jehovan todistajat), ECLI:EU:C:2018:551 Rn. 66.

[710] Vgl. *Schröder*, in: Rehbinder/Schelsky, Zur Effektivität des Rechts, S. 271 (276 f.).

der regelmäßig[711] anzufertigenden Kommissionsberichte eine Bewertung und Überprüfung des Gesetzes vorzunehmen ist. Dabei sind insbesondere die „Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft" (Abs. 5), ist aber auch die „Anwendung und Wirkungsweise" (Abs. 2)[712] einzelner Abschnitte der Verordnung zu evaluieren. Zweck dessen ist es, etwaige Mängel zu identifizieren und Vorschläge für Änderungen und Optimierungen der DSGVO zu erarbeiten.[713] Die Zielsetzung einer möglichst kontinuierlichen Evaluierung mit dem expliziten Bezugspunkt der eigenen Wirkungsweise, insbesondere im Verhältnis zu technischer Entwicklung und gesellschaftlichem Wandel[714], liegt der DSGVO also qua Selbstverpflichtung ihres Gesetzgebers inne. Vor dem Hintergrund der eben angestellten Differenzierung zwischen verfassungsrechtlich verpflichtenden prozeduralen Evaluationsmaßnahmen und darüber hinausgehenden Prüferwägungen hinsichtlich Zweckmäßigkeit und Effektivität lässt sich Art. 97 DSGVO unter beide Kategorien subsumieren: In seiner Breite und Berichtsfrequenz erfüllt er die verfassungsrechtlichen Anforderungen an prozedurale Beobachtungspflichten, weist aber gleichzeitig ein Prüfprogramm und einen Maßstab auf, das bzw. der auch Zweckmäßigkeits- und Effektivitätserwägungen in den Blick nimmt. Unterfüttert wird dieses weite Verständnis der Bewertungen und Überprüfungen des Kommissionsberichts auch durch die in den letzten Jahren vermehrt angestrengten generellen Zielsetzungen der EU in Richtung einer zweckmäßigeren und effektiveren Regulierung, die auch die DSGVO erfassen: Unter dem Schlagwort Better Regulation Agenda verpflichtet die Europäische Kommission sich selbst und die restlichen Institutionen bereits seit einiger Zeit zu konkreten und weitreichenden Anstrengungen zur Verbesserung der Rechtssetzungsqualität.[715] Dazu gehören ein transparenterer, nachvollziehbarerer und stärker auf multipolare Stakeholder-Beteiligung ausgerichteter Rechtsetzungsprozess, das stetige Bewahren der Subsidiaritäts- und Verhältnismäßigkeitsgrundsätze gegenüber den Mitgliedstaaten, aber auch die nachträgliche Evaluation und ggf. Überarbeitung bestehender Rechtsvorschriften vor dem Hintergrund von Kriterien wie Wirksamkeit, Effizienz und Kohärenz sowie dem Ideal des Abbaus von unnötiger Bürokratie und Gesetzesbelastung.[716]

---

[711] Zu Beginn einmalig bis zum 25.05.2020, danach alle vier Jahre, siehe Art. 97 Abs. 1.

[712] Die Norm legt den Fokus hier zwar explizit auf die Kapitel V und VII und die dort enthaltenen Vorschriften über Drittlandübermittlungen sowie Maßnahmen der Kohärenz und Zusammenarbeit, ohne sich aber abschließend auf diese zu beschränken („insbesondere"), siehe *Brink*, in: BeckOK Datenschutzrecht, Art. 97 DSGVO Rn. 3 f.

[713] Vgl. *Pauly*, in: Paal/Pauly, DSGVO/BDSG, Art. 97 DSGVO Rn. 1 f.

[714] Die informationsgesellschaftlichen Entwicklungen umfassen insbesondere auch Nutzungsverhalten und -präferenzen, vgl. *Brink*, in: BeckOK Datenschutzrecht, Art. 97 DSGVO Rn. 20.

[715] Umfassend zu dieser Zielsetzung *Smulders/Paquet*, in: Garben/Govaere, The EU better regulation agenda: a critical assessment, S. 79.

[716] Vgl. https://ec.europa.eu/info/law/law-making-process/evaluating-and-improving-existing-laws/evaluating-laws_de. Zuletzt abgerufen am 14.01.2022.

Einen ersten Eindruck von der praktischen Anwendung dieser Pflichten und Zielsetzungen brachte der kürzlich erschienene erste Prüfbericht der Europäischen Kommission gem. Art. 97 DSGVO.[717] Dort wird der DSGVO im Großen und Ganzen ein positives Zeugnis ausgestellt.[718] In Einklang mit den in Abs. 2 der Norm angelegten Schwerpunkten des Berichts wird Optimierungsbedarf in erster Linie auf Ebene der harmonisierten Anwendung der Verordnung, sowohl hinsichtlich des Handelns von Aufsichtsbehörden als auch der Umsetzung nationaler Gesetzgebung im Rahmen von Öffnungsklauseln, gesehen.[719] Auch bei dem oft kritisierten Thema des überbordenden Aufwands, den insbesondere kleine und mittelständische Unternehmen (KMU) zur Compliance betreiben müssen, sieht der Bericht keine handwerklichen Fehler der Verordnung, stattdessen seien die Aufsichtsbehörden in der Pflicht, hinreichende Unterstützung durch Konsultationen und bereitgestellte Tools und Toolboxes anzubieten.[720] Konsequenterweise konzentriert sich die Kommission daher auch hinsichtlich der eigenen Aufgaben und Verbesserungspotentiale für die Zeit bis zum nächsten Bericht auf die weitere Überwachung des Bestands effektiver und unabhängiger Aufsichtsbehörden, eine Verbesserung der Zusammenarbeit von nationalen Aufsichtsbehörden bei grenzüberschreitenden Fällen, weitergehende Anstrengungen bzgl. einer insgesamt harmonisierten Anwendung der Verordnung, sowie die laufende Anwendung auch auf neuartige Technologien und Entwicklungen wie der kürzlich im Zusammenhang mit Covid-19 aufgekommenen Tracking- und Tracing-Apps.[721] Eine tiefergehende Evaluation der grundlegenden Wirksamkeit und Zweckmäßigkeit einzelner Normen oder

---

[717] *European Commission*, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation.

[718] Vgl. *European Commission*, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, S. 4: „[…] the GDPR has successfully, [sic] met its objectives of strengthening the protection of the individual's right to personal data protection and guaranteeing the free flow of personal data within the EU."

[719] Vgl. *European Commission*, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, S. 5–7.

[720] Vgl. *European Commission*, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, S. 9 f.

[721] Vgl. *European Commission*, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, S. 15 ff.

gar übergreifender Konzepte der DSGVO lässt die Kommission vermissen.[722] Diese und die Tatsache, dass der Fokus stattdessen auf der Optimierung der Implementation und Durchsetzung der jeweiligen Instrumente und Pflichten liegt, ist zum Zeitpunkt von bloß drei Jahren nach Wirksamwerden der Verordnung nicht weiter verwunderlich.[723] Eine etwas angepasste und tiefergehende Analyse, die auch Bedürfnisse und Stellschrauben für legislative Nachbesserungen umfasst, wäre für die Zukunft aber wünschenswert und mit Blick auf die oben nur kursorisch erwähnten Beispiel potenziell defizitärer Instrumente und Ansätze ggf. auch verfassungsrechtlich geboten, sodass die erste Evaluation als „eine vertane Chance zur Verbesserung der Verordnung"[724] angesehen werden kann. An Input und Kritik als Basis für Inspiration mangelt es jedenfalls nicht.[725]

4. Zwischenergebnis

Verfassungsrechtliche Grenzen der legislativen Freiheit kommen somit – auf Basis der durch den Unionsgesetzgeber selbst getroffenen Entscheidungen für ein bestimmtes Regelungskonzept – grundsätzlich sowohl bei Erlass eines Gesetzes als auch in sich stetig aktualisierender Form nach Erlass in Betracht, werden aber nur selten erreicht. In Bezug auf die DSGVO ist, trotz zahlreicher nennenswerter Defizite, daher davon auszugehen, dass diese Schwelle (noch) nicht überschritten ist.

Auch wo diese Grenzen noch nicht erreicht sind, spricht jedoch aus rechtspolitischen Gründen sowie aus Gründen der Rechtseffizienz einiges dafür, offensichtliche, aber noch nicht (unmittelbar bevorstehende) verfassungsrelevante Gesetzesmängel sowie auf Zweckmäßigkeitsebene hinsichtlich der Gesetzeseffektivität untaugliche Prämissen auf Basis von früheren Falschannahmen oder veränderten Realgegebenheiten zu beheben. Auch wenn den Unionsgesetzgeber diesbezüglich nur bedingt bindende Rechtspflichten treffen, lassen selbst gesetzte rechtspolitische Zielsetzungen kaum etwas Anderes zu.

---

[722] Als Ausnahme kann hier einzig das Recht auf Datenportabilität genannt werden, dessen sehr begrenzte Nutzung durch Betroffene angesprochen, das bzgl. seines generellen Potentials aber nicht in Zweifel gestellt wird. Vgl. *European Commission*, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, S. 8.

[723] So auch *Roßnagel*, DuD 2020, 287 (292), nach dessen Eindruck sich dennoch „schon nach kurzer Zeit vielfältige initiale Defizite gezeigt [haben], die zahlreiche Änderungsvorschläge provoziert haben".

[724] *Roßnagel*, MMR 2020, 657 (657).

[725] Eine umfassende Evaluation liefern etwa *Roßnagel/Geminn*, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht – Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e. V. (vzbv). Konkrete Verbesserungsvorschläge bzgl. der Betroffenenrechte unterbreitet *Geminn*, DuD 2020, 307. Ein guter Einblick aus Perspektive der Aufsichtsbehörden findet sich bei *Jaspers/Jacquemain*, DuD 2020, 297.

Das private Datenschutzrecht als Versuch der normativen Strukturierung des Flusses und der Verarbeitung personenbezogener Daten innerhalb der Gesellschaft[726], zuweilen entgegen bestehenden sozialen und technischen Normen[727] (und damit als Paradebeispiel wirklichkeitsgestaltender Gesetzgebung)[728], lebt in besonderem Maße von (und kämpft in mindestens gleichem Maße mit den Schwierigkeiten der Erfüllung des Ideals) seiner Effektivität und Wirksamkeit. Davon zeugt nicht zuletzt die Institutionalisierung einer regelmäßigen Kontrolle in Form von Berichtspflichten in Art. 97 DSGVO. Dem von der DSGVO verfolgten Datenschutzkonzept ist daher mit Blick auf seine Effektivität nicht nur ein, insoweit verfassungsrechtlich bedingtes, Überprüfungsgebot hinsichtlich seiner grundlegenden Wirksamkeit, sondern auch ein darüberhinausgehendes Optimierungsgebot zu entnehmen.

Wie sich das Konzept der datenschutzrechtlichen Verantwortlichkeit innerhalb dieser beschriebenen verfassungsrechtlich gebotenen und qua Selbstverpflichtung gesetzten Grenzen verhält und ob es in Anbetracht der in Kapitel 1 skizzierten Akteurspluralität im digitalen Raum ggf. Gegenstand einer legislativen Nachbesserungspflicht ist bzw. sein sollte, soll deshalb noch eingehend – gewissermaßen in Form einer Evaluation, wie sie verfassungsrechtlich und auch in Art. 97 DSGVO gefordert ist – in Kapitel 3 diskutiert werden. Zweck des folgenden Abschnitts C. ist, als letztes benötigtes Teilstück vor dieser Diskussion, eine Analyse der von der DSGVO formulierten tatbestandlichen Voraussetzungen der Verantwortlichkeit unter Berücksichtigung ihrer jüngsten Auslegung durch den EuGH, und somit der Ebene der *Auswahl* des Verantwortlichen. Nur so ist im nächsten Schritt der Abgleich, ob die tatbestandliche Zuschreibung der Verantwortlichkeit *de lege lata* (weiterhin) solche Akteure mit Verantwortlichkeit belegt, in deren Person die geschilderten Grundprämissen (noch) erfüllt sind, möglich.

C. Die Verantwortlichkeit und ihre Voraussetzungen

Mit dem durch die obigen Erkenntnisse angereicherten Wissen um das Regelungskonzept des privaten Datenschutzrechts und die Bedeutung der Rolle des Verantwortlichen für diese lohnt nun ein Blick darauf, wie der Verordnungsgeber die Tatbestandsvoraussetzungen des Verantwortlichen im Rahmen der DSGVO ausgestaltet hat. Nachdem oben bei der Analyse der einzelnen Schutzinstrumente und Pflichten also primär die *Ausgestaltung* der Verantwortlichkeit

[726] Siehe *supra* bei A. I.

[727] Man denke an die zuweilen fehlende Sensibilität des Einzelnen für die Folgen seines freizügigen Verhaltens in Bezug auf die ihn betreffenden Daten.

[728] Vgl. *Schröder*, in: Rehbinder/Schelsky, Zur Effektivität des Rechts, S. 271 (274).

im Fokus stand,[729] sollen nun die *Auswahl* des Verantwortlichen und die damit verbundenen regulatorischen Folgen beleuchtet werden. Dabei soll ein kurzer zeitlicher Abriss der Entwicklung des Verständnisses der Tatbestandsvoraussetzungen im Laufe der Zeit und insbesondere der ereignisreichen letzten Jahre gewagt werden. Weil der Verantwortliche trotz seiner besonders herausgestellten Bedeutung nicht die einzige relevante Figurenkreation der DSGVO ist, sollen zudem auch die Rollen des Auftragsverarbeiters und des sog. Dritten als eigenständigen Verantwortlichen, jeweils hinsichtlich ihrer regulatorischen Bedeutung im Verhältnis zum Verantwortlichen, in der gebotenen Kürze portraitiert werden (I. und II.). Dies dient zudem der Schärfung der Tatbestandsmerkmale des Verantwortlichen. Abschließend soll diskutiert werden, inwieweit die durch die jüngere EuGH-Rechtsprechung angestoßene Entwicklung der Tatbestandsmerkmale zu einer klareren Konturierung der Voraussetzungen für die Verantwortlichkeitszuschreibung geführt hat (II. 4. c) und III.)

I. Grundlegende Bedeutung

Die grundlegende Bedeutung des Verantwortlichen für das Regelungskonzept DSGVO wurde nun[730] bereits ausführlich erörtert. Seine Rolle ist stets eine relative, die im Verhältnis zu einem oder mehreren konkreten Datenverarbeitungsakt(en) zu verstehen und zuzuschreiben ist. Dem datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt folgend legt sie der Partei, der sie zugeschrieben wird, bestimmte Pflichten auf, die sich ihrerseits losgelöst von der konkreten Verarbeitung auch auf die Organisation und das generelle Verarbeitungsumfeld des Verantwortlichen beziehen können, und schreibt bestimmten Personen Rechte und Ansprüche gegen sie zu.[731] Der Verantwortliche wird für die von ihm durchgeführten Verarbeitungsvorgänge zur zentralen Figur: Er muss bereits im Vorfeld organisatorische Maßnahmen ergreifen, Protokolle anfertigen, Betroffene informieren und im Generellen dafür Sorge tragen, dass die Risiken, die das Datenschutzrecht der Verarbeitung personenbezogener Daten beimisst und deren Verwirklichung es zu verhindern ersucht, korrekt identifiziert, eingeschätzt und minimiert werden[732]. Dafür muss er hinsichtlich der verarbeitungserheblichen Umstände möglichst weitreichendes Wissen und weitreichende Einflussmöglichkeiten haben.[733]

---

729 Siehe *supra* bei B.

730 Siehe Abschnitt B. dieses Kapitels.

731 *Mantz*, ZD 2014, 62 (64); ebenso noch zur inhaltsgleichen Rolle unter der DSRL *Van Alsenoy*, CLSR 2012, 25 (25): „Within the regulatory scheme of the Directive, the controller is the entity that carries primary responsibility for ensuring compliance with the substantive provisions of the Directive."

732 Zur Bestimmung des Schutzgebietes des Datenschutzrechts und den damit verbundenen Schwierigkeiten siehe oben bei A. I., zur Risikominimierung durch den Verantwortlichen bei B. I. 2. b).

733 Siehe *supra* bei B. II. 1.

Seine zentrale Rolle zeigt sich außerdem darin, nach außen hin sichtbare und erkennbare Anlaufstation zu sein für sowohl diejenigen Personen, deren Daten er verarbeitet, als auch für die Aufsichtsbehörden, die sein Tun überwachen und kontrollieren.[734]

Mit dieser Bündelung in einer Person soll somit in mehrfacher Hinsicht eine möglichst effektive Risiko- und Komplexitätsminimierung erreicht werden: Bei oftmals über verschiedene Akteure verteilten Beiträgen zur Verarbeitung soll der ausgewählte Akteur zentral die Verantwortung übernehmen und für datenschutzkonformes Agieren auf allen Ebenen sorgen.[735] Zudem soll er die für Aufsichtsbehörden nicht immer leicht zu durchschauende fachlich-technische Komplexität der eigenen Systeme und genutzten Verarbeitungstechniken durch Anlegen von Dokumentationen und Durchführung von Risikoabschätzungen auflösen und aufbereiten[736] und die dem Datenschutz inhärenten Rechtsdurchsetzungsdefizite und Unbestimmtheiten durch angeleitete und überprüfte Utilisierung der eigenen Innovationskräfte auflösen helfen[737].

Im Folgenden soll nun nachgezeichnet werden, nach welchen Kriterien die DSGVO die Auswahl dieser Akteure vornimmt.

II. Tatbestandsmerkmale

Die Definition des datenschutzrechtlichen Verantwortlichen findet sich in Art. 4 Nr. 7 der DSGVO. Diesem zufolge ist Verantwortlicher diejenige Partei, die „allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Dieser so griffigen wie abstrakten Definition lassen sich mehrere Tatbestandsmerkmale entnehmen, deren Bedeutung nicht ohne weiteres einleuchtend ist und daher einer näheren Untersuchung bedarf. Klar ist dabei, dass der Begriff des Verantwortlichen ein funktionaler ist, der die Verantwortung „entsprechend dem tatsächlichen und damit auf Grundlage einer faktischen anstelle einer formalen Analyse zuweist"[738]. Irrelevant ist daher etwa, ob ein Akteur die Stellung als Verantwortlicher formell von sich weist oder rechtlich gesehen keine Befugnis zur Verarbeitung hat, solange er faktisch den notwendigen Einfluss auf die – im Folgenden zu beleuchtenden – entscheidenden Verarbeitungsfaktoren hat. Mit anderen Worten: Es

---

734 Siehe *supra* bei B. II. 2.

735 Siehe *supra* bei B. I. 2. a) aa).

736 Siehe *supra* bei B. I. 2. a) bb).

737 Siehe *supra* bei B. I. 2. a) cc) und c).

738 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 38; in identischer Weise fortgeführt von *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 11. Ebenso *Europäischer Datenschutzbeauftragter*, Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725, S. 7 f., der auf den faktischen Einfluss abstellt.

kommt allein auf die Fähigkeiten, nicht auf die Berechtigung für ihren Einsatz an.[739] Im Umkehrschluss wird niemand allein dadurch zum Verantwortlichen, dass er sich selbst so bezeichnet oder im Rahmen eines Vertrages zu diesem erklärt wird, solange nicht die Realität die dafür notwendigen Gegebenheiten widerspiegelt.[740]

1. Die Verarbeitung

Erster Anknüpfungspunkt für die Bestimmung eines Verantwortlichen, auslösende Handlung für seine Verantwortlichkeit und gleichzeitig Zuordnungsobjekt für viele seiner Pflichten ist die Verarbeitung.[741] Gem. Art. 4 Nr. 2 DSGVO versteht das Datenschutzrecht darunter „jeden […] Vorgang oder jede […] Vorgangsreihe im Zusammenhang mit personenbezogenen Daten". Anders als das BDSG zu Zeiten der DSRL belässt es die DSGVO bei diesem Oberbegriff und normiert keine eigenständigen Verarbeitungsarten.[742] Nur beispielhaft zählt die Norm die klassischsten Verarbeitungshandlungen wie das Erheben, Speichern, Übermitteln, Abfragen, Verwenden, Verbreiten und Verknüpfen auf, ohne ihnen jeweils eigene Definitionen zukommen zu lassen.[743] Mit der Wahl eines solch abstrakten Oberbegriffs wollte der Verordnungsgeber bewusst einen weiten Anwendungsbereich gewährleisten. Dies zeigt sich auch in der Inklusion von nicht nur Verarbeitungsvorgängen, sondern auch ganzen *Vorgangsreihen*, sowie darin, dass ein *Zusammenhang* mit personenbezogenen Daten genügt. Ebenso gibt es keine zeitliche, qualitative oder quantitative Mindestgrenze, auch bloß kurzzeitige Zwischenspeicherungen oder Datenweitergaben werden erfasst. Letztlich hat dies jedoch eine größere Bedeutung für die Rolle der Verarbeitung als Tatbestandsmerkmal des sachlichen Anwendungsbereichs der Verordnung, vgl. Art. 2 Abs. 1. Im Rahmen der Bestimmung des Verantwortlichen dürfte er stets das unproblematischste Merkmal darstellen.

---

[739] Gleichwohl kann – insbesondere bei staatlichen Stellen – die ausdrückliche oder implizite rechtliche Zuständigkeit für eine Verarbeitung ein starkes Indiz für Verantwortlichkeit sein, vgl. *Europäischer Datenschutzbeauftragter*, Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725, S. 8 f.

[740] Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 11; etwas anderes gilt hingegen bei gesetzlich angeordneter Zuständigkeit. Siehe dazu *infra* bei 4.

[741] Vgl. *Roßnagel*, in: Simitis u. a., DSGVO/BDSG, Art. 4 Nr. 2 DSGVO Rn. 8.

[742] Das BDSG aF unterschied in § 3 etwa zwischen den Verarbeitungsphasen des Erhebens, Verarbeitens und Nutzens von Daten. Siehe m. w. N. *Roßnagel*, in: Simitis u. a., DSGVO/BDSG, Art. 4 Nr. 2 DSGVO Rn. 4.

[743] Vgl. *Roßnagel*, in: Simitis u. a., DSGVO/BDSG, Art. 4 Nr. 2 DSGVO Rn. 14 ff.

2. Die Zwecke der Verarbeitung

Die Kriterien, auf die bei der Bemessung des Einflusses eines Akteurs und nachfolgend bei der Beurteilung, ob dieser Einfluss die notwendige Schwelle zur Auslösung der Verantwortlichkeit überschreitet, abgestellt wird, sind die *Zwecke* und *Mittel* der Verarbeitung.

Der Zweck lässt sich dabei definieren als „erwartbares Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet".[744] Etwas umgangssprachlicher wird häufig auch vom „Warum" der jeweiligen Verarbeitungstätigkeit(en) gesprochen.[745] Dass das Datenschutzrecht die hinreichende Fähigkeit zur Einflussnahme auf dieses Kriterium zur Voraussetzung für die Verantwortlichkeitszuschreibung gewählt hat, leuchtet ein, wenn man sich vergegenwärtigt, dass die Festlegung eines konkreten Verarbeitungszwecks ebenso eine zentrale Pflicht und Voraussetzung für datenschutzkonforme Verarbeitungen ist wie die Begrenzung der Verarbeitungen auf solche, die diesem Zweck entsprechen, vgl. Art. 5 Abs. 1 lit. b DSGVO.

3. Die Mittel der Verarbeitung

Weniger offensichtlich und eingrenzbar erscheint zunächst die Bedeutung des Begriffs der *Mittel* der Verarbeitung. Untechnisch gesprochen wird hierunter regelmäßig das „Wie", also die Art und Weise der jeweiligen Verarbeitungstätigkeit(en) verstanden. Darunter fallen so weitreichende Elemente wie die Auswahl der konkret zu verarbeitenden Daten, die Dauer und das Ausmaß ihrer Verarbeitung sowie die Zugriffsmöglichkeiten, aber auch die Frage, auf welchem technischen Wege, also bspw. mittels welcher Soft- und Hardware die Verarbeitung vorgenommen wird. Abstrakter gesprochen geht es hier also um die technischen und organisatorischen Methoden, die die Art und Weise der Verarbeitung prägen.

4. Die Entscheidung über Zwecke und Mittel

Ist nun die Frage der Kriterien und ihrer Bedeutung geklärt, lässt sich das entscheidende und am schwersten zu bestimmende Merkmal in den Blick nehmen: die *Entscheidung* über die Zwecke und Mittel. Nur wer – allein oder gemeinsam mit anderen[746] – die Entscheidungshoheit über diese Kriterien innehat und auch faktisch in der Lage ist, sie auszuüben, ist Verantwortlicher für die betreffenden Verarbeitungen bzw. Verarbeitungsvorgänge. Die *Art. 29-Daten-*

---

[744] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 16.

[745] Vgl. etwa *Europäischer Datenschutzbeauftragter*, Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725, S. 9.

[746] Vgl. den Wortlaut von Art. 4 Nr. 7 DSGVO.

schutzgruppe versuchte sich bereits im Jahre 2010, und damit noch zu Zeiten der DSRL, an der Anfertigung einer Taxonomie von drei Fallgruppen, bei deren Vorliegen typischerweise von einem die Verantwortlichkeit auslösenden Einfluss auf die Verarbeitung auszugehen sei.[747] Demnach könne die Verantwortung sich aus einer ausdrücklichen[748] oder implizierten gesetzlichen Zuständigkeit[749] des betreffenden Akteurs,[750] aber auch aus einem tatsächlichen Einfluss[751] im konkreten Fall ergeben. Für die im Rahmen dieser Arbeit relevanten Verarbeitungskontexte im privaten Bereich ist primär die letztgenannte Kategorie von Bedeutung. Insbesondere im Bereich privater Datenverarbeitungen ist daher stets auf die faktische Einflusslage abzustellen. Vertragliche Vereinbarungen und Zuweisungen sind dafür, wie oben beschrieben, irrelevant, sofern sie nicht die Realität widerspiegeln.[752] Sie können dennoch ein erstes Indiz in die eine oder andere Richtung darstellen.

Entscheidend ist daher, welches Ausmaß an Entscheidungshoheit und Einfluss der Verordnungsgeber der DSGVO als Mindestmaß ausgemacht hat. Ist diese Frage in klassischen Verarbeitungskontexten mit simplen, dualen Akteurskonstellationen – eine Datenverarbeitung, die einen Betroffenen tangiert und auf die Handlungen und Entscheidungen eines Akteurs zurückgeht – leicht beantwortet und muss daher kaum aufgeworfen werden, wird sie mit zunehmender Anzahl beteiligter Akteure und komplexeren Verteilungen von Einflusssphären und Beteiligungen an einzelnen Verarbeitungsabschnitten umso wichtiger und schwieriger zu beantworten. Mit anderen Worten: Wo eine Verarbeitung personenbezogener Daten faktisch vorliegt und nur eine Person an ihr beteiligt ist (in Form von Zweck- und Mittelbestimmung), kann diese nur Verantwortlicher sein.

---

747 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 12 ff. Diese Taxonomie wurde in der Folge für die DSGVO sowohl von EDSB als auch EDSA übernommen, vgl. *Europäischer Datenschutzbeauftragter*, Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725, S. 7 f. und *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 11 f.

748 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 12 f.

749 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 13 f.

750 Genau genommen liegen hier Fälle vor, in denen meist – entweder gerade qua gesetzlicher Befähigung oder aufgrund eines entsprechenden Machtverhältnisses – auch eine faktische Einflussmöglichkeit besteht, die gesetzliche Zuständigkeit aber der offensichtlichere Anknüpfungspunkt ist. Im privaten Bereich gilt das etwa für Arbeitgeber in Bezug auf Daten ihrer Mitarbeiter.

751 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 14 f.

752 Vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 13.

Die Frage des notwendigen Grads an Einfluss und Entscheidungshoheit ist daher in erster Linie eine Frage der Bestimmung *eines* Verantwortlichen unter *mehreren potenziellen* Verantwortlichen, mithin eine Abgrenzungsfrage. Ihrer Beantwortung kann man sich daher am besten nähern, indem man sie von anderen Rollen innerhalb der DSGVO abgrenzt.

a) Die Abgrenzung zum Auftragsverarbeiter

Zunächst lässt sich eine Abgrenzung zur in Art. 4 Nr. 8 DSGVO definierten Rolle des Auftragsverarbeiters vornehmen. Auftragsverarbeiter ist nach dieser Norm diejenige Person, die personenbezogene Daten *im Auftrag* des Verantwortlichen verarbeitet. Entscheidend ist, mit Blick zurück auf die Definition in Art. 4 Nr. 7 DSGVO, dass die Entscheidung über Zwecke und Mittel der Verarbeitung bei einer anderen Stelle liegt, während der Auftragsverarbeiter nur für diese, gewissermaßen als ihr „Handlanger", Verarbeitungsvorgänge ausführt, die vom Verantwortlichen an sie delegiert wurden.[753] Die Norm trägt damit der praktischen Realität von Verarbeitungsvorgängen in der heutigen Zeit Rechnung – die Auslagerung einzelner bis sämtlicher Verarbeitungsschritte an Dritte, sei es mangels eigener Expertise oder technischer Ausstattung, sei es aus reinem Effizienzdenken, ist heutzutage eher die Regel als die Ausnahme.

Grenzt man den Auftragsverarbeiter also hinsichtlich seiner Bestimmung vom Verantwortlichen ab, so kann auf der anderen Seite die Abgrenzung zum sog. Dritten – in Art. 4 Nr. 10 DSGVO negativ definiert als jede Stelle, die weder Verantwortlicher oder Auftragsverarbeiter noch kraft deren Autorität zur Verarbeitung befugt ist – fruchtbar gemacht werden, um die *Wirkung* zu verdeutlichen, die mit der Rolle einhergeht. Werden personenbezogene Daten von einem Verantwortlichen an einen Dritten übermittelt, stellt dies eine Verarbeitung personenbezogener Daten iSv Art. 4 Nr. 1 DSGVO dar[754] und bedarf daher einer Erlaubnis durch Einwilligung oder gesetzlichen Tatbestand, Art. 6 DSGVO. Ist der Empfänger hingegen ein Auftragsverarbeiter, so wirkt sich diese Rolle für ihn und den übermittelnden Verantwortlichen privilegierend aus: Die Übermittlung wie auch die daran anschließende Verarbeitung, die der Auftragsverarbeiter für den Verantwortlichen vornimmt, werden zu großen Teilen so behandelt, als würde die Verarbeitung beim und durch den Verantwortlichen selbst vorgenommen. Um es mit den Worten der *Art. 29-Datenschutzgruppe* zu sagen: Sowohl Verantwortlicher als auch Auftragsverarbeiter befinden sich innerhalb

753 Vgl. *Van Alsenoy*, CLSR 2012, 25 (29).

754 Während die Übermittlung im die Datenschutzrichtlinie umsetzenden BDSG a. F., der generellen Tradition des deutschen Datenschutzrechts folgend, noch ein eigenständiger und eigens definierter Verarbeitungsschritt war, unterfällt sie nunmehr schlicht dem weiten Verarbeitungsbegriff nach Art. 4 Nr. 1 DSGVO. Die frühere Unterscheidung zwischen Übermittlung und Weitergabe ist damit obsolet. Vgl. *Buchholtz/Stentzel*, in: Gierschmann u. a., DSGVO, Art. 4 Nr. 2 Rn. 3.

des „inneren Kreises der Datenverarbeitung".[755] *In concreto* bedeutet das, dass die vom Auftragsverarbeiter vorgenommenen Verarbeitungsschritte mit unter die gesamte Verarbeitung des Verantwortlichen fallen, ihre Rechtmäßigkeit sich also vollends nach der Gesamtrechtmäßigkeit richtet. Vorteilhaft ist das einerseits für den Verantwortlichen: Er benötigt keine zusätzliche Rechtsgrundlage für die Übermittlung an den Auftragsverarbeiter.[756] Ebenso profitiert der Auftragsverarbeiter selbst: Auch er muss für die Verarbeitungsschritte, die unter seiner Schirmherrschaft ablaufen, keine Rechtsgrundlage suchen und ist vom Großteil der Pflichten, die die DSGVO bereithält, befreit: Unter anderem die dem Betroffenen gegenüber geltenden Pflichten der Art. 12 ff. DSGO richten sich einzig an den Verantwortlichen. Gleichzeitig soll durch die volle Verantwortlichkeit des Verantwortlichen, durch seine Pflicht zur Auswahl von Auftragsverarbeitern mit ausreichend Garantien gem. Art. 28 Abs. 1 DSGVO sowie durch die eigenen Pflichten des Auftragsverarbeiters sichergestellt werden, dass die Auslagerung an den Auftragsverarbeiter nicht zu einem Absenken des Datenschutzniveaus führt.[757]

Doch was bedeutet dies nun für die Konturierung der Tatbestandsmerkmale und die Konkretisierung des nötigen Einflussgrades? Die bis hierhin hinzugekommene Erkenntnis, dass ein Akteur (weiterhin) Verantwortlicher ist, wenn er die tatsächliche Verarbeitung nicht eigenhändig vornimmt, sondern auf seine Weisung hin von einem anderen Akteur ausüben lässt, sofern dieser keinen Einfluss auf die Zweck- und Mittelfestlegung hat, führt hinsichtlich der Frage, *wann* ein solcher Einfluss im Sinne des Datenschutzes vorliegt, zunächst zu einem Zirkelschluss. Fraglich ist somit weiterhin, wie präzise die Weisungen sein müssen und wie viel Handlungsspielraum der zweite Akteur haben darf, damit beide ihre jeweiligen Rollen beibehalten. Nähert man sich den beiden Akteursrollen von der Betrachtung der real existierenden Sachverhalte her kommend an, die durch die Rolle erfasst werden sollen, ergibt sich eine teilweise Schärfung von selbst: Die Auslagerung von Verarbeitungen und Verarbeitungsabschnitten an Dritte – die durch die Regelungen über die Auftragsverarbeitung gerade rechtlich ermöglicht bzw. erleichtert werden soll – geschieht typischerweise deshalb, weil die auslagernde Partei die Ressourcen und bzw. oder Kompetenzen für die Vornahme der Verarbeitung selbst nicht hat und die Auslagerung günstiger ist, als das Defizit intern zu beheben.[758] Praktisch wird dann aber bei einer Auslagerung auch regelmäßig ein gewichtiges Ausmaß an Handlungsfreiheit jedenfalls hinsichtlich der technischen Ausgestaltung gewährt werden – wo ein Unternehmen die Speicherung seiner Kundendaten an ein an-

---

[755] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 8.

[756] Vgl. *Petri*, in: Simitis u. a., DSGVO/BDSG, Art. 28 DSGVO Rn. 29 ff.

[757] Vgl. *Van Alsenoy*, CLSR 2012, 25 (33); *Petri*, ZD 2015, 305 (306).

[758] Vgl. *Van Alsenoy*, CLSR 2012, 25 (32).

deres Unternehmen auslagert, um nicht eigene Server sowie das nötige Personal zur Einrichtung und Wartung anzuschaffen, wird es dem Auslagerungs-Unternehmen kaum konkrete Weisungen hinsichtlich der genauen technischen Abläufe oder der Auswahl dieser oder jener Komponenten machen, weil es ihm dafür meist schon an dem nötigen Fachwissen mangelt, die Auslagerung aber auch gerade den Zweck erfüllt, sich mit solchen Fragen nicht befassen zu müssen.[759] Stattdessen wird ein auslagerndes Unternehmen regelmäßig nur die groben, wichtigsten Parameter[760] (welche Daten? Wer hat Zugriff auf diese?) und in erster Linie den Zweck der vorzunehmenden Verarbeitungen festlegen und mitteilen.

Daraus ergibt sich, dass jedenfalls hinsichtlich der Mittelfestlegung eine weitreichende Delegierung an den Auftragsverarbeiter möglich sein muss, will man nicht dessen Rolle innerhalb des Datenschutzrechts *ad absurdum* führen. So urteilt dann auch die *Art. 29-Datenschutzgruppe*, dass die Entscheidung über die Zwecke der Verarbeitung die grundlegendere Bedeutung für die Zuordnung der Verantwortlichkeit hat, während die Entscheidung über die Mittel weitgehend oder gar völlig einem anderen Akteur überlassen werden kann, ohne die Rolle des Verantwortlichen zu verlieren, sofern „gewisse Garantien" bestehen.[761]

Generalisiert man diese zunächst für die Abgrenzung zwischen Verantwortlichem und Auftragsverarbeiter geltende Erkenntnis, lässt sich daher sagen: Hat ein Akteur die Entscheidung über die Zwecke der Verarbeitung gänzlich in der Hand, so ist er allein durch diesen Einfluss Verantwortlicher, während die isolierte Entscheidungshoheit über die Mittel der Verarbeitung nur dann ausreicht, wenn sie die *wesentlichen* Aspekte der Mittel umfasst.[762] Wann genau die selbst entschiedenen Mittelaspekte hinreichend wesentlich sind, ist damit

---

[759] Vgl. *Van Alsenoy*, CLSR 2012, 25 (37): „[…] the determination of the ‚means' of the processing is the service offered by a processor."

[760] Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17: „[…] wesentliche Elemente, die traditionell und naturgemäß der Entscheidung durch den für die Verarbeitung Verantwortlichen vorbehalten sind […]."

[761] Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17 f.; ebenso auch der EDSA als Nachfolger der Gruppe, vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 16. Bei gänzlicher Abwesenheit von Weisungen muss bspw. gewahrt sein, dass der Verantwortliche vom Auftragsverarbeiter über die verwendeten Mittel informiert wird und diese auch zur Erreichung des festgelegten Zwecks beitragen.

[762] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 14.; vgl. auch *Europäischer Datenschutzbeauftragter*, Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725, S. 15, 18.

freilich noch nicht beantwortet – eine gewisse Restunklarheit bleibt also auch hier bestehen.[763]

b) Die Abgrenzung zu weiteren Verantwortlichen: gemeinsam, allein oder gar nicht?

Eine weitere, ungleich schwierigere Abgrenzung lässt sich für diejenigen Fälle vornehmen, in denen mehrere Akteure an einer Verarbeitung oder mehreren zusammenhängenden Verarbeitungstätigkeiten beteiligt sind, die jeweils für sich Beiträge zur Mittel- und Zweckfestlegung leisten und so gemeinsam dazu beitragen, was letztlich auf welche Art und Weise mit welchen Daten passiert. Zeichnet sich die Auftragsverarbeitung noch dadurch aus, dass der in dieser Rolle befindliche Akteur keinerlei eigene Interessen verfolgt und somit keinen Beitrag zur Zweckfestlegung leistet, sondern als (zugegebenermaßen kompetentes) „Werkzeug" die Weisungen des Verantwortlichen ausführt, gestaltet sich in anderen Szenarien eine Gemengelage an unterschiedlichen Interessen, Einflusssphären und Beiträgen. Die folgende Komplexität erschöpft sich dann nicht nur in der Vielzahl beteiligter Akteure, sondern erstreckt sich auch auf die zeitliche Dimension, da sich die verschiedenen Beitragshandlungen auf verschiedene Verarbeitungsabschnitte verteilen, dabei aber dennoch einem gemeinsamen übergeordneten Lebenssachverhalt angehören.

Davon betroffen sind in zunehmendem Maße Szenarien, die klassischerweise eher der Auftragsverarbeitung zuzuordnen waren. In der heutigen digitalen Servicelandschaft, in der es nahezu keine Dienste mehr gibt, deren Geschäftsmodell neben der eigentlichen Primärdienstleistung nicht auch in der Analyse und Monetarisierung der beim „Tagesgeschäft" anfallenden Daten besteht,[764] geht diese Einordnung regelmäßig ins Leere.

Die DSGVO ist, ebenso wie vor ihr auch die DSRL,[765] für ein solches Zusammentreffen mehrerer aktiv beteiligter Akteure grundsätzlich gewappnet. Bereits die Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO enthält die Möglichkeit eines Akteurs, der über die Zwecke und Mittel der Verarbeitung allein oder „mit anderen" entscheidet. Hinter diesem unscheinbaren Zusatz versteckt sich die Möglichkeit einer *gemeinsamen* Verantwortlichkeit, bei der zwei oder mehrere Akteure gemeinsam die Verantwortung für die Rechtmäßigkeit

[763] Vgl. *Van Alsenoy*, CLSR 2012, 25 (36): „While these criteria appear to be conceptually sound, it often remains debatable whether an entity is either acting as a controller or as a processor towards a particular processing operation." Auch der EDSA erkennt diese Unschärfe an, vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 27: „A case-by-case analysis remains necessary, however, in order to ascertain the degree of influence each entity effectively has […]."

[764] Siehe hierzu die beispielhaften Fallbeispiele in Kapitel 1 A.

[765] Vgl. Art. 2 lit. d DSRL, der mit identischem Wortlaut bereits die Figur des gemeinsamen Verantwortlichen vorsah.

einer Verarbeitung tragen. Während diese Möglichkeit regulatorisch grundsätzlich auch in der DSRL schon vorgesehen war,[766] wurden die aus einer solchen gemeinschaftlichen Verantwortlichkeit resultierenden Rechtsfolgen an keiner Stelle der Richtlinie erwähnt oder konkretisiert. Die DSGVO enthält in ihrem Art. 26 hingegen einige Pflichten und Konkretisierungen zur Haftung der betroffenen Akteure. An einer genaueren Bestimmung der Kriterien und insbesondere der jeweils sowie gemeinsam nötigen Beitragshöhe mangelt es aber weiterhin.

Nichtsdestotrotz gibt bzw. gab es – ebenfalls bereits zu Zeiten der DSRL – erste Versuche einer Konkretisierung und Systematisierung von Fällen gemeinsamer Verantwortlichkeit. So ist etwa das *gemeinsame Festlegen* von Mitteln und Zwecken nach Ansicht der *Art. 29-Datenschutzgruppe* dynamisch festzustellen, sodass der bestimmende Einfluss nicht bei beiden (bzw. allen) Parteien für die gesamte Bandbreite an Verarbeitungsschritten in gleichem Ausmaß vorhanden sein muss; möglich sind stattdessen vielschichtige Arten arbeitsteiliger Einflussnahme, die sich auch nur auf einzelne Abschnitte der Verarbeitung beziehen können: „Unter diesem Aspekt muss der Begriff ‚gemeinsam' im Sinne von ‚zusammen mit' oder ‚nicht alleine' in unterschiedlichen Spielarten und Konstellationen ausgelegt werden."[767]

Sodann genügt es, in Fortführung der oben beschriebenen Feststellung, dass das gemeinsame Festlegen sich nicht zwingend kumulativ, sondern bereits *alternativ* auf *entweder* die Zwecke *oder* aber die (wesentlichen!) Mittel der Verarbeitung bezieht.[768] Dies stellt letztlich die konsequente Fortführung der obigen Feststellung zur Bedeutung von Zweck und Mitteln im Rahmen der Abgrenzung zum Auftragsverarbeiter dar.

Nicht jeder der beschriebenen Fälle arbeitsteiliger Zusammenarbeit verschiedener Akteure an der Verarbeitung personenbezogener Daten stellt somit zwingend einen Fall *gemeinsamer* Verantwortlichkeit dar. Gerade dort, wo schlicht Daten übermittelt und nachgelagert voneinander verarbeitet werden, stellt sich der Fall regelmäßig eher als einer von isolierten Verantwortlichkeiten der beteiligten Akteure dar, sofern keine hinreichende Kongruenz zwischen den jeweiligen Zwecken und bzw. oder Mitteln besteht.[769] Ebenso kommen Kon-

---

[766] Sie befand sich in der nahezu wortgleichen Definition des Verantwortlichen in Art. 2 lit. d.

[767] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 22; weiterhin identisch in *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 19.

[768] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 23; ebenso *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 19.

[769] Vgl. das Beispiel bei *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 24, wonach ein

stellationen infrage, in denen Akteure zwar beteiligt sind und Beiträge leisten, dabei aber die nötige Beitragshöhe nicht erreichen und somit keine datenschutzrechtliche Rolle einnehmen.

Auch in diesen Fällen kommt es daher für eine Abgrenzung darauf an, eine Konturierung der Zweck- und Mittelbegriffe sowie der jeweils notwendigen Beitragshöhe zu erreichen. Eine solche, über konkrete Einzelfälle hinausgehende, abstrahierende Konkretisierung gelingt der *Art. 29-Datenschutzgruppe* nicht. Stattdessen konzediert sie, dass eine feste und abschließende Definierung von Konstellationen ob der zahlreichen denkbaren Formen und Ausgestaltungen von Zusammenarbeit und Entscheidungsbeteiligungen nicht möglich, es also vielmehr nötig ist, sich der Lösung über eine Vielzahl von Typologien gemeinsamer Kontrolle anzunähern, wobei „eine gewisse Flexibilität erforderlich ist, um der zunehmenden Komplexität der heutigen Gegebenheiten im Bereich der Datenverarbeitung Rechnung zu tragen."[770] Sodann führt sie eine Reihe von Fallbeispielen als exemplarische Fälle, in denen mehrere Akteure die notwendige Schwelle – entweder als jeweils isolierte oder als gemeinsame Verantwortliche – überschritten haben. So sei etwa ein Personalvermittler gemeinsam mit dem Unternehmen, für das er geeignete Bewerber aus seinem eigenen Pool an Arbeitssuchenden sowie aus den sich unmittelbar beim Unternehmen Bewerbenden auswählen soll, verantwortlich für die Verarbeitungen im Zusammenhang mit der Vermittlung.[771] Ebenso verhalte es sich, wenn verschiedene Unternehmen durch Errichtung einer gemeinsamen Verarbeitungsinfrastruktur die wesentlichen Verarbeitungsmittel gemeinsam festlegen, selbst wenn sie dann – wie ein Reisebüro, eine Fluggesellschaft und ein Hotel – dieselben Daten zu jeweils eigenen Zwecken verarbeiten.[772] Demgegenüber steht die bloß isolierte Verantwortlichkeit einzelner Akteure für die von ihnen in eine gemeinsame Datenbank eingebrachten Daten (sog. „herkunftsbasierter Ansatz"), sofern auch nur sie jeweils die Kontrolle über die Nutzung der betroffenen Daten haben.[773] Gerade am letzten Beispiel zeigt sich die Konsequenz des funktionalen Ansatzes der Zuschreibung datenschutzrechtlicher Verantwortlichkeit, und damit auch die Wechselwirkung zwischen Verantwortlichkeitszuschreibung und den daraus folgenden Pflichten: Die notwendige Kontrolle über Mittel und Zwecke der Verarbeitung zeigt sich nicht zuletzt darin, dass ein Akteur faktisch in der

---

Reisebüro ebenso eigenständiger Verantwortlicher für die Verarbeitung von Kundendaten ist wie die Fluggesellschaften und Hotels, an die es die Daten weitergibt.

[770] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 24.

[771] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 23.

[772] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 24.

[773] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 26.

Lage ist, konkrete Pflichten zu erfüllen und Betroffenenrechten nachzukommen. Dennoch ist auch dies nur ein Indikator, der im Einzelfall widerlegt sein kann, darf also die (teilweise) Unfähigkeit der Pflichtenerfüllung nicht zwingend als Ausschlusskriterium der Verantwortlichkeit missverstanden werden.[774] Ein Akteur, der eigenhändig die betreffenden Daten nicht löschen oder an den Betroffenen herausgeben kann, kann dies etwa möglicherweise kraft Vertrages von seinem Auftragsverarbeiter verlangen; ein Akteur, der aufgrund organisatorischer Defizite keinen Überblick hat und deshalb keine vollständige Auskunft über die von ihm verarbeiteten Daten erteilen kann, hat sich dieses Manko selbst zuzuschreiben und verletzt die entsprechenden Pflichten, verliert aber nicht seinen grundsätzlich vorhandenen Einfluss und mithin auch nicht seine Stellung als Verantwortlicher.

Wie bereits beschrieben kommen auch Fälle in Betracht, in denen zwar mehrere Akteure gemeinsam die Mittel und Zwecke der Verarbeitung bestimmen und daher grundsätzlich gemeinsame Verantwortliche sind, dabei aber nicht in identischem Maße zur Bestimmung beitragen, sodass ihre Beiträge also ungleich verteilt sind. Die Beiträge können sich dabei qualitativ unterscheiden, sie können aber auch auf temporaler Ebene nur teilweise Überschneidungen aufweisen und schlicht nacheinander geschehen. Hier spannt sich eine zusätzliche Komplexitätsebene hinsichtlich des Zusammenspiels zwischen Verantwortlichkeitszuschreibung und (Erfüllbarkeit von) Verantwortlichenpflichten auf: Je nach Verteilung der Kontrolle im Einzelfall stellt sich die Frage, wie weit die gemeinsame Verantwortlichkeit reicht und für welche Verarbeitungsabschnitte die davon erfassten Akteure jeweils verantwortlich sind. Letzteres betrifft streng genommen nicht die Pflichtigkeit an sich, stellt doch Art. 26 Abs. 3 DSGVO jedenfalls für die Betroffenenpflichten explizit klar, dass diese bei und gegenüber jedem Verantwortlichen geltend gemacht werden können.[775] Stattdessen ist hier die nachgelagerte Ebene der Haftbarkeit betroffen, also die Frage, welcher Verantwortliche im Falle einer festgestellten Pflichtverletzung im Außenverhältnis gegenüber dem Betroffenen haftet[776] oder von der zuständigen Behörde sanktioniert oder anderweitig mit Maßnahmen belegt werden kann. Diese Thematik soll hier zunächst außenvorbleiben und im nächsten Kapitel erörtert werden. Von Bedeutung kann die trennscharfe Eingrenzung der jeweiligen (gemeinsamen) Verantwortlichkeit aber auch dort sein, wo sich einzelne Verarbeitungsabschnitte definieren lassen, sodass es denkbar erscheint, dass für nachgelagerte bzw. vorgelagerte Verarbeitungen nur (noch) ein einzelner Akteur isolierter Ver-

---

774 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 27.

775 Vgl. auch *Hornung*, in: Simitis u. a., DSGVO/BDSG, Art. 26 DSGVO Rn. 28.; *Specht-Riemenschneider/Schneider*, MMR 2019, 503 (508).

776 Hier ordnet Art. 82 Abs. 4 DSGVO grundsätzlich eine gesamtschuldnerische Haftung mit Regressmöglichkeit gem. Abs. 5 der Norm an.

antwortlicher ist, wenn die bisher gemeinsamen Verantwortlichen keine Beiträge (mehr) leisten.

Waren diese Ausführungen der *Art. 29-Datenschutzgruppe* zwar umfangreich und durchdacht, stellten sie aufgrund lange mangelnder praktischer Relevanz des Rechtsinstituts der gemeinsamen Verantwortlichkeit dennoch primär eine theoretische Vorüberlegung ohne praxisrelevante gerichtliche bzw. behördliche Konturierung dar.[777] Änderung brachte jüngst eine Reihe von EuGH-Entscheidungen, die das bis dato rein theoretische Thema in die Praxis brachte und zugleich zahlreiche (teils hitzige) Diskussion in der Literatur auslöste.[778]

aa) Der Fall Wirtschaftsakademie SH

Den ersten Auslöser stellt dabei das Urteil in der Sache Wirtschaftsakademie Schleswig-Holstein dar. Der diesem zugrundeliegende Ursprungsfall betraf die Wirtschaftsakademie Schleswig-Holstein, ein privates Bildungsunternehmen, das Bildungsdienstleistungen anbietet und zur Bewerbung dieser eine sog. Fanpage auf Facebook anbot. Auf solchen können Privatpersonen oder Unternehmen bei Facebook ihr Angebot bewerben oder ihr thematisches Anliegen behandeln und Beiträge und Kommentare werbender oder inhaltlicher Art absetzen. Unabdingbarer Teil des zwischen den Betreibern einer solchen Fanpage und Facebook bestehenden Nutzungsverhältnisses ist Facebook Insights, ein Analysetool, mit dem Facebook den Betreibern aggregierte anonyme Statistiken über die Besucher der Fanpage aufbereitet. Diese Statistiken speisen sich aus den personenbezogenen Daten der einzelnen Besucher, die mittels sog. Cookies erhoben werden, die ihrerseits auf den Endgeräten der Besucher gespeichert werden.[779] Erfasst werden dabei sowohl Besucher mit eigenem Facebook-Konto als auch externe Besucher ohne Konto, die etwa über einen Suchmaschinen-Eintrag oder eine Verlinkung auf der Website des Fanpage-Betreibers zur Fanpage gelangen können. Zudem besteht für Betreiber die Möglichkeit, aktiv die für sie relevanten Parameter der von Facebook zu erstellenden Statistik zu setzen und so die der Statistik zugrundeliegenden Daten und damit die betroffenen Besucher zu spezifizieren. Ist ein Betreiber etwa nur daran interessiert, wie viele

---

[777] *Golland*, ZD 2019, 381 (381) spricht von einem „de facto unbeachteten Relikt der Datenschutzrichtlinie."

[778] Zur Bedeutung der Urteile und für eine generelle konzeptionelle Aufteilung von EuGH-Urteilen in Definitionsurteile und Abwägungsurteile siehe *Lindroos-Hovinheimo*, Information & Communications Technology Law 2019, 225. Für die Aktualisierung der Stellungnahme der *Art. 29-Datenschutzgruppe* durch ihren Nachfolger, den EDSA, siehe *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[779] Eine gute Erklärung der technischen Abläufe und Datenflüsse im konkreten Fall findet sich bei *AK I „Staatsrecht und Verwaltung" der IMK*, Ergebnisbericht der Arbeitsgruppe des AK I „Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken, S. 7 ff. Ebenfalls, auf diesen Bericht bezugnehmend, in verkürzter Form in der erstinstanzlichen Entscheidung des VG Schleswig, ZD 2014, 51 (52).

männliche Besucher im Alter zwischen 25–35 Jahren seine Fanpage in einem bestimmten Zeitraum besucht haben oder wie die Geschlechter- oder Altersverteilung seiner Besucher generell aussieht, so fließen auch nur diese Parameter in die für ihn angefertigte und ihm übermittelte Statistik ein.

Im November 2011 verpflichtete die für die Wirtschaftsakademie zuständige Aufsichtsbehörde – das ULD Schleswig-Holstein – im Wege einer Anordnung[780] das Unternehmen, den Betrieb der Fanpage einzustellen: Die Verarbeitung der Besucherdaten durch Facebook verstoße mangels Information der betroffenen Nutzer, eingeräumter Widerspruchsmöglichkeit sowie Einholung einer wirksamen Einwilligung gegen geltendes Datenschutzrecht[781] und die Wirtschaftsakademie sei jedenfalls gemeinsam mit Facebook für die entsprechenden Verarbeitungen verantwortlich.[782] Das in der ersten Instanz im Rahmen einer Anfechtungsklage der Wirtschaftsakademie mit dem Fall befasste VG Schleswig war diesbezüglich anderer Meinung und verneinte eine (gemeinsame) Verantwortlichkeit des Unternehmens neben Facebook. Dabei stützte das VG sich in erster Linie auf die Tatsache, dass die Wirtschaftsakademie in keiner Weise eigenhändig an der Übertragung der Daten von den Fanpage-Besuchern an Facebook sowie an der späteren Verarbeitung durch Facebook beteiligt war. Indem es zunächst den „fehlende[n] Kontakt“ des Betreibers und seines „operativen Instrumentarium[s]“ zu den personenbezogenen Daten des Nutzers betonte und darauf verwies, ohne diesen Kontakt könne eine Verantwortlichkeit nur bei Einsatz eines Auftragsverarbeiters bestehen,[783] offenbarte das VG bei seiner Einschätzung eine sehr strenge Orientierung am Wortlaut des BDSG aF. Dieses definierte den Verantwortlichen in § 3 Abs. 7 als die Person, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch einen anderen im Auftrag vornehmen lässt. Demgegenüber entsprach der Wortlaut von Art. 2 lit. d DSRL – in dessen Lichte der Verantwortlichenbegriff des BDSG aF auszulegen war – dem heutigen Wortlaut von Art. 4 Nr. 7 DSGVO und bezog sich allein auf das Merkmal der Entscheidung über Mittel und Zwecke der Verarbeitung. Auf dieses ging das VG ausführlich im Rahmen der Prüfung der (vom ULD vertretenen) gemeinsamen Verantwortlichkeit des Fanpage-Betreibers mit Facebook ein und sah den nötigen tatsächlichen und/oder rechtlichen Einfluss auf die Entscheidung – und damit die Herrschaft über die Daten[784] – letztlich nur bei Facebook und nicht bei der Wirtschaftsakademie. Es stützte diese Einschätzung in erster Linie auf die Tatsache, dass

[780] Gem. § 38 Abs. 5 BDSG aF.

[781] In Form der zu diesem Zeitpunkt geltenden § 13 Abs. 1 und 3 TMG als Umsetzung der DSRL.

[782] Vgl. auch hier die zusammenfassende Beschreibung des VG Schleswig, Urt. v. 09.10. 2013, Az. 8 A 14/12, in: ZD 2014, 51 (52).

[783] VG Schleswig, ZD 2014, 51 (53).

[784] *Martini/Fritzsche*, NVwZ-Extra 2015, 1 (3).

die Wirtschaftsakademie als Betreiber der Fanpage einzig im Rahmen der Entscheidung für oder gegen die Eröffnung und inhaltliche Bespielung der Fanpage eine eigene Entscheidungsmacht ausübe, während Zwecke *und* Mittel aller weiteren Entscheidungen vollständig von Facebook entschieden würden und in ihren Einzelheiten auch nicht verhandelbar seien.[785] Eine solch beschränkte Möglichkeit zur Einflussnahme sah das VG daher insgesamt als nicht ausreichend an und kam nach einem kurzen Verweis auf den (vermeintlich) abschließenden Regelungscharakter der datenschutzrechtlichen Verantwortlichkeit und die daher ausgeschlossene Möglichkeit des Rückgriffs auf deliktsrechtliche und allgemeine polizei- und ordnungsrechtliche Haftungstatbestände oder das Institut der Störerhaftung[786] zum Ergebnis der Rechtswidrigkeit der gegen die Wirtschaftsakademie gerichteten Untersagung.

Das nach Berufung des ULD in der nächsten Instanz mit dem Fall beschäftigte OVG Schleswig schloss sich diesem Ergebnis durchgängig an und wies die Berufung ab. Auch hier betonte das Gericht, dass eine Verantwortlichkeit der Wirtschaftsakademie mangels hinreichenden Einflusses auf die Verarbeitung nach keiner der möglichen Konstellationen infrage käme und insbesondere Facebook mangels schriftlichem Vertrag wie auch faktischer Einflusslage der Wirtschaftsakademie nicht als Auftragsverarbeiter in deren Auftrag agiere.[787] Darüber hinaus wiederholte es die Feststellung des VG Schleswig, wonach weder ein Rückgriff auf andere Verantwortlichkeiten außerhalb der DSRL erlaubt sei noch die vom ULD ergriffene Maßnahme aus § 38 Abs. 5 BDSG aF ihrerseits an einen Akteur gerichtet werden könne, der nicht selbst Verantwortlicher ist.[788] Die Gefahr einer offen bleibenden Schutzlücke durch das Fehlen einer (genuin datenschutzrechtlichen oder anderweitigen) Verantwortlichkeit der Wirtschaftsakademie schloss das OVG mit Verweis auf die weiterhin bestehende Verantwortlichkeit Facebooks aus: Wo es zu jeder Verarbeitung auch eine verantwortliche Stelle gebe, seien „unverantwortliche Aktivitäten“ ausgeschlossen.[789]

Nach von Seiten des ULD eingelegter Revision gegen das OVG-Urteil nahm sich das BVerwG dem Fall an, sah sich aber – trotz grundsätzlicher Übereinstimmung mit den Entscheidungen der Instanzgerichte[790] – ohne vorherige europa-

---

[785] VG Schleswig, ZD 2014, 51 (54).

[786] VG Schleswig, ZD 2014, 51 (54).

[787] OVG Schleswig, Urt. v. 04.09.2014, Az. 4 LB 20/13, in: ZD 2014, 643 (644).

[788] OVG Schleswig, ZD 2014, 643 (645); eine weitere Feststellung des Gerichts, die hier von geringerer Bedeutung bleiben kann, liegt in der abgestuften Natur des § 38 Abs. 5 BDSG aF. Demnach sei die Maßnahme des ULD auch deshalb rechtswidrig, weil gem. S. 2 der Norm ein Verbot der Verarbeitung insgesamt erst nach erfolglosem Versuch der Beseitigung durch andere Mittel ausgesprochen werden dürfe.

[789] OVG Schleswig, ZD 2014, 643 (645).

[790] Siehe die Ausführungen zum vorlegenden Gericht von Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 27.

rechtliche Begriffsklärung nicht in der Lage, den Fall eindeutig zu beantworten. Er legte deshalb insbesondere[791] die Frage, ob in einer solchen Konstellation trotz – nach Ansicht des BVerwG – nicht vorliegender Verantwortlichkeit iSd Art. 2 lit. d DSRL Raum für andere Verantwortlichkeiten, etwa hinsichtlich einer Auswahlverantwortlichkeit analog zu der im Rahmen einer Auftragsverarbeitung, verbleibe, dem EuGH zur Vorabentscheidung vor.[792] Dass dieser anderer Ansicht als die mit dem Fall befassten deutschen Gerichte sein und (jedenfalls im Ergebnis) der Ansicht des ULD folgen könnte, wurde zum ersten Mal mit Veröffentlichung der Schlussanträge des Generalanwalts *Bot* offenbar.[793] Dieser wies bereits die hinter den zentralen Fragen des BVerwG stehende Prämisse einer fehlenden datenschutzrechtlichen Verantwortlichkeit iSd Art. 2 lit. d DSRL zurück und konstatierte, dass seines Erachtens eine solche durchaus bestehe. So sei aufgrund der zentralen Bedeutung, die der Bestimmung des Verantwortlichen für das System der DSRL zukommt, sowie im Interesse des wirksamen und umfassenden Schutzes von Betroffenen und in Fortführung der mit der Google Spain-Entscheidung[794] des Gerichtshofs etablierten Linie der Begriff grundsätzlich weit auszulegen.[795] Unter Berücksichtigung dieser Tatsachen, so *Bot*, genüge das kausale Ingangsetzen und damit initiale Ermöglichen der Verarbeitung infolge der Entscheidung eines Unternehmens oder eines anderen Akteurs, eine Fanpage in Betrieb zu nehmen, in Kombination mit den Einflussmöglichkeiten hinsichtlich der konkreten Verarbeitungskriterien, für das gefordert Maß an Einfluss auf die Verarbeitungsmodalität aus.[796] Zusätzlich sah *Bot* eine enge Verknüpfung zwischen den von Facebook und der Wirtschaftsakademie (oder anderen Fanpage-Betreibern) jeweils mit der Analyse der Besucherdaten verfolgten Zwecken: Der Letztgenannten dienten die daraus entwickelten Statistiken der Steuerung und besseren Anpassung der Vermarktung ihrer Tätigkeiten durch Postings auf der Fanpage, während die Verarbeitung derselben Daten Facebook ebenfalls zur gezielteren Verbreitung ihrer Werbung diene.[797] Insgesamt stünden in Anbetracht der insoweit entscheidenden

---

[791] Die anderen an den EuGH gestellten Fragen – die hier nicht weiter behandelt werden sollen – bezogen sich auf die Bestimmung der zuständigen Behörde und damit auch die Anwendbarkeit des jeweiligen nationalen Rechts.

[792] BVerwG, Beschl. vom 25.02.2016, Az. 1 C 28.14. Siehe hier insbesondere die Rn. 27 f. bzgl. der Einschätzung des BVerwG gegen eine (Mit-)Verantwortlichkeit der Wirtschaftsakademie.

[793] Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796.

[794] EuGH Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317.

[795] Vgl. Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 44 f.

[796] Vgl. Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 56 f.

[797] Vgl. Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 59.

Kriterien (die durch freie Entscheidung des Betreibers herbeigeführte kausale Ermöglichung und die hinreichend ähnlichen Zwecke) daher die fehlende Einflussnahme auf die Vertragsgestaltung und der fehlende Zugang zu den zu verarbeitenden Daten einer Einordnung als gemeinsamer Verantwortlichkeit unter der DSRL nicht entgegen.[798] Generell bedürfe es keiner umfassenden Kontrolle über alle Phasen und alle Gesichtspunkte der Verarbeitung hinweg, sodass insbesondere in „mehrstufige[n] Informationsanbieterverhältnisse[n]" eine auf bestimmte Abschnitte und Verarbeitungsumstände beschränkte Einflusssphäre ausreichen müsse, um Schutzlücken zu vermeiden.[799]

Der EuGH schloss sich diesen Ausführungen und Ansichten des Generalanwalts umfassend, wenn auch nicht in vergleichbarer Breite und Ausführlichkeit, an. Noch stärker als der Generalanwalt betonte er dabei vor allem zwei Aspekte: einerseits die Freiheit des Fanpage-Betreibers, eine sog. Parametrierung hinsichtlich derjenigen Kriterien vorzunehmen, nach denen Facebook die zur Erstellung der Besucherstatistik heranzuziehenden Besucherdaten auswähle.[800] Andererseits die Tatsache, dass die kausale Ermöglichung der von Facebook vorgenommenen Verarbeitungen von Besucherdaten hinsichtlich derjenigen Nutzer, die als nicht mit einem eigenen Konto auf dem Netzwerk von extern kommend die Fanpage besuchen, noch schwerer wiegt – schließlich befänden sich bereits angemeldete Nutzer sowieso eigenverantwortlich auf Facebook und könnte Facebook deren Daten jedenfalls teilweise unabhängig vom Besuch der einzelnen Fanpage verarbeiten, während die Daten von Nichtnutzern ohne deren Fanpagebesuch grundsätzlich nicht erreichbar gewesen wären.[801] Zudem stellte der Gerichtshof in genereller Weise erneut die insofern identische Empfehlung des Generalanwalts fest, wonach die (jederzeitige) Zugriffsmöglichkeit auf die zu verarbeitenden Daten im Rahmen der gemeinsamen Verantwortlichkeit nicht zwingend für jeden Verantwortlichen vorliegen müsse und das Fehlen dieser Möglichkeit somit auch hinsichtlich der Wirtschaftsakademie irrelevant sei.[802]

---

[798] Vgl. Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 60 f.

[799] Vgl. Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 62.

[800] EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 36–39.

[801] EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 41.

[802] EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 38; darauf bezugnehmend auch explizit noch einmal in anderer Konstellation festgehalten in EuGH, Rs. C-25/17 (Jehovan todistjajat), ECLI:EU:C:2018:551 Rn. 69.

bb) Der Fall Fashion ID

Einen ähnlich gelagerten und vom EuGH parallel behandelten, aber etwas später entschiedenen Fall legte das OLG Düsseldorf in der Sache Fashion ID vor. Dieser Fall betraf mit Fashion ID einen Online-Shop für Modeartikel, der auf seiner Website ein Facebook-Plugin in Form des sog. „Gefällt mir"-Buttons implementiert hatte.[803] Eine Einbindung dieser Art erfolgt mittels eines auf der jeweiligen Website gesetzten Verweises auf den entsprechenden externen Inhalt, der dann bei jedem Besuch der Website vom Browser des Besuchers angefordert und geladen wird. Gemeinsam mit der Anforderung des externen Inhalts übermittelt der Browser des Besuchers Informationen an den Server der Herkunftswebsite des externen Inhalts – darunter befindet sich die IP-Adresse des Besuchers sowie technische Daten über den Browser, aber auch weitere, ggf. personenbezogene, Daten in Form von verschiedenen Cookies und der Identität der Website, auf der sich der Button befindet.[804] Die Website selbst bzw. ihr Betreiber hat nach Einbindung des Verweises (hier in Form des „Gefällt-mir"-Buttons) keinen Einfluss mehr darauf, welche Daten übermittelt werden und welche Verarbeitungen zu welchen Zwecken durch den Empfänger vorgenommen werden.[805] Im vorliegenden Fall diente der eingebundene Button der Möglichkeit, auf die Existenz und Anzahl von „Fans" der Fanpage von Fashion ID auf Facebook hinzuweisen sowie Besuchern zu erlauben, noch auf der Website von Fashion ID die Fanpage mit „Gefällt mir" zu markieren. Zudem wurden bei Nutzern, die bereits ein Facebook-Konto besaßen und per Einstellung dauerhaft im Netzwerk eingeloggt waren, eine Vorschau von Profilbildern ihrer Freunde und anderer Netzwerkmitglieder angezeigt, die die Fanpage ebenfalls mit „Gefällt mir" markiert hatten. Personenbezogene Daten der Besucher der Fashion ID-Website wurden dabei unabhängig von der Existenz eines Facebook-Kontos und ohne Kenntnis oder gar aktives Mitwirken des Besuchers bereits im ersten Moment des Seitenaufrufs an Facebook übermittelt, unabhängig davon, ob dieser den „Gefällt mir"-Button betätigte oder nicht.[806]

Ausgangspunkt des Fall war eine von der Verbraucherzentrale NRW beim LG Düsseldorf gegen Fashion ID eingereichte Klage auf Unterlassung der Einbindung des beschriebenen Facebook-Plugins. Die Verbraucherzentrale berief sich auf eine Unlauterkeit der Praxis wegen Datenschutzwidrigkeit gem. § 3a UWG i. V. m. § 13 TMG durch fehlende rechtzeitige Aufklärung des Besuchers

[803] Siehe generell zur Funktionsweise der Überkategorie sog. *social plugins Kremer*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 28 Rn. 86 f.

[804] Eine ausführliche Erläuterung der technischen Abläufe findet sich bei LG Düsseldorf, Urt. v. 09.03.2016, Az. 12 O 151/15, in: MMR 2016, 328 (328) sowie bei OLG Düsseldorf, Beschl. v. 19.01.2017, Az. I-20 U 40/16, in: ZD 2017, 334 (334 f.).

[805] Vgl. zu all dem EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 26.

[806] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 27; LG Düsseldorf, MMR 2016, 328 (329).

über die durch Facebook vorzunehmenden Verarbeitungen und sah Fashion ID aufgrund der von ihr vorgenommenen Einbindung des Plugins als Verantwortliche gem. § 3 Abs. 7 BDSG. Das LG gab der Klage jedenfalls teilweise Recht und stufte Fashion ID als mit Facebook gemeinsam verantwortlich für die mittels des eingebundenen „Gefällt mir"-Plugins übermittelten und weiter verarbeiteten Besucherdaten ein. Dabei ordnete sie den Beitrag der Fashion ID in Form des aktiven und bewussten Implementierens des relevanten Plugins recht knapp und ohne Differenzierung zwischen den Wortlauten von § 3 Abs. 7 BDSG einerseits und Art. 2 lit. d DSRL andererseits bereits als „Beschaffen" der betroffenen Daten und damit als eigenständige Verarbeitungstätigkeit ein.[807] So löste bereits die Implementierung des Plugins zwingend die bei jedem Websitebesuch erfolgende Übermittlung eines HTML-Codes aus, der seinerseits die Übermittlung der Browseranfrage an den Facebook-Server anstoße und somit den ersten Teilakt des späteren Datenabrufs darstelle.[808] Dieser Anteil genüge bereits für eine eigene Verantwortlichkeit der Fashion ID und könne auch durch den fehlenden Einfluss auf die weiteren Verarbeitungsabschnitte, die fehlende Kenntnis über den Umfang und die genauen Zwecke der Verarbeitung und den fehlenden eigenen Zugriff auf die betroffenen Daten nicht wett gemacht werden.[809] Eine präzisere Auseinandersetzung mit dem Wortlaut von Art. 2 lit. d DSRL und der Frage des Einflusses auf insbesondere die Zwecke der Verarbeitung ließ das LG ebenso vermissen wie eine Konkretisierung der infragestehenden Verarbeitungsvorgänge.

Gegen das Urteil legten beide Parteien Berufung zum OLG Düsseldorf ein. Dieses sah sich, ähnlich wie das BVerwG in der Sache Wirtschaftsakademie, nicht in der Lage, den Erfolg der Berufung zu beurteilen, ohne die Auslegung der relevanten Abschnitte der DSRL zunächst vom EuGH klären zu lassen. Insbesondere fragte es diesen daher, ob die Einbindung eines Plugins wie dem von Facebook zur Einordnung des Einbindenden als datenschutzrechtlichen Verantwortlichen führe bzw. ob, wenn dies nicht der Fall sei, die DSRL die Haftung und Verantwortlichkeit abschließend regele oder ein Rückgriff auf zivilrechtliche Haftungsregime (wie das der Störerhaftung) nach nationalem Rechte möglich sei.[810] In seinem Vorlagebeschluss ließ es aber bereits gewisse Zweifel an der Verantwortlichenstellung der Fashion ID durchscheinen und betonte – ganz im Gegenteil zur Ansicht des LG Düsseldorf in der vorigen Instanz[811] –, die faktische Unmöglichkeit bzw. Datenschutzwidrigkeit des Einbezugs von Dritten bereitgestellter Inhalte mangels hinreichender Kontrolle über diesen Dritten.[812]

---

807 LG Düsseldorf, MMR 2016, 328 (330).
808 LG Düsseldorf, MMR 2016, 328 (330).
809 LG Düsseldorf, MMR 2016, 328 (330).
810 Siehe OLG Düsseldorf, ZD 2017, 334.
811 LG Düsseldorf, MMR 2016, 328 (330).
812 OLG Düsseldorf, ZD 2017, 334 (335).

Etwas umfassender und differenzierter als die beiden deutschen Gerichte beschäftigte sich sodann EuGH-Generalanwalt *Bobek* mit dem Fall, sowohl hinsichtlich der (datenverarbeitungs-)technischen Details als auch möglicher rechtspolitischer und realweltlicher Auswirkungen bestimmter Lesarten der Definition der Verantwortlichkeit. Er empfahl dem Gerichtshof letztlich die Fortsetzung der bereits mit Wirtschaftsakademie eingeschlagenen Richtung, das heißt eine Einordnung der Fashion ID und Facebook als gemeinsame Verantwortliche für die von Facebook mittels ihres auf der Website der Fashion ID eingebundenen Plugins.[813] Gleichzeitig können seine weiteren Ausführungen als Konkretisierungen und teilweise auch Relativierungen dieser Linie mit leisen kritischen Untertönen verstanden werden. So bezog *Bobek* explizit Stellung zu der Notwendigkeit einer durchdachten und klar zuordenbaren Definition gemeinsamer Verantwortlichkeit mit sinnvollen Kriterien, um eine uferlose Zuschreibung von Verantwortlichkeiten zu verhindern. Er schrieb:

„Das Problem liegt darin, dass die Abgrenzung der Verantwortlichkeit sich bisher nicht aus dem weiten Begriff des gemeinsam für die Verarbeitung Verantwortlichen ergibt. Die Gefahr einer zu weit gefassten Definition besteht darin, dass sie eine ganze Reihe von Personen gemeinsam für die Verarbeitung von personenbezogenen Daten verantwortlich sein lässt".[814]

Eine sachgemäße und die tatsächliche Verteilung von Macht und Einfluss widerspiegelnde Verteilung von Verantwortlichkeit sei daher nötig, um zu verhindern, dass Akteure zu Verantwortlichen gemacht würden, die die an sie adressierten Verpflichtungen gar nicht erfüllen können[815] oder hinter denen sich die primär kontrollierenden Akteure als bloß einige unter vielen verstecken könnten[816]. Weiter hob der Generalanwalt einmal mehr die Bedeutung des Wortlauts und damit der Kriterien der Entscheidung über *Zweck* und *Mittel* des konkreten *Verarbeitungsvorgangs* als entscheidenden Anknüpfungspunkt für die Strukturierung der Verantwortlichkeitszuschreibung heraus. Im Ergebnis kam er somit ebenfalls zum Ergebnis einer gemeinsamen Verantwortlichkeit von Fashion ID und Facebook, die sich allerdings explizit nur auf die Verarbeitungsphasen der *Erhebung* und *Übermittlung* der Besucherdaten erstrecken sollte, da der Einfluss des Websitebetreibers in Form der Entscheidung für den Einbezug des Plugins eben nur bis dorthin reiche und jedenfalls die nachfolgenden

[813] Vgl. Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 66 ff.

[814] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 75.

[815] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 93. Siehe zur grundlegenden Bedeutung dieser Prämisse für das datenschutzrechtliche Regelungskonzept auch *supra* bei B. II. 1.

[816] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 92.

Verarbeitungen durch Facebook umfasse.[817] Besondere Erwähnung verdienen neben diesem, zum Zeitpunkt der Veröffentlichung neuartigen, Fokus auf die konkreten Verarbeitungsphasen zur Konkretisierung der Verantwortlichkeitsreichweite, zudem die Ausführungen zur notwendigen Kongruenz der *Zwecke*: Hier erteilte *Bobek* dem Erfordernis einer kompletten *Identität* der jeweils verfolgten Zwecke eine Absage und lies eine kategorielle Ähnlichkeit bzw. „Einheit" sich „wechselseitig ergänzende[r]" Zwecke in Form von einerseits kommerziellen, andererseits werblichen Zwecken ausreichen.[818]

In seinem nachfolgenden Urteil schloss sich der EuGH diesen Empfehlungen des Generalanwalts weitgehend an und setzte die mit Wirtschaftsakademie begonnene Linie unter expliziter Bezugnahme fort.[819] Insbesondere griff er die vom Gerichtshof selbst zuvor noch abstrakt gelassene und vom Generalanwalt teilweise konkretisierte Überlegung einer nicht zwangsläufig gleichwertigen und daher je nach Verarbeitungsphasen und Ausmaß des Einflusses ihrem Grad nach im Einzelfall zu bestimmenden Verantwortlichkeit auf und stellte fest, dass eine gemeinsame Verantwortlichkeit nur soweit reichen könne, wie auch beide Akteure noch Einfluss auf die Mittel- und Zweckfestlegung haben.[820] Diesbezüglich sah der Gerichtshof – den Empfehlungen *Bobeks* folgend – eine gemeinsame Zweck- und Mittelfestlegung für die Verarbeitungsphasen der Erhebung und Übermittlung qua bewussten Einbezugs des „Gefällt mir"-Plugins (und damit Ermöglichung der Verarbeitung durch Facebook) zur Verfolgung kommerzieller und werblicher Ziele.[821]

c) Auswirkungen der EuGH-Linie seit Wirtschaftsakademie und Fashion ID

Die Veröffentlichung des initialen Bescheids des ULD Schleswig-Holstein, spätestens aber der Erlass des ersten Urteils durch das VG Schleswig, sollte den Beginn einer mit den endgültigen Entscheidungen des EuGH gipfelnden und bis dato noch immer andauernden Flut an Abhandlungen über die Möglichkeit und Notwendigkeit der erweiterten datenschutzrechtlichen Verantwortlichkeit im digitalen Umfeld darstellen. Dabei lässt sich grob unterteilen zwischen Ansichten, die die Sinnhaftigkeit der Idee dem Grunde nach diskutieren, und solchen, die mit den konkret zu ziehenden Schlüssen aus den Urteilen und ihrer Praxistauglichkeit hadern. Einerseits können die Urteile als erste praktische ge-

---

[817] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 102, 108.

[818] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 105.

[819] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629.

[820] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 70, 74 mit Verweis auf Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 101.

[821] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 77 ff.

richtliche Klärung des Rechtsinstituts der gemeinsamen Verantwortlichkeit angesehen werden und somit zur Konkretisierung der Tatbestandsmerkmale in Abgrenzung zur jeweils einzelnen Verantwortlichkeit der beteiligten Akteure und zu Beiträgen, die keine Verantwortlichkeit nach sich ziehen, beisteuern. Gleichzeitig geht mit ihnen eine nicht unerhebliche Öffnung der Verantwortlichkeit einher, die ihrerseits das Gegenteil von Konkretisierung erreicht, indem der nun größere Kreis potenziell Verantwortlicher nicht ohne weiteres bestimmbar erscheint.

aa) Generelle Rezeption

Der Gedanke einer (Mit-)Verantwortlichkeit von Akteuren, die (in den konkreten Fällen) die Infrastruktur und Verarbeitungen von Facebook nutzen und davon profitieren bzw. (genereller) die Infrastrukturen und Dienste datenverarbeitender Dritter, wie im Zeitalter arbeitsteiliger und mehrstufiger Informationsanbieterverhältnisse und Plattformen üblich, in ihre Dienste einbinden und die Früchte der Verarbeitungen genießen, ohne selbst eigenhändig Daten zu verarbeiten, löste dabei schon früh vielfältige Reaktionen aus.

Einerseits wurde, insbesondere aus Richtung der Aufsichtsbehörden, aber auch von Teilen der Literatur, die (rechtspolitische) Notwendigkeit einer solchen die neuartigen Modelle des Zusammenwirkens bei Datenverarbeitungen kompensierenden weit verstandenen Verantwortlichkeit benannt[822] und das grundlegende Vorgehen des ULD Schleswig-Holstein gegen die Wirtschaftsakademie, das auf einer Linie mit der Ansicht der deutschen Aufsichtsbehörden insgesamt war,[823] deshalb gelobt und wurden die Urteile von VG und OVG Schleswig kritisiert.[824] Auch die Vorlage zur Klärung der Zulässigkeit eines solchen Vorgehens durch den EuGH wurde in der der Hoffnung auf die gerichtlich festgestellte Verabschiedung von einem möglicherweise veralteten und überholten Konzept der Verantwortlichkeitszuschreibung begrüßt: „Man muss sich […] im Rahmen allgegenwärtiger Vernetzung und monopolartiger Plattformen

[822] In diese Richtung argumentiert auch (ohne Verweis auf die obigen Verfahren) *Engeler*, Die Auftragsdatenverarbeitung braucht ein Reboot – mit der DSGVO in der Hauptrolle: „In all diesen Fällen mangels konkreter Entscheidung über die eingesetzten Techniken und Prozesse automatisch die Verantwortlichkeit abzulehnen, wird der Wirklichkeit des Massenmarktes an digitalen Dienstleistungen nicht gerecht." Ebenso *Ernst*, NJOZ 2010, 1917 (1918); *Polenz*, VuR 2012, 207 (211).

[823] Vgl. schon *Düsseldorfer Kreis*, Datenschutz in sozialen Netzwerken: […] „Unternehmen, die durch das Einbinden von *social plugins* eines Netzwerks auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots."

[824] Vgl. *Karg*, ZD 2014, 51 (56), der von der Gefahr spricht, dass öffentliche wie private Stellen sich „der Anwendung deutschen öffentlichen Rechts durch geschickte Auswahl des Dienstes und einer entsprechenden Vertragsgestaltung […] entziehen". Vgl. auch *Petri*, ZD 2016, 231 (234); ebenso *Föhlisch/Pilous*, MMR 2016, 328 (331); *Weichert*, ZD 2014, 605 (605 ff.).

fragen, ob dieses Konzept noch forensischen und haftungstechnischen Kriterien gerecht wird."[825]

Demgegenüber stand die (insgesamt wohl überwiegende) Skepsis großer Teile der Literatur, aber auch vieler Praktiker hinsichtlich drohender Haftungsrisiken und weiterer Auswirkungen auf etablierte Geschäftsmodelle und Praktiken.[826] Andere brachten der Idee einer Erweiterung der Verantwortlichkeit zwar Sympathien entgegen, sahen eine Herleitung *de lege lata* aber als nicht gegeben an und daher den Gesetzgeber in der Pflicht.[827]

Noch zahlreicher und kontroverser wurden die Reaktionen auf die Entscheidungen des EuGH zu den beiden Fällen. Auch hier wechselten sich Zustimmung[828], Ablehnung[829] und generelle Ratlosigkeit ob der Konsequenzen[830] ab.

bb) Die Tatbestandsmerkmale – Konkretisierung oder bleibende Unschärfe?

Inhaltlich konzentrierten sich die Reaktionen einerseits auf die definitorischen Auswirkungen der Urteile. Zwar hatte der EuGH – aufbauend auf dem funktio-

[825] *Marosi*, Fanpages vor dem Bundesverwaltungsgericht; Ähnlich auch *Petri*, ZD 2016, 393 (399): „[…] liegt es aber zumindest heute durchaus nahe, bei bewusst arbeitsteiligem Vorgehen zumindest eine gewisse Mitverantwortlichkeit des Inhalteanbieters anzunehmen, der die datenschutzwidrig betriebene Infrastruktur eines anderen Anbieters auswählt."

[826] Vgl. etwa *Werkmeister/Schröder*, ZD 2014, 643 (646), die argumentieren, eine Ausweitung könne „nicht kalkulierbare Haftungsrisiken nach sich ziehen, da bereits die bloße Nutzung eines Diensts ohne Einfluss auf etwaige Datenverarbeitungsvorgänge des Diensteanbieters eine datenschutzrechtliche (Mit-)Verantwortlichkeit begründen". Ebenso, bereits ganz zu Beginn der Debatte, *Voigt/Alich*, NJW 2011, 3541; *Piltz*, CR 2011, 657 (662).

[827] So *Hoffmann/Schulz*, Facebook-Fanseiten deutscher Unternehmen – Verlängerung vor dem EuGH: „Insofern dürften die Gerichte – BVerwG wie EuGH – nicht der richtige Ort sein, um Erweiterungen der Verantwortlichkeiten jenseits des geschriebenen europäischen und nationalen Rechts zu diskutieren. Gefordert sind die europäischen und ggf. nationalen Gesetzgeber."

[828] Vgl. *Petri*, EuZW 2018, 534 (540); *Lindroos-Hovinheimo*, Information & Communications Technology Law 2019, 225 (233) zum Wirtschaftsakademie-Urteil: „[…] the judgment is concise and the analysis follows a clear and logical form." Zustimmend im Grunde auch *Globocnik*, IIC 2019, 1033 (1037), der aber eine weitergehende als die im Fashion ID-Urteil explizit herausgestellte auf beeinflussbare Verarbeitungsphasen begrenzte Verantwortlichkeit fordert. In die gleiche Richtung gehend *Zalnieriute/Churches*, When a ‚Like' is not a ‚Like', S. 879 ff.; siehe außerdem *Lee/Cross*, MMR 2019, 559 (560 f.); stellvertretend für die behördliche Zustimmung *Die Landesbeauftragte für den Datenschutz Niedersachen*, 25. Tätigkeitsbericht 2019, S. 51 f.

[829] So etwa *Schulz*, ZD 2018, 357: „[…] würde die Verantwortlichkeit ins Unendliche ausdehnen […]." Vgl. auch *Ducuing* u. a., EDPL 2018, 547: „[…] it will in our view at least remain difficult to delineate respective processing activities and responsibilities […]." Ähnlich kritisch *Edwards* u. a., Data subjects as data controllers.

[830] Vgl. *Marosi/Matthé*, ZD 2018, 357 (363): „[…] ein Urteil, das mehr Fragen aufwirft, als es beantwortet." Siehe auch *Blanc*, EDPL 2018, 120 (124), der die Frage aufwirft, ob damit auch Betreiber von Seiten auf anderen sozialen Netzwerken oder gar private Nutzerprofile verantwortlich würden. Zwiegespalten auch *Paun*, EuCML 2020, 35 (37), die Schwierigkeiten bei der trennscharfen Aufteilung nach Verarbeitungsphasen in der Praxis sieht und zusätzliche Intransparenzen ob der resultierenden Pflichtenlimitierung befürchtet.

nalen Ansatz der *Art. 29-Datenschutzgruppe*[831] – gewisse Konkretisierungen des Tatbestandsmerkmals der Entscheidung über die Mittel und Zwecke der Verarbeitung erreicht. Doch wie diese im Detail zu verstehen sind, welche Anforderungen also zwingend gestellt werden, ist bis dato unklar geblieben. Aus der Gesamtschau der beiden Urteile lassen sich verschiedene jeweils zentrale Beitragselemente entnehmen, die, je nach Lesart der Urteile, wahlweise alternativ, kumulativ oder gar nicht zwingend vorliegen müssen. Rückgeführt auf die Dogmatik der DSGVO geht es darum, wann ein (insbesondere nur geringfügig entscheidungsbefugter und nicht unmittelbar mit den zu verarbeitenden Daten befasster) Akteur hinreichenden Einfluss auf die Zwecke und Mittel der Verarbeitung ausübt.[832]

Eine Lesart der beiden Urteile wäre es, die bloße kausale Ermöglichung der Verarbeitung durch den zweiten Akteur, in den konkreten Fällen also Facebook, ausreichen zu lassen. In beiden Fällen betonen sowohl der EuGH selbst[833] als auch die Generalanwälte[834] die herausgehobene Bedeutung dieses Elements der Einflussnahme durch den vordergründigen Akteur. Würde dieser keine Fanpage eröffnen bzw. das Facebook-Plugin nicht auf seiner Website einbinden, wäre Facebook faktisch nicht in der Lage, jedenfalls diese konkret anfallenden Daten der entsprechenden Besucher zu verarbeiten.[835] Klar ist, dass mit einem solchen Definitionsverständnis auf dem Papier der weitreichendste Schutz für Betroffene einhergehen würde. Dogmatisch ließe sich dieser Beitrag als Entscheidung über die Mittel der Verarbeitung vergleichsweise leicht konstruieren. Zwar bleibt dem die Infrastruktur von Facebook nutzenden Akteur nur ein „alles oder nichts"-Modell, da er (mit Ausnahme der gleich noch zu behandelnden Parametrierung im Falle einer Fanpage) keinen Einfluss auf die Einzelheiten der Verarbeitungsumstände hat – weder vertraglich noch technisch kann er Facebook dazu bewegen, die Anzahl der Daten oder die Art und Weise der Verarbeitung anzupassen. Dennoch ist die bloße Entscheidung zugunsten der Nutzung der Infrastruktur bereits so weitreichend, selbst wenn sie sich „nur" auf

---

831 Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 12.

832 A. A. *Mahieu* u. a., jipitec 2019, 85 (95), nach denen Generalanwalt und EuGH die Unterscheidung zwischen den beiden Merkmalen völlig fallengelassen hätten: „‚Purposes and means' is consistently used as one noun-phrase and there is no discussion if and to what extent both elements are needed to be a controller."

833 Vgl. EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 34; Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 75.

834 Vgl. Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 56; Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 103.

835 Dass dabei der Verursachungsgrad für Besucher ohne eigenes Konto bei Facebook naturgemäß höher ist als bei solchen mit Konto, betont auch der EuGH, so etwa in Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 41 und Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 83.

ein bereits von Facebook fertig geschnürtes Verarbeitungspaket bezieht, dass die Qualifizierung als ausreichender Beitrag zur Mittelentscheidung vertretbar erscheint.[836] Dieser Gedanke ließe sich grundsätzlich auch auf andere Konstellationen übertragen, in denen ein Akteur durch sein Tun die Datenverarbeitung durch einen Dritten unmittelbar ermöglicht. Denkbar wären hier aber eingrenzende Voraussetzungen bzw. eine Schärfung des Begriffs der Unmittelbarkeit – ähnlich wie im Strafrecht oder Deliktsrecht würde ein reines Abstellen auf ein *conditio-sine-qua-non*-Element die Kausalitätskette viel zu weit werden lassen. Teils wird bereits in das Fashion ID-Urteil eine solche Eingrenzung in Form eines zusätzlich vorliegenden kognitiven Elements, also des Wissens darum, durch den Einbezug bzw. die Nutzung fremder Infrastruktur bestimmte Verarbeitungsvorgänge zu ermöglichen, hereingelesen.[837]

Weitaus schwieriger wäre unabhängig davon jedenfalls der notwendige Beitrag zu den Verarbeitungs*zwecken* nach dieser Lesart zu konstruieren. Lässt man bereits einen Beitrag des Akteurs genügen, der sich darin erschöpft, dass er die Verarbeitung faktisch ermöglicht, so bleibt allein eine konkludente, stillschweigende Akzeptanz bzw. Billigung der Zwecke des Anbieters der eingebundenen Infrastruktur, die man als Einfluss auf die Zweckbestimmung verstehen könnte. Dies aber erscheint bei aller Öffnung und dogmatischen Weiterentwicklung zu weitgehend.[838] Nicht umsonst wiegt nach Ansicht der *Art. 29-Datenschutzgruppe* der Einfluss auf die Zwecke regelmäßig schwerer als der auf die Mittel[839] und ist hier also ein strengerer Maßstab gefragt. Die bloße Billigung fremder Zwecke kann dafür kaum ausreichen. Nicht zuletzt widerspräche ein solches Verständnis auch dem Wortlaut der beiden EuGH-Urteile, die zwar kein gänzlich einheitliches Verständnis hinsichtlich der (gemeinsamen) Zweckbestimmung an den Tag legen, sich aber jedenfalls darin einig sind, ein gewisses „Mehr" zu verlangen. Mit Blick auf das Wirtschaftsakademie-Urteil könnte das Element der sog. Parametrierung dieses gewisse „Etwas" darstellen.[840] Nach Ansicht des Gerichtshofs war es in diesem Fall gerade die Tatsache, dass Fanpage-Betreiber die Parameter der zu verarbeitenden Daten und damit den Zuschnitt der Betroffenen, aber auch den detaillierten Zweck der Verarbeitung, selbst festlegen konnten, der zur Einordnung als Verantwortlicher führte. Letzt-

---

836 So etwa *Hanloser*, ZD 2019, 455 (459); a. A. aber *Marosi/Matthé*, ZD 2018, 357 (362).

837 Vgl. *Hanloser*, ZD 2019, 455 (459), wohl gestützt auf EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 77; so auch verstanden von *Paun*, EuCML 2020, 35 (37); *Mahieu* u. a., jipitec 2019, 85 (95).

838 So den EuGH verstehend (und kritisierend) aber *Lee/Cross*, MMR 2019, 559 (561 f.), wonach dieser letztlich „eine Abstraktion einer der beiden Voraussetzungen [vornimmt], sobald die jeweils andere Voraussetzung vorliegt".

839 Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17.

840 So auch, allerdings noch vor Erlass des Fashion ID-Urteils, *Marosi/Matthé*, ZD 2018, 357 (362).

lich wirkt ein solcher Einfluss auf die Auswahl der konkret zu verarbeitenden Daten sowohl auf die Mittel als auch auf die Zwecke der Verarbeitung ein, ist er doch Ausdruck des „erwartete[n] Ergebnis[ses], das beabsichtigt ist oder die geplanten Aktionen leitet“[841] und bestimmt gleichzeitig wesentliche Umstände und Aspekte der betroffenen Daten bzw. der Personen, auf die sie verweisen.

Gleichwohl kam derselbe Gerichtshof in seinem Fashion ID-Urteil ebenfalls zum Ergebnis der Verantwortlichkeit, obwohl eine solche Parametrierung dort nicht gegeben war. Stattdessen stellten der Generalanwalt[842] wie auch der Gerichtshof selbst hier auf eine Art Zweckkongruenz[843] ab, die, gewissermaßen als mitenthaltenes Minus, auch Fällen der Parametrierungen zugrunde liegt. Entscheidend abgestellt wird dabei auf die Tatsache, dass die einbeziehende Partei und Facebook jeweils einen konkreten Profit aus dem Zusammenwirken ziehen, ohne dass dieser Profit vollkommen identisch sein muss.[844] Beeinflusst eine Partei also aktiv den Zuschnitt der zu verarbeitenden Daten und damit, wie im Wirtschaftsakademie-Fall, auch den Aussagegehalt der Statistiken, die sie später zu Gesicht bekommt, so steht hinter dieser Handlung die Erwartung, aus dem aus diesen Statistiken ausgehenden Erkenntnisgewinn (etwa: Besucht meine primäre Zielgruppe meine Seite? Welche Schnittmenge der Zielgruppe muss ich noch besser ansprechen?) Vorteile zu ziehen.[845] Nach diesem Verständnis wäre die im Wirtschaftsakademie-Urteil festgestellte Parametrierung zwar eine hinreichende (eher: überschüssige oder überobligatorische), aber eben keine notwendige Voraussetzung und hätte der EuGH erst mit seinem Fashion ID-Urteil das erforderliche Mindestmaß bzgl. des nötigen Beitrags zur Zweckbestimmung festgesetzt. Fraglich wäre dann, wie stark die Kongruenz zwischen den jeweils verfolgten Zwecke sein müsste. Auch hier kann ein Gefälle zwischen den beiden Urteilen festgestellt werden: Teilte im Fall der Wirtschaftsakademie noch Facebook die eben erwähnten Datenverarbeitungsergebnisse in Form von Statistiken mit dem Fanpage-Betreiber und lässt sich somit

---

[841] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, S. 16.

[842] Dieser warf aber zumindest auch die – letztlich nicht überzeugende – Möglichkeit auf, bereits die reine Implementierung des Plugins könnte eine Parametrierung darstellen, vgl. Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 69. Dahinter steht letztlich wieder der Gedanke einer Billigung, hier nämlich der von Facebook selbst gesetzten Parameter, nach denen das Plugin Besucherdaten verarbeitet. Eine *aktive* Parametrierung wie im Wirtschaftsakademie-Urteil kann darin aber kaum gesehen werden.

[843] So auch *Golland*, K&R 2018, 433 (435 f.), der ausführlich die letztliche Abängigkeit von Kongruenz oder Inkongruenz von Abstraktionshöhe und Betrachtungswinkel bei der Zweckbestimmung aufzeigt.

[844] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 105 spricht hier von einer „Einheit“ der kommerziellen und werblichen Zwecke.

[845] Vgl. *Martini/Fritzsche*, NVwZ-Extra 2015, 1 (3).

ein gemeinsamer, auf die zu verarbeitenden Daten und den daraus folgenden Erkenntnisgewinn gerichteter, Zweck formulieren, so kamen Fashion ID im dem zweiten Urteil zugrundeliegenden Fall keine Statistiken oder anderen Verarbeitungsergebnisse zuteil. Hier lag der Vorteil für den Websitebetreiber darin, zusätzliche Werbung in Form von Mund-zu-Mund-Propaganda seiner Kunden und so generell zusätzliche Aufmerksamkeit zu generieren, indem er sich die Reichweite von Facebook zunutze machte.[846] Demnach würde eine hinreichende Kongruenz bereits bei jeweiligen wirtschaftlichen Interessen genügen, die mit dem Einbezug bzw. der Nutzung der Infrastruktur des Dritten, in diesem Falle Facebook, verfolgt werden.[847] Ob der Nutzen für den Einbeziehenden sich, wie bei Fashion ID, bereits aus dem Einbezug selbst ergibt oder, wie bei Wirtschaftsakademie, unmittelbar mit den infragestehenden Datenverarbeitungen zusammenhängt, wäre somit irrelevant. Denkbar wäre zudem das Erfordernis eines Konnexes zwischen den Zwecken in Form einer Wechselseitigkeit der Interessen.[848] Ob dies als einschränkendes Merkmal taugen kann, darf jedoch bezweifelt werden – ein irgendwie gearteter wechselseitiger Vorteilsgewinn für alle Beteiligten liegt dem Phänomen der Nutzung fremder Infrastrukturen bzw. dem Einbezug fremder Versatzstücke wie Plugins oder Code-Schnipseln schließlich gerade inne. Offen bleibt, ob dabei, wie in den beiden Urteilen vorliegend, stets ein im weitesten Sinne wirtschaftlicher Vorteil notwendig ist, oder auch nichtwirtschaftliche Interessen ausreichen.[849]

Abschließend lässt sich damit festhalten, dass – nach derzeitigem Stand – jedenfalls eine gewisse Konturierung sowie eine nicht unerhebliche Ausweitung der Tatbestandsmerkmale der (gemeinsamen) Verantwortlichkeit infolge der jüngeren EuGH-Rechtsprechung festzustellen ist. Auf Seite der notwendigen Mittelbeiträge genügt ein vom Wissen des Akteurs getragener Beitrag, der kausal die Verarbeitung ermöglicht, selbst wenn die dahinterstehende Entscheidung sich nur auf das „Ob", nicht aber auf die Einzelheiten der ermöglichten Verarbeitung erstreckt.[850] Auf Seite der notwendigen Zweckbeiträge genügen separat verfolgte, aber miteinander in Verbindung stehende, Zwecke der Akteure in Form von Vorteilen, die sich wahlweise aus den ermöglichten Datenver-

---

[846] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 80.

[847] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 80.

[848] Vgl. Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 105; auch EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 80 lässt sich dahingehend verstehen, wenn dort von der Datennutzung durch Facebook als „Gegenleistung für den Fashion ID gebotenen Vorteil" die Rede ist. Auch *Europäischer Datenschutzausschuss*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 20 f. interpretiert den EuGH so.

[849] Siehe dazu auch die Überlegungen im nächsten Abschnitt bei cc) (2).

[850] So auch die Lesart von *Europäischer Datenschutzausschuss*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 21.

arbeitungen oder schlicht aus der Nutzung der Infrastruktur bzw. dem einbezogenen Code ergeben.[851]

cc) Die Konsequenzen

Zum Abschluss soll nun kurz angerissen werden, welche Konsequenzen aus diesen Erkenntnissen und Veränderungen folgen (könnten). Dabei werden nicht alle aufgeworfenen Fragen abschließend beantwortet werden (können) – teils, weil es bis dato schlicht keine abschließende Antwort gibt, teils, weil sie im nächsten Kapitel noch ausführlich behandelt werden.

Hier drängen sich in erster Linie drei Fragen auf: Welchen konkreten Zweck kann der EuGH mit der Ausweitung des Anwendungsbereichs der Verantwortlichkeit verfolgt haben, wie könnte diese also zu einer besseren Gewährleistung eines „wirksamen und umfassenden Schutz[es]" der Betroffenen beitragen? Auf welche anderen Konstellationen und Akteure lassen sich die Feststellungen übertragen, wann liegt nun also noch überall eine gemeinsame Verantwortlichkeit (insbesondere bisher vermeintlich Nichtverantwortlicher) vor? Und welche Feststellungen hat der EuGH bzgl. des Ausmaßes der jeweiligen Verantwortlichkeit getroffen – sowohl hinsichtlich der Stellung an sich als auch hinsichtlich der Reichweite einzelner Pflichten?

(1) Die erhoffte Wirkung

Hinsichtlich der konkreten Art und Weise, mittels derer die erweiterte Verantwortlichkeit in den beiden durch den EuGH entschiedenen Fällen das Schutzniveau für Betroffene erhöhen soll, lassen sich zwei parallel laufende Anknüpfungspunkte bzw. Stoßrichtungen herausbilden: die unmittelbare, durch die neue Pflichtigkeit ausgelöste Verhaltenssteuerung des dem Betroffenen näherstehenden Einzelakteurs, der sich Dienste oder Infrastruktur eines größeren Akteurs zunutze macht, in den beiden Fällen also des Fanpage-Betreibers respektive des das Facebook-Plugin nutzenden Websitebetreibers; zudem die durch dessen Verantwortlichkeit ausgelöste mittelbare Verhaltenssteuerung des im Hintergrund befindlichen, aber unmittelbar die betreffenden Daten verarbeitenden Akteurs, in diesen Fällen also Facebook.

Blickt man zunächst auf die unmittelbare Verhaltenssteuerung des Einzelakteurs, fällt sofort dessen sehr begrenzte Handlungsfähigkeit auf. Bereits die einzelnen mit den Fällen befassten Gerichte[852], insbesondere aber die zahlrei-

---

[851] Vgl. *Europäischer Datenschutzausschuss*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 20: „[…] joint controllership may also […] be established when the entities involved pursue purposes which are closely linked or complementary. […] Such may be the case, for example, when there is a mutual benefit arising from the same processing operation […]."

[852] Siehe hier besonders prägnant Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH,

chen Kritiker der Urteilslinie[853] betonten die schwache Position einzelner Akteure gegenüber Facebook. Wollen diese Statistiken über die Besucher ihrer Fanpage bzw. den „Like"-Button auf ihrer Website einbinden, so sind sie gezwungen, die von Facebook einseitig angebotenen Bedingungen zu akzeptieren – Raum für Verhandlungen, etwa über die Weiterverwendung der gewonnenen Besucherdaten durch Facebook für eigene Zwecke, existiert nicht. Vermag die Argumentation, der Beitrag dieser Akteure sei dennoch so gewichtig, dass eine Verantwortlichkeit sich als zwingend darstellt, im Ergebnis auch überzeugen, muss nun doch die Frage aufgeworfen werden, welches Handeln mit positiver Wirkung für Betroffene sich die Regulierungsinstanz erhofft. Eine Besserung der Situation für Betroffene unmittelbar durch eine entsprechende Verhaltensanpassung des jeweiligen Verantwortlichen selbst – so wie klassischerweise im Regelungskonzept des Datenschutzrechts angedacht – ist hier auf den ersten Blick einzig dadurch denkbar, dass dieser sich von Facebook abwendet und seine Zielgruppe durch einen anderen Anbieter mit vergleichbarer Reichweite und besseren Datenschutzstandards zu erreichen versucht.[854] In diese Richtung lässt sich auch das BVerwG verstehen, das im Falle Wirtschaftsakademie nach Urteil und Zurückverweisung durch den EuGH urteilte, die Abschaltungsanordnung durch das ULD sei rechtmäßig (und insbesondere nicht etwa, mit Blick auf die Möglichkeit der Inpflichtnahme von Facebook selbst, ermessensfehlerhaft), weil ihm effektive Mittel zur Beseitigung des Rechtsverstoßes zur Verfügung stünden; da jedoch kein unmittelbarer (vertraglicher oder technischer) Einfluss auf Facebook zur rechtskonformen Ausgestaltung der Verarbeitungstätigkeit bestünde, bliebe als Maßnahme einzig die Abschaltung seiner Fanpage.[855] Etwas ausdifferenzierter könnte die Antwort in Szenarien mit *social plugins*, wie im Falle Fashion ID, aussehen. Hier steht das endgültige Urteil des OLG Düsseldorf (und dann ggf. des BGH) noch aus, doch hat die Praxis im Laufe des langjährigen Prozesses die Problematik der Fallgestaltung bereits überholt: Plugins dieser Art werden inzwischen regelmäßig nur noch als sog. Zwei-Klick-Lösung eingebunden, müssen also bei Besuch der Seite vom Besucher erst durch aktives Handeln aktiviert werden, bevor sie Daten an die Server des Plugin-Anbieters senden.[856] In Fällen anderer Plugins, die eine ent-

---

Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 84. Diesem zufolge führe die unvorsichtige Ausweitung der Verantwortlichkeit ggf. „in einen Bereich, in dem einem potenziellen gemeinsam für die Verarbeitung Verantwortlichen die Erfüllung geltenden Rechts tatsächlich unmöglich ist".

853 Vgl. etwa *Kartheuser/Nabulsi*, MMR 2018, 717 (720).

854 *Blanc*, EDPL 2018, 120 (124): „Thus, the platform's reputation as regards data processing might become one of the choice criteria for a fan page administrator […]."

855 BVerwG, Urt. v. 11.09.2019, Az. 6 C 15.18 (Wirtschaftsakademie Schleswig-Holstein) Rn. 32.

856 Vgl. *Solmecke*, in: Hoeren u. a., Handbuch Multimedia-Recht, Teil 21.1. Rn. 49; siehe ebenfalls *Kremer*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 28

sprechende Ausgestaltung nicht anbieten, bleibt nur der Verzicht auf die Einbindung.[857]

Ob der quasi-singulären und konkurrenzlosen Stellung von Facebook und anderen, vergleichbar marktmächtigen Plattformen, können die Erfolgsaussichten dieser unmittelbaren Verhaltenssteuerung aber nicht nur in diesen, sondern auch in anderen denkbaren Anwendungsfällen angezweifelt werden: Trotz der Vielzahl an bspw. sozialen Netzwerken insgesamt – die Problematik der sich kaum unterscheidenden jeweiligen Datenschutzniveaus noch gänzlich ausklammernd –, verteilen sich diese größtenteils doch auf unterschiedliche Zielgruppen und Nischen und bleibt tatsächliche Konkurrenz somit größtenteils aus, sodass ein breitflächiges Abwandern von Betreibern, jedenfalls zu anderen Anbietern, eher nicht zu erwarten ist.[858]

Nicht nur mit Blick auf die eben beschriebene Limitierung der Verhaltensänderungsmöglichkeiten des Einzelnen, sondern auch generell über den bloßen Einzelfall hinaus gedacht, dürfte die zweite denkbare Zielrichtung von größerer Bedeutung sein: Von der Gefahr der Abwendung zahlreicher Nutzer des Fanpage-Angebots – sei es aus Angst vor Haftungsrisiken, sei es aus gewachsener Kenntnis oder Überzeugung von den datenschutzwidrigen Praktiken von Facebook – ausgehend könnte Facebook sich mittelbar gezwungen sehen, sein bis dato datenschutzwidriges Angebot datenschutzkonform zu gestalten. Dieser Gedanke wurde vom BVerwG in seinem Wirtschaftsakademie-Urteil explizit erwähnt. So könne Facebook bei Bestand der Abschaltungsanordnung unter „Zugzwang" gesetzt werden, sich „um eine datenschutzrechtskonforme Lösung bemühen [zu] müssen, um sein Geschäftsmodell in Deutschland weiterverfolgen zu können."[859] Problematisch könnte dieser letztlich also darauf gerichtete Versuch, Facebook treffende Datenschutzbestimmungen durch die Hintertür[860] und auf dem Rücken der nun ebenfalls verantwortlichen Einzelakteure effektiver durchzusetzen, aus zwei sich gegenseitig bedingenden Gründen sein. Zum einen bleibt fraglich, ob der erhoffte Abschreckungseffekt wirklich eintritt und Facebook und vergleichbar marktmächtige Akteure sich tatsächlich gezwungen sehen, ihre Praktiken anzupassen. Bisher ist von einer solchen Entwicklung

---

Rn. 88 mit Verweis auf die freilich dadurch nicht gelöste Grundproblematik der Datenschutzwidrigkeit der Verarbeitung durch den Bereitsteller des Plugins.

[857] So jüngst etwa VG Wiesbaden, Beschl. v. 01.12.2021 – 6 L 738/21.WI Rn. 66 bzgl. eines (öffentlich-rechtlichen) Unterlassungsanspruchs aus § 1004 BGB gegen die Einbindung eines fremden Dienstes auf einer Website: „Die Rechtsverletzung des Antragstellers kann nur abgestellt werden, indem der Dienst insgesamt von der Website genommen wird."

[858] So auch *Blanc*, EDPL 2018, 120 (124): „However, this new form of incentive may be somewhat limited by the lack of alternative among social networks."

[859] BVerwG, Urt. v. 11.09.2019, Az. 6 C 15.18 (Wirtschaftsakademie Schleswig-Holstein) Rn. 31.; siehe auch mit diesem Verständnis bereits vor Erlass des Urteils *Blanc*, EDPL 2018, 120 (124); ebenfalls in diese Richtung argumentierend *Mahieu* u. a., jipitec 2019, 85 (96).

[860] *Globocnik*, IIC 2019, 1033 (1042) spricht von „enforcement against Big Tech by the back door".

noch wenig zu sehen und hat etwa Facebook nach wie vor keinen überzeugenden Vertrag über die Verteilung der Pflichten innerhalb der gemeinsamen Verantwortlichkeit gem. Art. 26 Abs. 1 S. 2 DSGVO bereitgestellt – eine der eindeutigsten und grundlegendsten aus dem Urteil folgenden Pflichten.[861] Zum anderen ist fraglich, ob die entstehenden und die zahlreichen nun verantwortlichen Einzelakteure treffenden Kollateralschäden[862] in einem angemessenen Verhältnis zu dieser erhofften Wirkung stehen. Gerade in diesem Lichte sind wohl auch die im Fashion ID-Urteil spezifizierten Limitierungen der Verantwortlichkeit auf Verarbeitungsphasen, an denen Websitebetreiber konkret beteiligt sind, zu verstehen – eine überbordende Verantwortlichkeit soll verhindert werden, um den drohenden Schaden zu begrenzen. Dabei versucht man freilich die Quadratur des Kreises, denn die eine Zielrichtung behindert die andere: Soll Facebook unter Druck gesetzt werden, setzt dies die echte Gefahr eines Absprungs von Kunden voraus – dies wiederum hängt in starkem Maße von deren Haftungsrisiken ab, die aber gleichzeitig möglichst gering gehalten werden sollen. Hier zeigt sich die inhärente Widersprüchlichkeit des vom EuGH gewählten Wegs. Ist das Mittel, die die Verarbeitungen auslösenden Einzelakteure in die Verantwortung zu nehmen, um damit das Datenschutzniveau der verarbeitenden Plattformen mittelbar zu erhöhen, grundsätzlich nachvollziehbar, erscheint es für die Erreichung des verfolgten Zwecks insgesamt doch nur bedingt zielführend.

Zwar ist daher einleuchtend, dass einzelne, meist lokale Fanpage-Betreiber oder *social plugin*-nutzende Websitebetreiber für Aufsichtsbehörden leichter zu greifen und Datenschutzrecht daher leichter durchzusetzen ist als gegenüber großen Plattformen wie Facebook, bei denen auch unter dem harmonisierten Rechtsrahmen der DSGVO noch die jeweiligen Zuständigkeiten mitgliedstaatlicher Aufsichtsbehörden beachtet werden müssen. Eine ausreichende Anzahl einzelner Akteure zu belangen, um einen wirksamen Einfluss auf Facebook und andere Plattformen auszuüben, erscheint aber unter dem Eindruck des eben Gesagten wie eine Sisyphos-Aufgabe. Sollte es hier tatsächlich völlig an der beabsichtigten Wirkung fehlen, so hätte dies mit dem oben zur Verhältnismäßigkeit des Verantwortlichkeitskonzepts Gesagten[863] ggf. auch Implikationen für die unionsgrundrechtliche Legitimität mit Blick auf die Grundrechte der neu erfassten Akteure.

---

[861] Vgl. *Datenschutzkonferenz (DSK)*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit: „Diese von Facebook veröffentlichte ‚Seiten-Insights-Ergänzung bezüglich des Verantwortlichen' erfüllt nicht die Anforderungen an eine Vereinbarung nach Art. 26 DSGVO."

[862] *Globocnik*, IIC 2019, 1033 (1042).

[863] Siehe dazu *supra* bei B. III. 1.

(2) Die Übertragbarkeit auf andere Fälle

Bei den Erwägungen zu den Tatbestandsmerkmalen bereit angesprochen wurde die Frage nach der Übertragbarkeit auf andere, ähnlich gelagerte Fälle. Auch wenn der EuGH grundsätzlich nur konkrete Vorlagefragen bzgl. der Auslegung von EU-Recht für konkrete Sachverhalte beantwortet, erwächst daraus auch eine Bedeutung für die Auslegung über den konkreten Fall hinaus.[864] Vorliegend sind die Erwägungen zur weiten Auslegung der datenschutzrechtlichen Verantwortlichkeit in arbeitsteiligen Verarbeitungsszenarien dementsprechend in großen Teilen abstrakt genug gehalten, um legitime Überlegungen über die generalisierte Anwendbarkeit anzustellen. Generalanwalt *Bobek* bezog in seiner Stellungnahme im Vorlauf der Fashion ID-Entscheidung die Auswirkungen des Urteils auf andere Fälle ähnlicher Art explizit in seine Überlegungen mit ein und machte sie zu einem entscheidenden Kriterium für das Herausarbeiten legitimer Auslegungsergebnisse:

„Soll also die in zupackender Weise getroffene Bestimmung des Begriffs der (gemeinsamen) Verantwortlichkeit nicht in eine an alle Akteure gerichtete und gerichtlich gestützte Anordnung mutieren, offline zu gehen und soziale Netzwerke, Plugins sowie gegebenenfalls sonstige Drittinhalte nicht mehr zu nutzen, muss bei der Bestimmung der Verpflichtungen und Verantwortlichkeiten die Lebenswirklichkeit eine Rolle spielen, wobei wiederum die Fragen von Kenntnis, originärer Verhandlungsmacht und der Fähigkeit, auf beliebige der hier in Rede stehenden Aktivitäten Einfluss zu nehmen, einzubeziehen sind.“[865]

Klar scheint zunächst, dass mit der durch die Urteile hinzugewonnenen Aufmerksamkeit auf das Institut der gemeinsamen Verantwortlichkeit sich in vielen Szenarien gemeinsame Verantwortlichkeiten offenbaren werden, in denen die betroffenen Akteure sich bereits bis dato ihrer jeweils verarbeitungserheblichen Beiträge bewusst waren, aber von wahlweise getrennten Einzelverantwortlichkeiten oder Auftragsverarbeitungsverhältnissen ausgegangen waren.[866] Hier ist zu erwarten, dass die weitreichende Berichterstattung zu einem Augenöff-

[864] Die jeweilige Vorlagefrage beschränkt sich also nicht auf die Bedeutung für den Ausgang des konkreten Verfahrens, sondern kann auch Bedeutung für die generelle Auslegung des Unionsrechts sein. Sie ist daher stets „mit einem ausreichenden Abstraktionsgrad auf die Auslegung oder die Gültigkeit einer konkreten Unionsvorschrift zu richten, sollte aber andererseits […] den konkreten Rechtsstreit und/oder die innerstaatlichen Rechtsvorschriften einbeziehen“. Vgl. Karpenstein, in: *Grabitz* u. a., Das Recht der Europäischen Union, Art. 267 AEUV Rn. 32.

[865] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 93.

[866] Vgl. etwa *Gierschmann*, ZD 2020, 69 (71): „Die EuGH-Rechtsprechung macht deutlich, dass weit mehr Anwendungsfälle für eine gemeinsame Verantwortlichkeit in Frage kommen als bisher angenommen.“ Ebenso *Kremer*, CR 2019, 676 (688): „Damit sind im arbeitsteiligen Zusammenwirken mehrerer Verantwortlicher nur noch wenige Konstellationen denkbar, in denen nicht zumindest wegen einzelner ‚Phasen‘ der Verarbeitung […] von einer gemeinsamen Entscheidung über Zwecke und Mittel der Verarbeitung auszugehen sein wird.“

nen und teilweise auch zu einem Umdenken geführt hat und noch führen wird, insbesondere bei vermeintlichen Auftragsverarbeitern, die in Wahrheit schon immer faktisch als Verantwortliche einzustufen gewesen wären.[867] Diese Fälle sind gewissermaßen unechte Übertragungen der geschärften Kriterien aus den EuGH-Urteilen.

Daneben kommen speziell im Bereich des Internets Szenarien in Betracht, in denen Akteure ihre Beiträge bisher als überhaupt nicht datenverarbeitungsrelevant eingestuft haben und nun gezwungen sind, dies neu zu beurteilen. Die naheliegendsten Fälle, die auch von Generalanwalt *Bot* in seinem obigen Zitat explizit angesprochen wurden, betreffen die Ausweitung auf sämtliche sozialen Netzwerke, über den Einzelfall Facebook hinaus. So erlaubt bspw. auch Twitter die Bereitstellung von Besucheranalysen mittels seiner Audience Insights, ähnlich den Statistiken, die Facebook für Betreiber von Fanpages bereithält. Anders als bei Facebook bedarf es dafür nicht einmal einer eigens eingerichteten Fanpage, es werden bereits die Interaktionen mit den einzelnen Tweets analysiert. Auch sog. *social plugins* wie der von Facebook bereitgestellte Like-Button zum Einbinden auf Websites werden von nahezu allen sozialen Netzwerken angeboten.[868] Hier ist mit den oben analysierten Tatbestandsmerkmalen zu erwarten, dass diese in gleicher Weise auch bei anderen Netzwerkbetreibern vorliegen.[869] Umstritten bleibt aber, welche Art von Nutzern ihrerseits die nötigen Beiträge leisten. Die Hauptsorge hier betrifft Privatnutzer, denen im schlimmsten Fall allein aufgrund des Betriebs bspw. eines Twitter-Accounts die Verantwortlichkeit gemeinsam mit Twitter und damit ggf. die Haftung für deren etwaige Datenschutzverstöße drohen könnte: „At this rate, everyone will be a [joint] controller of personal data!“[870] Die in Art. 2 Abs. 2 lit. c DSGVO verankerte Haushaltsausnahme, die rein persönliche Verarbeitungen aus dem Anwendungsbereich der Verordnung herausnimmt, wird in diesen Fällen mit Blick

---

867 So wurde auch bis zur Wirtschaftsakademie-Entscheidung des EuGH verbreitet davon ausgegangen (und von Facebook selbst propagiert), Facebook könne im Verhältnis zu Fanpage-Betreibern als bloßer Auftragsverarbeiter agieren. Siehe hierzu *Marosi*, Fanpages vor dem EuGH – Keiner will's gewesen sein; zur schwierigen Abgrenzung zwischen den beiden Rollen siehe *Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 26 DSGVO Rn. 4–7.

868 Beispielhaft sind hier etwa die unter Twitter for Websites zusammengefassten Plugins von Twitter (https://developer.twitter.com/en/docs/twitter-for-websites) oder der Youtube Subscribe Button (https://developers.google.com/youtube/subscribe) zu nennen. Beide Links zuletzt abgerufen am 14.01.2022.

869 Siehe die Ausführungen bei *Europäischer Datenschutzausschuss*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 21 f.: „[…] the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities.“ Vgl. auch *Golland*, K&R 2018, 433 (438) sowie als Beispiel für erste Fälle aus der gerichtlichen Praxis VG Wiesbaden, Beschl. v. 01.12.2021 – 6 L 738/21. WI Rn. 55 ff.

870 So der Titel des Editorials von *Millard*, IDPL 2019, 217 (217); ähnliche Sorgen bzgl. nicht-gewerblichen Akteuren äußernd *Lee/Cross*, MMR 2019, 559 (562).

auf die Lindqvist-Rechtsprechung[871] des EuGH keine Abhilfe schaffen können.[872] Blickt man zurück auf die oben erörterte Schärfung der Tatbestandsmerkmale, spitzt sich die Abgrenzung letztlich auf die Frage des gemeinsamen Zwecks bzw. der Vergleichbarkeit der jeweiligen Zwecke zu. Dass auch Privatnutzer die Verarbeitungen der ihre Profile besuchenden Freunde im gleichen Maße veranlassen, wie dies ein professioneller Fanpage-Betreiber bzgl. seiner Besucher tut, erscheint naheliegend. Entscheidend kommt es daher darauf an, ob die vom EuGH spezifizierte Mindestähnlichkeit der jeweiligen Zwecke eine irgendwie geartete Wirtschaftlichkeit in Form einer Gewinnerzielungsabsicht oder eines generell auf finanziellen Gewinn ausgelegten Profilbetriebs voraussetzt.[873] In den beiden entschiedenen Fällen war dies unproblematisch der Fall, nutzten sowohl die Wirtschaftsakademie als auch Fashion ID als private Unternehmen die Angebote von Facebook doch unstrittig geschäftsmäßig. Auch der EuGH selbst betonte in seinem Fashion ID-Urteil die Kongruenz der jeweiligen Zwecke gerade aufgrund der jeweiligen *wirtschaftlichen* Interessen,[874] sodass es im Ergebnis überzeugend scheint, hier eine irgendwie geartete Einschränkung anzunehmen.[875] Demnach wäre grundsätzlich nicht jeder Nutzer eines sozialen Netzwerks automatisch auch gemeinsamer Verantwortlicher für die Verarbeitung der Daten, die bei Interaktionen mit seinem Profil oder seinen Beiträgen vorgenommen werden. Wie genau eine Abgrenzung im konkreten Fall aussehen könnte, ist damit jedoch noch nicht geklärt, die Ungewissheit also alles andere als aus der Welt geschafft. Nach welchen Kriterien sollte die Wirtschaftlichkeit zu beurteilen sein? Wären Vereine und gemeinnützige Einrichtungen als Verantwortliche erfasst oder nicht? Wie sähe es mit privaten Nutzern aus, die gelegentlich Werbung für ihren Betrieb oder ihr Unternehmen auf ihren Profilen teilen? Sollte man sich hierfür an in anderen Rechtsbereichen entwickelten Kriterien, etwa denen zur Unternehmereigenschaft von Ebay-Verkäufern, orientieren? Letztlich führen diese Überlegungen wieder zum Kern der oben beschriebenen Problematik: Wie weit soll die Inpflichtnahme und etwaige Haftung einzelner Nutzer gehen, um damit das eigentliche Ziel der Durchsetzung des Datenschutzes gegenüber den von diesen genutzten Plattformen durchzusetzen? Eine einfache Lösung dafür scheint es auch hier nicht zu geben.

---

[871] EuGH, Rs. C-101/01 (Lindqvist), ECLI:EU:C:2003:596, wonach eine Verarbeitung zu rein persönlichen Zwecken beim Verbreiten von Daten im Internet an eine potenziell unbegrenzte Anzahl an Personen prinzipiell nicht angenommen werden kann.

[872] So auch *Marosi*, in: Maute/Mackenrodt, Recht als Infrastruktur für Innovation, S. 245 (256 f.).

[873] Auch der EDSA klärt diese Frage nicht, sondern betont einzig, dass gemeinsame kommerzielle Interessen alleine nicht ausreichen, um eine gemeinsame Verantwortlichkeit zu begründen, vgl. *Europäischer Datenschutzausschuss*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 22.

[874] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 80.

[875] So auch *Golland*, K&R 2019, 533 (535).

Weiter stellt sich die Frage, inwieweit sich die Feststellungen aus dem Urteil auch auf Akteurskonstellationen außerhalb sozialer Netzwerke erstrecken, in denen die grundlegende Fallgestaltung sich dennoch ähnlich bis nahezu identisch darstellt. *Bot* erwähnt diesbezüglich selbst Fälle der Einbindung weiterer Plugins oder, noch genereller, jeglicher Drittinhalte in das eigene Angebot.[876] Besonders relevant und interessant gestalten sich hier die Überlegungen hinsichtlich der von Akteurspluralität gekennzeichneten Fällen, die im vorigen Kapitel ausführlich behandelt wurden.[877] „Die Zuordnungsverwirrung datenschutzrechtlicher Handlungen ist Plattformen des Web 2.0 immanent […].“[878]

Hier scheint nach hiesigem Verständnis der EuGH-Kriterien zunächst einleuchtend, dass eine Übertragung auf die Kategorie von Fällen, in denen Plattformbetreiber abseits der Plattform durch Mithilfe von Einzelakteuren Daten verarbeiten,[879] konsequent und logisch wäre. Jedenfalls überall dort, wo etwa aus wirtschaftlichem Interesse fremder Code in die eigene App bzw. das eigene Angebot einbezogen und dabei dem Urheber des Codes wissentlich die Möglichkeit zur Verarbeitung der jeweiligen Nutzerdaten ermöglicht wird, lassen die Feststellungen des EuGH kein anderes Ergebnis zu.[880] Konsequenterweise müsste dies zudem auch für den Einbezog von Einzelakteuren gelten, die nicht im engeren Sinne als Plattform klassifiziert werden können. Der weiten Linie des EuGH folgend müssten dabei unter den Begriff des wirtschaftlichen Interesses nicht nur die offensichtlichen Fälle der direkten Monetarisierung (untechnisch gesprochen: Daten gegen Geld), sondern auch diejenigen, in denen der Funktionsumfang oder der Nutzungskomfort, und damit letztlich der Gesamtwert, des Dienstes gesteigert wird oder anderweitig vom Einbezug profitiert wird, subsumiert werden. Erfasst wären daher beispielsweise auch die im vorigen Kapitel beschriebenen sog. *social login*- oder *single sign-on*-Funktionen, mittels derer Nutzer ihren bestehenden Account bei Facebook, Google oder anderen großen Plattformen nutzen können, um sich bei anderen Diensten auf Websites oder in Apps anzumelden.

Weniger klar gestaltet sich die Frage bei der zweiten Kategorie von Fällen, in denen Nutzerdaten auf Plattformen, aber von Einzelakteuren und ggf. Drittparteien auf Plattformen verarbeitet werden. Hier käme eine Verantwortlichkeit auch der Plattformbetreiber für diese Datenverarbeitungen mit dem neuen Verständnis der Tatbestandsmerkmale zumindest in Betracht. Indem diese bestimmte Dienste auf ihre Plattform aufnehmen und die technische Infrastruktur gestalten und bereitstellen, die gleichermaßen Grundlage und Limitierungen

---

876 Siehe *supra* bei Kapitel 1 A.
877 Siehe *supra* bei Kapitel 1 A.
878 *Golland*, K&R 2018, 433 (437).
879 Siehe *supra* bei Kapitel 1 A. II.
880 In diese Richtung auch *Europäischer Datenschutzausschuss*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 21.

der Verarbeitungsmöglichkeiten festlegen, ermöglichen sie letztlich die vorgenommenen Verarbeitungen sowohl der Dienste selbst als auch der in diese einbezogenen Drittparteien. Hier wird die oben bereits erwähnte Frage der Kausalitätseingrenzung wieder besonders virulent: Genügt diese, im Vergleich zu den Urteilsfällen weitaus mittelbarere, Kausalitätskette der Ermöglichung noch aus, um einen ausreichenden Mittelbeitrag anzunehmen? Wie absehbar müssen die konkreten Verarbeitungen sein, um das erforderliche Wissenselement zu erfüllen? Auch auf Ebene des Zweckelements ist die Konnexität zwischen den beiden Zwecken geringer als in den EuGH-Fällen. Einerseits profitiert der Plattformbetreiber insofern von der Existenz möglichst vieler Apps und Dienste auf seiner Plattform, als ein lebhaftes Ökosystem mit vielen Anbietern einen großen Attraktivitätsaspekt ausmacht und somit Nutzer anzieht. Andererseits ist dieser Vorteil nicht das unmittelbare Äquivalent (oder: Synallagma) zu den Datenverarbeitungen der jeweiligen Anbieter, denn deren Profit liegt in erster Linie in der eigenen Existenz auf der Plattform und damit in der Auffindbarkeit und Präsenz gegenüber potenziellen Nutzern, während die Möglichkeit zur Datenverarbeitung erst auf sekundärer Ebene zu betrachten ist. Nichtsdestotrotz stellt die Möglichkeit der Verarbeitung von Nutzerdaten, insbesondere im Zusammenhang mit personalisierter Werbung, für viele Dienste ein gewichtiges, wenn nicht gar das einzige Geschäftsmodell dar.[881] Es wäre daher nicht gänzlich fernliegend, hier letztlich doch eine hinreichende Konnexität der jeweils gewährten Vorteile und damit auch eine hinreichende Kongruenz und Verarbeitungsbezogenheit der jeweiligen Zwecke anzunehmen. Ein abschließendes Urteil soll hier außen vor bleiben, es kann aber festgehalten werden, dass es gute Argumente für und gegen eine Anwendung auf diese Szenarien gibt. Eine ausführlichere Betrachtung mitsamt dem Blick auf die zu erwartende Wirksamkeit einer Anwendung soll im nächsten Kapitel folgen.

(3) Das Ausmaß der Verantwortlichkeit

Das eben Geschilderte ist eng verknüpft mit der abschließend zu betrachtenden Konsequenz aus den Urteilen: Wie sich die Ausweitung auf andere und insbesondere neue Szenarien in der Praxis auswirkt und welche regulatorische Wirkung sie zeitigt, hängt in großem Maße davon ab, welches Ausmaß die gemeinsame Verantwortlichkeit für die betroffenen Akteure im Detail erreicht. Von dieser Frage erfasst ist zunächst die Verteilung der einzelnen Pflichten, sodann auch deren Reichweite und das Ausmaß der Haftung bei Verstoß gegen diese. Unmittelbar zusammen hängt dieser Aspekt auch mit dem oben unter (1) geschilderten Versuch des EuGH, die Belastung für die Neupflichtigen nicht aus

[881] Siehe die Studie von *Libert/Nielsen*, Third-Party Web Content on EU News Sites: Potential Challenges and Paths to Privacy Improvement, nach der insbesondere für viele Nachrichtenwebsites das Einkommen durch Drittparteien einen essenziellen Anteil ausmacht.

dem Ruder laufen zu lassen. Kann demnach der Versuch des EuGH, mit dem Fashion ID-Urteil die Reichweite der Verantwortlichkeit selbst durch Rückgriff auf Verarbeitungsphasen und die Limitierung jene Phasen, auf die der jeweilige Akteur tatsächlich Einfluss hat, zu begrenzen,[882] angesehen werden, so bilden die Verteilung und Reichweite der einzelnen Pflichten einerseits und der Haftung für ihre Missachtung andererseits zwei zusätzliche und feingliedrigere Ebenen der Belastungssteuerung. Sie klingen vorsichtig ebenfalls in den Urteilen des EuGH an, wenn dieser, wie vor ihm auch schon die *Art. 29-Datenschutzgruppe*, den *Grad* der Verantwortlichkeit betont, der zwischen den gemeinsamen Verantwortlichen nicht zwingend gleichmäßig verteilt sein müsse.[883] Hinsichtlich der Frage, wie genau sich ein unterschiedlicher Grad an Verantwortlichkeit auf den beschriebenen beiden zusätzlichen Ebenen unterhalb der Verarbeitungsphase, an die die Verantwortlichkeit anknüpft, auswirkt, herrscht auch nach den EuGH-Urteilen größtenteils Ungewissheit.[884]

Blickt man auf die Ebene der Pflichten*verteilung*, ließe sich zunächst andenken, der jeweilige Grad an Verantwortlichkeit könne darüber bestimmen, welche Verantwortlichenpflichten einen gemeinsamen Verantwortlichen überhaupt treffen. So könnte ein nur zu geringem Grad erfasster Verantwortlicher mit bestimmten Pflichten, die seine(n) Mitverantwortlichen treffen, nicht belegt werden. In diese Richtung gehend ließe sich die Feststellung des EuGH verstehen, wonach etwa die Pflicht zur Information des Betroffenen ihn nur hinsichtlich der initialen Datenerhebung und -weitergabe (in diesem Falle an Facebook) treffe, nicht aber hinsichtlich der nachfolgenden Verarbeitungen durch den (oder die) weiteren Verantwortlichen.[885] Bei näherem Hinsehen zeigt sich aber, dass der EuGH hier schlicht die geschilderte Limitierung auf Verarbeitungsphasen konsequent anwendet. Ist also der Websitebetreiber in diesem Fall nur für die Phasen der Erhebung und Weitergabe, nicht aber für die nachfolgenden Verarbeitungen durch Facebook verantwortlich, so erscheint logisch, dass auch seine Informationspflicht sich allein auf diese Phasen erstreckt. Diese Annexwirkung der Limitierung der Verantwortlichkeit als Ganze sollte aber von der Limitierung der Pflichtenverteilung im Einzelnen klar getrennt werden. Fraglich ist somit konkret, ob auch im Rahmen der Verarbeitungsphasen,

---

882 Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 74 ff.

883 Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 39; siehe außerdem EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 70 mit Verweis auf Rs. C-25/17 (Jehovan todistjajat), ECLI:EU:C:2018:551 Rn. 66 und Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), E-CLI:EU:C:2018:388 Rn. 43.

884 Auch die im Nachgang der beiden Urteile erlassenen Guidelines des EDSA liefern hier keine neuen Erkenntnisse, sondern erschöpfen sich in Wiederholungen, vgl. *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 20, 48.

885 Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 101.

auf die sich die Verantwortlichkeit aller beteiligten gemeinsamen Verantwortlichen erstreckt, eine punktuelle Verteilung möglich ist. Hierzu lassen sich dem EuGH keine klaren Erläuterungen entnehmen. Auch der Wortlaut der DSGVO ist uneindeutig. Art. 26, der die Rechtsfolgen – und nicht etwa, wie teilweise fälschlich verstanden, die Voraussetzungen[886] – der gemeinsamen Verantwortlichkeit normiert, erlaubt den Verantwortlichen einerseits in seinem Abs. 1 S. 2 nicht nur, sondern verpflichtet sie gar dazu, die Pflichten der Verordnung untereinander aufzuteilen und diese Aufteilung vertraglich festzuhalten. Gleichzeitig schränkt Abs. 2 S. 1 ein, dass solche Verteilungen nur wirksam sind, solange sie die „jeweiligen tatsächlichen Funktionen und Beziehungen […] gegenüber betroffenen Personen gebührend widerspiegeln" und statuiert Abs. 3, dass unabhängig von der vereinbarten Verteilung Betroffene ihre Rechte prinzipiell bei und gegenüber jedem Verantwortlichen geltend machen können.[887] Insbesondere letzteres deutet stark darauf hin, dass eine über die Verarbeitungsphasenlimitierung hinausgehende einflussabhängige Allokation von Pflichten, jedenfalls im Außenverhältnis gegenüber den Betroffenen, in der DSGVO nicht vorgesehen ist. Zwar ließe sich gegen ein solches Verständnis wiederum der Aussagegehalt der Einschränkung in Art. 26 Abs. 2 S. 1 DSGVO ins Feld führen: Legt die DSGVO explizit Wert darauf, dass die Pflichtenverteilung die Lebenswirklichkeit widerspiegelt, so könnte dies möglicherweise nicht nur für die gewillkürte, sondern auch für die gesetzliche Verteilung gelten. Ein solcher Umkehrschluss wäre aber ohne weitere Grundlage im Wortlaut zu weitgehend. Zudem verbliebe auch dann die Tatsache, dass mit Abs. 3 der Norm ein Durchschlagen der internen Verteilung gegenüber den Betroffenen keine Geltung entfaltet. Möglich erschiene letztlich mit Blick auf die Schutzwirkung von Art. 26 Abs. 3 DSGVO für den Betroffenen einzig die Überlegung, zumindest im Verhältnis zwischen Verantwortlichen und Behörden eine selektive Pflichtenlast der Verantwortlichen anzunehmen. Auch dagegen sprechen aber gewichtige Argumente: Wie oben dargelegt wurde, kommt den Behörden im Regelungskonzept der DSGVO und im Rahmen ihrer Aufgabe zur Durchsetzung der Verordnung auch die Rolle zu, die Betroffenen bei der Rechtsdurchsetzung zu unterstützen.[888] Der Schutzgedanke der genannten Norm würde daher unterlaufen, erlaubte man eine solche Selektierung der Pflichten. Zudem erscheint eine Trennung der beiden Ebenen in der Praxis mit Blick darauf, dass viele Pflichten gleichermaßen von Betroffenen und Aufsichtsbehörden kontrolliert

---

[886] So verstanden etwa von *Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 26 DSGVO Rn. 1; ebenso *Voigt*, CR 2017, 428 (431); *Kartheuser/Nabulsi*, MMR 2018, 717 (718) stellen auf Art. 4 Nr. 7 i. V. m. Art. 26 Abs. 1 DSGVO ab.

[887] Vgl. *Spoerr*, in: BeckOK Datenschutzrecht, Art. 26 DSGVO Rn. 37; *Martini*, in: Paal/Pauly, DSGVO/BDSG, Art. 26 DSGVO Rn. 36; *Mahieu* u. a., jipitec 2019, 85 (98).

[888] Siehe die Ausführungen *supra* bei B. I. 1. a) sowie die explizite Aufgabenzuweisung in Art. 57 Abs. 1 lit. b, e und f.

und bzgl. ihrer Verletzung angemahnt werden können, sehr schwierig umzusetzen.

Es bleibt damit dabei, dass auch bei unterschiedlichen Graden an Verantwortlichkeiten zwischen gemeinsam Verantwortlichen grundsätzlich alle Verantwortlichen jeglichen Pflichten der DSGVO unterworfen sind.[889] Zwar können im Rahmen der Pflicht zur Verteilung der Pflichten untereinander auch exklusive Zuordnungen vereinbart und somit einzelne Verantwortliche privatautonom von bestimmten Pflichten freigestellt werden. Doch wirkt sich dies nur im Innenverhältnis der gemeinsamen Verantwortlichen aus, nicht aber im Außenverhältnis gegenüber Betroffenen und, grundsätzlich, auch den Aufsichtsbehörden.[890] Als Konsequenz daraus haftet ein Verantwortlicher deshalb im Außenverhältnis auch gesamtschuldnerisch mit, wenn eine Pflicht verletzt wird, die qua Vereinbarung ein anderer Mitverantwortlicher hätte erfüllen müssen, wie Art. 82 Abs. 4 DSGVO für zivilrechtliche Schadensersatzansprüche klarstellt. Nur unter hohen Voraussetzungen kommt gem. Art. 82 Abs. 3 DSGVO eine anspruchsausschließende Exkulpation in Betracht. Eine darüber hinausgehende abmildernde Wirkung kann hier höchstens daraus gezogen werden, dass bei verteilungswidriger Inanspruchnahme und ggf. Haftung eines Verantwortlichen dieser im Innenverhältnis gem. Art. 82 Abs. 5 DSGVO Regress beim eigentlich pflichtigen Mitverantwortlichen nehmen kann. Das Risiko der Erreichbarkeit und Durchsetzbarkeit des Regressanspruchs sowie einer etwaigen Insolvenz des Mitverantwortlichen bleibt dabei freilich ihm aufgebürdet. Auch hinsichtlich Behördenmaßnahmen ist davon auszugehen, dass grundsätzlich jeder der Verantwortlichen adressiert werden kann.[891]

Einen wirksameren Beitrag zur Belastungssteuerung könnte daher die Ebene der Pflichtenreichweite mit sich bringen. Wie bereits erörtert sind zahlreiche DSGVO-Pflichten hinsichtlich ihrer Reichweite stark kontext- und risikoabhängig, geben also nicht ohne weiteres klare Vorgaben für ihre Erfüllung. Stattdessen werden die zu ihrer Erfüllung zu ergreifenden Maßnahmen in Abhängigkeit von beispielsweise den Umständen und Zwecken der jeweiligen Verarbeitung sowie der jeweiligen Eintrittswahrscheinlichkeit und Schwere der Risiken für

---

[889] So im Ergebnis auch das Fazit des EDSA, der festhält, dass auch Aufsichtsbehörden nicht an die interne Pflichtenverteilung der Verantwortlichen gebunden sind und Maßnahmen gegen jeden von ihnen ausüben können, vgl. *Europäischer Datenschutzausschuss*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 48.

[890] Ob diese eine Anordnung wegen Verletzung einer DSGVO-Pflicht auch ermessensfehlerfrei an einen Verantwortlichen richten könnten, der nach interner Verteilung ersichtlich nicht für diese Pflicht zuständig war, steht auf einem anderen Blatt und hängt – mit Blick auf das Gebot der effektiven und wirkungsvollen Gefahrenabwehr, vgl. BVerwG, Urt. v. 11.09.2019, Az. 6 C 15.18 (Wirtschaftsakademie Schleswig-Holstein) Rn. 31 – von den Umständen im Einzelfall, insbesondere von der jeweiligen Fähigkeit zum Abstellen des Verstoßes, ab.

[891] Vgl. *Hartung*, in: Kühling/Buchner, DSGVO/BDSG, Art. 26 DSGVO Rn. 31; *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 48.

Betroffene gesetzt.[892] Hier erscheint denkbar, in die jeweilige Abwägung zur Bestimmung der Pflichtenreichweite auch die Verteilung der faktischen Einflussmöglichkeiten der jeweiligen Parteien einfließen zu lassen und so bei den verschiedenen Parteien zu unterschiedlichen Ergebnissen zu kommen. Letztlich führt aber auch das wieder in die oben beschriebene Sackgasse: Soll, entsprechend dem Schutzzweck von Art. 26 Abs. 3 DSGVO, der Betroffene bei Ausübung seiner Rechte nicht unter der internen Verteilung der Pflichten zwischen den verschiedenen Verantwortlichen leiden müssen, so gilt dies erst recht hinsichtlich etwaiger Abweichungen bei der Reichweite der Pflichten; ein Verantwortlicher A, der möglicherweise nur bestimmte Daten, auf die er selbst Zugriff hat, eigenhändig löschen kann, weshalb die Pflicht des Art. 17 DSGVO intern größtenteils dem Verantwortlichen B übertragen wurde, kann dies nach außen hin dem Betroffenen nicht entgegenhalten, sondern muss seinen Teil dazu beitragen, auch B zur Löschung der restlichen Daten zu bewegen[893] und kann, wenn ihm dies nicht gelingt, haftbar gemacht werden. Einzig im Verhältnis gegenüber den Aufsichtsbehörden kommt daher eine Bedeutung unterschiedlicher Pflichtenreichweiten noch in Betracht. Hier ließe sich andenken, im Rahmen der Prüfung der Voraussetzung einer Maßnahme zu differenzieren. Die oben angesprochene Problematik der schwierigen Trennung zwischen der Rechtsdurchsetzung durch Betroffene einerseits und Aufsichtsbehörden andererseits, die sich auf ein und dieselbe Pflicht beziehen können, bleibt jedoch bestehen. Zudem haben die EuGH-Urteile gezeigt, dass es jedenfalls in Fällen großflächiger Datenschutzwidrigkeit ggf. müßig sein kann, der Möglichkeit der leichteren Erfüllung einzelner Pflichten durch Mitverantwortliche geringeren Grades zu viel Bedeutung beizumessen: So wie im Falle der Wirtschaftsakademie die Möglichkeit der gänzlichen Abschaltung der infragestehenden Fanpage in den Mittelpunkt gestellt wurde, ließe sich auch in anderen Szenarien letztlich immer auf diese *ultima ratio*-Maßnahme verweisen. Wer also einen erkennbar datenschutzrechtlichen Dienst nutzt und diesem dadurch die Verarbeitung von Daten ermöglicht, hat im schlimmsten Fall bereits durch die reine Nutzung gegen datenschutzrechtliche Pflichten verstoßen, sodass es auf die möglicherweise dennoch erfüllten einzelnen Pflichten auf der Mikroebene dann nicht mehr ankommt.

III. Zwischenergebnis

Die bereits im Laufe der Zeit seit Erlass der DSRL im Jahre 1995 infolge zunehmend komplexer werdender Verarbeitungsumstände und Konstellationen be-

[892] So etwa Art. 24 Abs. 1 S. 1 und 32 Abs. 1 DSGVO bzgl. technisch-organisatorischen Maßnahmen zur generellen DSGVO-Konformität bzw. Maßnahmen der Datensicherheit.

[893] Vgl. zu dieser impliziten Einwirkungspflicht *Martini*, in: Paal/Pauly, DSGVO/BDSG, Art. 26 DSGVO Rn. 36.

teiligter Akteure ebenso zunehmend schwieriger werdende Zuordnung datenschutzrechtlicher Verantwortlichkeit auf Basis der schon Jahre vor der DSRL in der jetzigen Form existenten Kriterien der Zweck- und Mittelfestlegung hat durch die beiden EuGH-Urteile Wirtschaftsakademie und Fashion ID eine Zäsur erfahren, deren Auswirkungen nicht abschließend eingeschätzt werden können. Klar ist, dass sie eine nicht unerhebliche Ausweitung der Verantwortlichkeit zur Folge hat, und klar scheint bis dato, dass mit dieser gleichzeitig eine Konkretisierung und Verwässerung der Tatbestandsmerkmale einherging. Gerade für den digitalen Raum ist nun klarer, in welchen Konstellationen eine – einfache oder gemeinsame – Verantwortlichkeit von Akteuren in Betracht kommt und von welchen Umständen dies in erster Linie abhängt.[894] Gleichzeitig fehlt es an eindeutig definierten oder interpretierbaren Grenzen, sodass nun zwar geklärt ist, welche bisher unscheinbar daherkommenden Fälle und Akteure tatsächlich eine Verantwortlichkeit auslösen respektive tragen müssen. Dafür bleibt ungewiss, bis genau wohin diese Öffnung reicht. Damit zusammenhängend besteht Unklarheit über die Konsequenzen und Wirkweisen – sowohl beabsichtigt als auch unbeabsichtigt – mit Blick auf das Datenschutzniveau einerseits und die Befürchtung überbordender Inanspruchnahme Mitverantwortlicher geringen Einflusses andererseits.[895] Betrachtet man die Ausweitung der Verantwortlichkeit im Kontext des generellen Regelungskonzepts der datenschutzrechtlichen Verantwortlichkeit, zeigt sich eine leichte Verschiebung des Primärzwecks: Wo es klassischerweise darum geht, durch Regulierung des eigenen Umgangs mit Datenverarbeitungstechniken die aus der Nutzung der Techniken resultierenden Risiken einzudämmen, wird nun das Verhalten von Akteuren (mit)reguliert, die mit ihrem regulierten Verhalten Einfluss auf das, ebenfalls regulierte, Verhalten und insbesondere die Verarbeitungstätigkeiten anderer Akteure nehmen sollen. In dieser Verschiebung zeigt sich der Versuch, die Schwierigkeiten bei der Durchsetzung des Datenschutzes unmittelbar gegen große, marktmächtige Akteure zu kompensieren. Die beschriebenen Unklarheiten und möglichen Nebeneffekte zeigen, dass diese Herangehensweise ihrerseits neue Defizite mit sich bringt.

D. Ergebnis

In diesem Kapitel wurde ein weiter Bogen geschlagen, um, ausgehend von der grundlegenden Frage des datenschutzrechtlichen Schutzguts und Regelungszwecks (A.), die Verantwortlichkeit in ihrer Funktion als Herzstück des über-

894 Vgl. *Lee/Cross*, MMR 2019, 559 (561).

895 Vgl. *Mahieu* u. a., jipitec 2019, 85 (97) zur Fanpage-Entscheidung des EuGH: „[…] that the existing frameworks for assigning responsibilities are inconclusive with respect to the question of how far the responsibility of the fan page administrator reaches."

geordneten Regelungskonzepts zu erklären und in ihre Bestandteile zu zerlegen (B.). Die dabei erreichte Aufgliederung in die Grundprämissen, von denen die Effektivität des Gesamtkonzepts abhängt (B. II.), bildet den Grundstein für den im nächsten Kapitel folgenden Abgleich mit der heutigen Verarbeitungsrealität am Beispiel der in Kapitel 1 portraitierten Beispielsfälle komplexer Verarbeitungsszenarien im Lichte zunehmender Akteurspluralität. Die ebenfalls aufgezeigten, insgesamt kaum verdichteten, verfassungsrechtlichen Vorgaben (A. III.) bilden im Lichte ihrer Ausprägung als andauernde Beobachtungs- und Nachbesserungspflichten den Legitimationsrahmen für diesen Abgleich und die aus ihm folgenden Vorschläge für eine vorsichtige Weiterentwicklung der Verantwortlichkeit. Ebenfalls in diesem Kapitel aufgezeigt und analysiert wurde der vom EuGH bereits eingeschlagene Weg einer Öffnung und Weiterentwicklung der Verantwortlichkeit (C. II.). An diesem und seinen bereits in Anklängen aufgezeigten Limitierungen soll sich der im nächsten Kapitel zu entwickelnde Ansatz einer eigenständigen Weiterentwicklung orientieren.

Kapitel 3

Die klassischen Akteursrollen in Zeiten der Akteurspluralität – Weiterentwicklung oder Kontinuität?

„While this might appear a consequent policy option, in line with what has been known in the data protection field for the past decades, it is likely not to be compatible with the contemporary processing reality."[1]

Mit den vorangegangen Kapiteln wurden bereits mehrere zentrale Erkenntnisse erlangt: Einerseits, dass die heutige Verarbeitungsrealität im Bereich digitaler Dienste (nicht nur) hinsichtlich der beteiligten Akteure weitaus komplexer, verteilter und vielschichtiger ist, als zum Zeitpunkt der erstmaligen europarechtlichen Normierung des mit der DSGVO nach wie vor geltenden Verantwortlichkeitskonzepts und seiner Zuordnungsvoraussetzungen.[2] Zum anderen, dass das Regelungskonzept der DSGVO eine vielschichtige Melange unterschiedlicher interdependenter Regelungsinstrumente ist, deren Herzstück die datenschutzrechtliche Verantwortlichkeit darstellt. Diese lebt – teils implizit, teils explizit – von bestimmten, die Rolle des Verantwortlichen betreffenden, Prämissen.

In diesem Kapitel soll daher zunächst abgeglichen werden, was die veränderte Verarbeitungsrealität für die Verantwortlichkeit und ihre Prämissen bedeutet, und aufgezeigt werden, dass die zentralen Prämissen zu großen Teilen nicht mehr gegeben sind (A.). Im nächsten Schritt soll dann – aufbauend auf den bereits beleuchteten Entwicklungen durch die EuGH-Urteile zur gemeinsamen Verantwortlichkeit – gezeigt werden, dass eine gezielte Öffnung der Verantwortlichkeit und damit eine Modifizierung der *Auswahl* sowie in Teilen auch der *Ausgestaltung* des Verantwortlichen und seiner Pflichten nötig und legitimierbar ist, um der modernen Verarbeitungsrealität Rechnung zu tragen und den aus ihr resultierenden Gefahren entgegenzuwirken (B.). Dabei kommen unterschiedliche Ansätze in Betracht und können verschiedene Modelle extensiver Verantwortlichkeitszuschreibung aus anderen, aber hinsichtlich der geregelten Konstellationen vergleichbaren Rechtsregimen zum Vorbild genommen

---

[1] *de Hert/Papakonstantinou*, CLSR 2016, 179 (184) zur Beibehaltung der althergebrachten Akteursrollen im Übergang von DSRL zu DSGVO.

[2] Vgl. auch hier *de Hert/Papakonstantinou*, CLSR 2016, 179 (184): „The idea of a single data controller that will carry all liability under data protection law while all other parties to the same processing carry less or no responsibility at all is outdated and lacks an understanding of where technology and lifestyles are headed."

werden (C. und D.). Hier gilt es insbesondere, den in Kapitel 2 aufgezeigten Kontrollverlust vieler Akteure in Verbindung mit der besonderen Kontrollstellung digitaler Plattformen zu berücksichtigen. Dabei ist diese Kontrollstellung insbesondere im Lichte ihrer spezifisch technischen Besonderheiten, aber auch Limitierungen zu betrachten.

A. Dysfunktionalität durch organisierte Verantwortungslosigkeit

„The Directive's assumed power of the data controller will therefore in practice be ‚carved out', to a greater or lesser extent, by the power of (or choices made by) other entities with whom it interacts, even though the legal obligations for compliance will (at least in principle) remain with the data controller."[3]

Das europäische Datenschutzrecht mit seiner sekundärrechtlichen Verkörperung in der DSRL fand seinen Ursprung Mitte der 1990er Jahre, zu einer Zeit, die in Retrospektive als ein gänzlich anderes digitales Zeitalter betrachtet werden kann. Nicht nur das Internet, auch die Alltäglichkeit computergestützter Handlungen steckte noch in ihren Kinderschuhen. Kritik, wonach der gewählte Ansatz des Datenschutzrechts ob der stetigen technischen, aber auch gesellschaftlichen Weiterentwicklung bzgl. der digitalen Lebenswelt veraltet sein könnte, traf daher schon die, zwischenzeitlich zwar oberflächlich modernisierte, DSRL[4] ebenso wie die Anstrengungen des deutschen Gesetzgebers dort, wo ihm noch Spielräume verblieben[5]. Die mit der DSGVO angestrebte Modernisierung wurde in Teilen wahr und wohlwollend aufgenommen, zog aber auch Kritik von unterschiedlichen Seiten und aus unterschiedlichen Gründen auf sich.[6] Wie auch immer man zu den mit der Einführung der DSGVO erfolgten Veränderungen steht, eine Sache ist klar: Die *Zuordnung* der Verantwortlichkeit hat sich, jedenfalls gesetzgeberisch und normtextlich, nicht verändert,[7] und bleibt dem Grunde nach ihrem klassisch linearen Vorstellungsmodell einer Verarbeitung mit einem Betroffenen und einem Verantwortlichen treu.[8] Die im vo-

[3] *Van Alsenoy*, CLSR 2012, 25 (36).

[4] Vgl. *Robinson*, MMR 2009, 725; *de Hert/Papakonstantinou*, CLSR 2016, 179; *Tene*, Ohio State Law Journal 2013, 1217.

[5] Vgl. *Marosi*, K&R 2016, 389 (392): „Innovative Rechtsfortbildung, wie man sie noch mit dem TMG bzw. TDDSG gesehen hat und die ein Vorbild für europäische Gesetzgebung sein kann, findet schon länger nicht mehr statt."

[6] Stellvertretend für die kritischen Stimmen aus der deutschen Literatur kann hier *Veil*, NVwZ 2018, 686 (686 ff.) genannt werden. Aus dem internationalen Raum siehe etwa *Zarsky*, Seton Hall L. Rev. 2017, 995 (995 ff.).

[7] Siehe etwa *European Data Protection Board*, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, S. 9: „A general observation regarding the concepts of controller and processor in the GDPR is that they have not changed compared to the Directive 95/46/EC and that overall, the criteria for how to attribute the different roles remain the same."

[8] Vgl. *Tene*, Ohio State Law Journal 2013, 1217 (1219): „[…] [it] remains rooted on a

rangegangenen Kapitel erörtere Rechtsprechungslinie des EuGH zeigt jedoch, dass hier gleichermaßen eine Achillesferse wie auch eine taugliche Stellschraube des modernen Datenschutzrechts liegen kann.

Dieser Abschnitt konzentriert sich auf die mögliche Achillesfersen-Eigenschaft des klassischen Verarbeitungsmodells. Mittels der bereits identifizierten Grundprämissen, von denen die Wirksamkeit des Verantwortlichkeitskonzepts (unter anderem) abhängt, werden die Auswirkungen einer zunehmend komplexen und verteilten Datenverarbeitungsrealität untersucht. Damit wird gezeigt werden, wie sich die Tatsache, dass an alltäglichen Datenverarbeitungen im digitalen Raum häufig eine Vielzahl an Akteuren mit häufig ganz unterschiedlichen, aber regelmäßig jeweils begrenzten Ausmaßen beteiligt sind, auf die Erwartungen auswirkt, die das Datenschutzrecht an die Rolle des Verantwortlichen stellt. Zu diesem Zweck sollen zunächst die einzelnen Prämissen mit der Akteurspluralität und ihren Auswirkungen abgeglichen werden. Können die Prämissen unter den festgestellten Realweltbedingungen keine (vollständige) Geltung mehr für sich beanspruchen, so können daraus im nächsten Schritt zwei Erkenntnisse gezogen werden: Einerseits, dass hier ein Bedarf für Anpassung besteht, um die Geltung der Prämisse(n) wiederherzustellen. Andererseits findet sich, je nach Prämisse und Grund ihrer fehlenden Geltung, ein erster Anknüpfungspunkt dafür, wie eine solche Anpassung aussehen müsste, welche(n) realweltlichen Gegebenheiten also ausgeglichen oder entgegengewirkt werden muss bzw. müssen.

I. Die einzelnen Prämissen auf dem Prüfstand

1. Der Verantwortliche als zentraler, kenntnis- und einflussreicher Akteur

Wie im vorangegangenen Kapitel[9] festgestellt, kann ein Akteur nur dann die Erwartungen erfüllen, die aus einer Regelungsperspektive an seine Rolle als Verantwortlicher gestellt werden, wenn er die Verarbeitungsumstände, also den Lebensausschnitt, der seinem Verantwortungsbereich zugeordnet wird, umfassend kontrollieren und beeinflussen kann und ausreichend Wissen über alle Verarbeitungsumstände inklusive beteiligter Akteure besitzt. Dabei sind Wissen und Kontrolle in einem gewissen Rahmen wechselseitig zu betrachten und lässt die DSGVO zumindest ein Minus an Detailwissen zu, sofern dies durch ein Plus an übergeordneter Kontrolle (und, auf der nachgelagerten Ebene, durch ein Plus an Haftung, wenn die Kontrolle nicht hinreichend ausgeübt wurde) ausgeglichen wird, wie die Ausgestaltung der Figur des Auftragsverarbeiters zeigt.[10]

---

linear approach to processing whereby an active ‚data controller' collects information from a passive individual, and then stores, uses, or transfers it until its ultimate deletion."

[9] Siehe Kapitel 2 B. II. 1.

[10] Hier wird die weitreichende Delegation der Mittel, also der technischen Einzelheiten

Mit Blick auf die oben beschriebene Realität, in der die unmittelbar mit Betroffenen agierenden Diensteanbieter nur noch einen Bruchteil des „Unterbaus" ihres Dienstes eigenständig kontrollieren und beeinflussen, während zahlreiche Bestandteile des Codes eines Dienstes ebenso wie die zugrundeliegende Infrastruktur meist von anderen Akteuren stammen, die ihrerseits Datenverarbeitungen vornehmen, erscheint das Aufrechterhalten dieses Ideals zweifelhaft.

Nutzt ein Diensteanbieter beispielsweise SDKs dritter Akteure, kann er nach dieser einmaligen Entscheidung keinen unmittelbaren Einfluss mehr darauf nehmen, welche Datenverarbeitungen die involvierten Dritten mittels ihrer SDKs durchführen. Der Entscheidungsspielraum erschöpft sich in dem „Ob" eines Einbezugs, eine spätere Möglichkeit der Einflussnahme fehlt. Auch fehlt die nötige Transparenz, um (möglicherweise vertragswidrige) Verarbeitungstätigkeiten überhaupt im Detail zu erkennen und einzuordnen. Zwar können hier je nach Identität des Dritten und Grund seines Einbezugs Unterschiede vorherrschen, sind also einige Akteure transparenter als andere und kann je nach Verhandlungsposition auch vertraglich eine weitergehende Kontrolle vereinbart werden. Doch lässt sich insgesamt nicht verhindern, dass technisch betrachtet der Einbezug eines SDKs dem Einladen eines trojanischen Pferdes gleichkommt. Alles, was der Diensteanbieter verarbeitungstechnisch selbst zu tun in der Lage ist, kann auch der von ihm einbezogene Dritte tun, ohne dass der Diensteanbieter die entsprechenden Handlungen tatsächlich mitbekommt – unabhängig davon, ob das Szenario eine Website oder bspw. eine App betrifft und unabhängig davon, ob die Dritten zum Bereitstellen von Inhalten, zu Zwecken der Monetarisierung oder zum Auffinden von Fehlern und zur Analyse des Nutzerverhaltens zwecks Qualitätsverbesserung eingebunden wurden. Auf technischer Ebene erfolgt die Einbindung regelmäßig auf identische Art und Weise. Auch an einer Verhandlungslage mangelt es regelmäßig, SDKs sind typischerweise bereits vorgestaltet und weisen höchstens minimale Konfigurationsmöglichkeiten auf, die sich meist auf die vom Diensteanbieter zu beziehende Funktionalität auswirken und damit theoretisch den Umfang der verarbeiteten Daten einschränken, nicht aber die (technischen Grundlagen der) Berechtigungen des Drittanbieters tangieren.[11] Regelmäßig gilt hier ein vergleichbares *take it*

---

des „Wie" der Verarbeitung, an den Auftragsverarbeiter erlaubt. Im Gegenzug muss der Verantwortliche die hinreichende Kontrolle in Form von Informations- und Interventionsmöglichkeiten behalten. Zudem übernimmt er die Auswahlverantwortung für die Wahl eines zuverlässigen Auftragsverarbeiters. Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17 f. sowie die Ausführungen *supra* in Kapitel 2 C. II. 4. a).

[11] So wird etwa im Zusammenhang mit Google Analytics von Seiten der Aufsichtsbehörden empfohlen, die übermittelte IP-Adresse der Nutzer zu kürzen. Vgl. *Datenschutzkonferenz (DSK)*, Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, S. 6. Siehe zudem die Handlungsempfehlungen der Gesellschaft für Datenschutz und Datensicherheit (GDD, https://www.gdd.de/aktuelles/startseite/eugh-urteil-mit-starker-breitenwirkung). Zuletzt abgerufen am 14.01.2022.

or leave it-Modell wie es bereits bei den den EuGH-Urteilen Wirtschaftsakademie[12] und Fashion ID[13] zugrundeliegenden Fällen um Fanpages und Like-Buttons von Facebook beobachtet werden konnte.[14]

Das angesprochene Defizit auf Wissensebene bezieht sich nicht nur auf die Einhaltung der vertraglichen Regelungen und das Ob und die Details eines etwaigen Fehlverhaltens, sondern betrifft schon grundlegend die Frage, welche Verarbeitungsmöglichkeiten einem einbezogenen Dritten überhaupt eingeräumt werden, wie der in Kapitel 1 aufgeführte Fall des DRK Bayern eindrucksvoll zeigt.[15] Hier vermengen sich also strukturelle Kontroll- und Wissenslimitierungen auf *technischer* Ebene mit *vorgelagerten* systematischen Kontroll- und Wissenslimitierungen, die mit den verfestigten Geschäftsmodellen und Praktiken einhergehen.

Von Bedeutung sind die unterschiedlichen Zwecke jedoch für die rechtliche Einordnung. Nehmen Dritte etwa bewusst Datenverarbeitungen für Diensteanbieter vor, ohne selbst auch Daten zu eigenen Zwecken zu verarbeiten, liegt ein klassischer Fall der Auftragsverarbeitung vor. Hier ist sowohl der Wissensvorsprung als auch die Verlagerung der (technischen wie auch faktischen) Kontrolle auf den Dritten bereits eingepreist, wird also der verteilten Verarbeitungsrealität zu einem gewissen Maß bereits Rechnung getragen. Naturgemäß geht auch mit diesen Fällen immer eine gewisse Missbrauchsgefahr einher, kann also auch ein Auftragsverarbeiter ohne weiteres die ihm überlassenen Daten auch zu eigenen Zwecken weiterverarbeiten, ohne dass dies dem ihn beauftragenden Verantwortlichen auffallen muss. Hier sorgen jedoch nicht zuletzt Sorgfalts- und Überwachungspflichten hinsichtlich Auswahl und Weiterverwendung des Auftragsverarbeiters für ein gewisses Gegengewicht und zeichnen sich viele Akteure bewusst durch Zertifizierungen oder die bestätigte Einhaltung genehmigter Verhaltensregeln aus. Hinzu kommt, dass für (klassische) Auftragsverarbeiter der sorgsame Umgang mit Daten erkenn- und einsehbar ihr Geschäftsmodell darstellt.[16] Ihre Auswahl durch Auftraggeber findet in der Regel bewusst und auf Basis von Zertifikaten und anderen Garantien statt, ein etwaiger Reputati-

[12] EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388.

[13] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629.

[14] Siehe *Mahieu* u. a., jipitec 2019, 85 (105): „Many of the building blocks of digital services, such as payment services, user analytics, maps integration and many others, have the same characteristics."

[15] Hier wurde zur Steigerung der Reichweite und Auffindbarkeit ein Facebook Pixel auf der eigenen Website eingebunden, der Antworten auf die sensiblen Fragen eines Blutspende-Fragebogens an Facebook übermittelte. Siehe die Ausführungen und Quellenverweise in Kapitel 1 A.

[16] Was nicht zuletzt darauf zurückzuführen ist, dass diesbezüglich seit Jahren klare Vorgaben für Verantwortliche und Auftragsverarbeiter bestehen. Zu den Anforderungen, die die DSGVO an die Auswahl von Auftragsverarbeitern stellt, siehe *Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 28 DSGVO Rn. 22–25; *Eckhardt*, CCZ 2017, 111 (114).

onsverlust durch offengelegtes Fehlverhalten hat daher unmittelbare Auswirkungen.[17] Eine solche Offenheit herrscht bei den mit Drittanbietereinbezug verbundenen Geschäftszweigen, die eine Datenverarbeitung zu drittanbietereigenen Zwecken vorsehen, regelmäßig nicht ohne weiteres vor.[18] Zudem fehlt es überall dort, wo eine Auftragsverarbeitung mangels Begrenzung der Verarbeitungen auf die Zwecke des aufraggebenden Diensteanbieters nicht infrage kommt, an der entsprechenden rechtlichen Umrahmung, wie sie Art. 28 f. DSGVO für Auftragsverarbeiter statuiert. Einem Missbrauch (oder auch einer bewusst kollusiv datenschutzwidrigen Erhebung von Daten durch den Dritten) steht hier also weitaus weniger im Wege.

Die einbezogenen Drittanbieter selbst haben demgegenüber die volle Kontrolle über die Ausführung ihrer eigenen Datenverarbeitungen. Sie unterliegen einzig den Limitierungen, denen auch der jeweilige Diensteanbieter, in dessen Dienst sie einbezogen wurden, unterliegt. Etwaige vertragliche Limitierungen sind nur insoweit von Bedeutung, wie auch eine Gefahr der Feststellung ihrer Missachtung besteht – eine solche Gefahr ist, wie beschrieben, aufgrund der fehlenden Transparenz als eher gering einzustufen.

Welchen Limitierungen Diensteanbieter bei der eigenen Verarbeitung von Daten (und damit nachgelagert auch Drittanbieter bei ihrer Verarbeitung von Daten „durch den Dienst hindurch“) unterliegen, ergibt sich aus einem weiteren Minus der Kontrolle, das aus der regelmäßig auftretenden Nutzung einer fremden Basisinfrastruktur folgt. Wie in Kapitel 2 erläutert, werden Dienste in zunehmender Häufigkeit auf Plattformen angeboten, die unter anderem die Infrastruktur und damit die grundlegenden Parameter dessen bestimmen, was Diensteanbieter und die von ihnen einbezogenen Dritten tun können. Das umfasst unter anderem die Art und Weise, wie datenverarbeitungsrelevante Handlungen auf einer Plattform durchgeführt werden, aber auch, welche Daten(-kategorien) überhaupt und unter welchen Umständen dem Zugriff offenstehen. Durch diese Definierung von Kategorien und Zugriffskanälen, aber auch schon durch die Festlegung der Regeln für die Aufnahme auf die Plattform und ihren Distributionskanal, wird zudem eine Vorselektion der erlaubten (Weiter-)Verarbeitungszwecke vorgenommen, sodass sich die Kontrolle des Diensteanbieters auch hier nur in einem bereits eingeschränkten Handlungsraum entfalten kann. Dabei kann unterschieden werden zwischen Zugriffskanälen, die kom-

[17] Vgl. hierzu die Ausführungen bei *Selzer*, Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit, S. 38 ff.

[18] Das zeigt sich exemplarisch bereits an der Konstellation um Fanpage-Betreiber und Facebook, bei der Facebook nicht einmal die für eine wirksame Vereinbarung gem. Art. 26 DSGVO notwendigen Informationen über sein eigenes Datenverarbeitungsverhalten bereitstellt. Vgl. *Datenschutzkonferenz (DSK)*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit. Auch die in Kapitel 1 A. I. erläuterten Fallbeispiele verdeutlichen die Problematik.

plett offen und frei von Beschränkungen sind,[19] solchen, die gegenüber dem Plattformbetreiber begründungs- und genehmigungsbedürftig sind,[20] und solchen, die qua Designentscheidung des Plattformbetreibers von der Einwilligung des Nutzers abhängig gemacht werden[21]. Einen gewissen Einfluss darauf, auf welche *Kategorien* von Daten Drittanbieter potenziell Zugriff haben können, haben Diensteanbieter über die initiale Festlegung der Daten, die für ihren Dienst notwendig sind. Nichtsdestotrotz verbleibt Drittanbietern dann immer noch ein nicht unerheblicher Spielraum für die Erhebung dieser insofern prädeterminierten Datenkategorien zu anderen als den festgelegten Zwecken, wie das Beispiel um die AccuWeather-App zeigt.

Für die Erwartungen, die hinsichtlich seiner (etwas überspitzt formuliert) Allmächtigkeit und Allwissenheit im Rahmen der ihm zugewiesenen Realweltausschnitte an den Verantwortlichen gestellt werden, kann daraus Folgendes geschlussfolgert werden: Insbesondere die Kontroll- und Wissensdefizite gegenüber Drittanbietern versetzen Diensteanbieter in eine Lage, in der sie weder selbst hinreichend die Risiken für Betroffene einschätzen, noch Betroffene ausreichend aufklären können, um deren Selbstschutzmechanismen zu aktivieren. Auch eine Einschätzung der Gefahrenlage, wie sie etwa im Rahmen einer Datenschutzfolgenabschätzung gefordert ist, kann von ihnen mangels hinreichender Sicherheit über Möglichkeiten und Transparenz über bereits getätigte Handlungen von Drittanbietern kaum seriös geleistet werden.

2. Der Verantwortliche als nach außen erkennbarer Akteur

Neben der eben geschilderten Zentralität des Verantwortlichen als allmächtiger und allwissender Akteur in Relation zu konkreten Verarbeitungsvorgängen setzt das datenschutzrechtliche Regelungskonzept auch seine hinreichende Erkennbarkeit nach außen voraus.[22] Bezweckt wird damit in erster Linie die Befähigung des Betroffenen, der Aufsichtsbehörden und, in geringerem Maße, auch Wettbewerbern und Interessensverbänden, eine wirksame Kontrolle auszuüben. Insofern korrespondiert diese Prämisse eng mit der eben beschriebenen und

[19] So etwa auf Apples iOS-Plattform lange Zeit die Captive Network API, die Entwicklern berechtigungsfrei den Zugriff auf Netzwerkdaten erlaubte, oder die Speech-to-text API unter Googles Android-Plattfform, die berechtigungsfrei den mittelbaren Zugriff auf Mikrofoneingaben erlaubte. Siehe für letztgenanntes Beispiel *Alepis/Patsakis*, in: Ali/Danger/Eisenbarth, Security, Privacy, and Applied Cryptography Engineering, S. 53 (61 f.).

[20] So etwa Apples CNCopyCurrentNetworkInfo API (https://developer.apple.com/documentation/systemconfiguration/1614126-cncopycurrentnetworkinfo), die den Zugriff auf Netzwerkdaten nun nur noch für abschließend aufgezählte Gründe gewährt, die von Entwicklern plausibel geltend gemacht werden müssen. Link zuletzt abgerufen am 14.01.2022.

[21] So etwa Apples Core Location API (https://developer.apple.com/documentation/corelocation/), die den unmittelbaren Zugriff auf Standortdaten nunmehr nur noch bei erteilter Nutzergenehmigung erlaubt. Link zuletzt abgerufen am 14.01.2022.

[22] Siehe *supra* Kapitel 2 B. II. 2.

sichern sich beide Prämissen gegenseitig ab: Nur, wenn die Identität des Verantwortlichen klar erkennbar ist und er leicht oder mit zumutbarem Aufwand erreicht werden kann, können Betroffenenrechte und Behördenüberprüfungen ausgeübt bzw. durchgeführt werden, während dieses Identitätswissen allein nicht genügt, solange nicht ebenfalls ausreichend Wissen über die genauen Umstände der Verarbeitung und damit über etwaige Gefahrenquellen und Fehler vorliegt. Gleichzeitig ist auch dieses inhaltliche Wissen nutzlos, wenn nicht eindeutig ist, an welchen Akteur man sich halten muss, um etwa Auskunftsansprüche geltend zu machen oder als Aufsichtsbehörde Maßnahmen anzuordnen.

Diese Rolle behalten Diensteanbieter auch unter der oben festgestellten veränderten Verarbeitungsrealität grundsätzlich bei, wenn sie selbst Daten im Rahmen der Nutzung ihrer Dienste erheben und weiterverarbeiten. Wenngleich Plattformbetreiber hier zunehmend die Rolle eines Intermediäres einnehmen und Distribution und Vermarktung eines Dienstes teils komplett übernehmen und somit für die nötige Sichtbarkeit beim Nutzer sorgen, sucht dieser sich eine App oder einen Dienst noch immer selbstständig aus und weiß somit in der Regel, wer der Diensteanbieter ist und dass keine Personenidentität zwischen ihm und dem Plattformbetreiber besteht. Auch wenn etwa die Datenschutzerklärungen von Diensteanbietern zunehmend von den Plattformbetreibern selbst im Rahmen ihrer Distributionskanäle vorgehalten werden – so etwa in Apples AppStore[23] –, nennen sie doch eindeutig den Diensteanbieter als Verantwortlichen und lassen ihn so erkennen. Gleiches gilt für Abfragen von Nutzereinwilligungen in die Verarbeitung bestimmter Datenkategorien, die immer häufiger und immer granularer vom Plattformbetreiber auf Systemebene durchgeführt werden,[24] aber keine Verwirrung darüber aufkommen lassen, dass es um die Berechtigung eines unabhängigen (und damit nicht systemseitigen) Dienstes geht. Trotz dieser grundsätzlich leichten Erkennbarkeit besteht jedoch häufig ein Defizit auf der Ebene der Erreichbarkeit und damit der Durchsetzbarkeit von Betroffenenrechten; hier mangelt es mitunter nicht nur an einheitlichen Kommunikationswegen, sondern auch an transparenten und korrekten Antworten von Seiten der Diensteanbieter.[25]

---

[23] Neben der Datenschutzerklärung der jeweiligen Diensteanbieter zeigt Apple inzwischen sogar komplette *privacy labels* für Apps an, anhand derer interessierte Nutzer mehr über das Datenverarbeitungsverhalten und etwaige Risiken erfahren sollen. Siehe *Nick Statt*, Apple launches new App Store privacy labels so you can see how iOS apps use your data, The Verge vom 14.12.2020 (https://www.theverge.com/2020/12/14/22174017/apple-app-store-new-privacy-labels-ios-apps-public). Zuletzt abgerufen am 14.01.2022.

[24] Auch hier ist stellvertretend Apple zu nennen. Die Core Location API unter iOS erlaubt Nutzern nicht nur die Wahl zwischen einmaliger oder dauerhafter Einwilligung, sondern auch zwischen der Einwilligung in die Übermittlung konkreter oder bloß approximierter Standortdaten. Siehe hierzu *Benjamin Mayo*, iOS 14 lets users grant approximate location access for apps that don't require exact GPS tracking, 9to5mac vom 12.08.2020 (https://9to5mac.com/2020/08/12/ios-14-precise-location/). Zuletzt abgerufen am 14.01.2022.

[25] Siehe die Studienergebnisse bei *Kröger* u. a., How do app vendors respond to subject

Anders gestaltet es sich bei Verarbeitungen, die unmittelbar durch Drittanbieter vorgenommen werden. Hier ist der Diensteanbieter als mittelbar beteiligter Akteur weiterhin sichtbar, da die Verarbeitung schließlich weiterhin im Rahmen der Nutzung seines Dienstes stattfindet. Weder wird aber die eigentliche Verarbeitung selbst wahrgenommen, noch macht sich der Drittanbieter aktiv gegenüber dem Nutzer kenntlich. Anders als in den EuGH-Urteilen Wirtschaftsakademie und Fashion ID, bei denen (in abgestufter Form) die Nutzer stets sehen konnten, dass sie zwar die Fanseite oder Website des von ihnen angesteuerten Unternehmens oder sonstigen Akteurs besuchten, diese sich aber auf Facebooks Plattform befand oder jedenfalls einen sichtbaren inhaltlichen Bestandteil aufwies, der erkennbar von Facebook kam, sind einbezogene Drittparteien in den allermeisten Fällen in keiner Weise sichtbar. Das gilt für Apps gleichermaßen wie für Websites, bei denen Dritten der Zugriff etwa durch Einbezug unsichtbarer Pixel gewährt wird, wie im oben geschilderten Fall des DRK Bayern[26] gesehen werden konnte. *En gros* verläuft die Grenze hier zwischen solchen Drittparteien, die einen unmittelbaren Mehrwert für den Nutzer bei der aktiven Nutzung des Dienstes einbringen und solchen, aus denen ausschließlich der Diensteanbieter einen Nutzen ziehen kann. Beispiele für die erste Kategorie sind etwa *social login*-Plugins oder „Like"-Buttons, Beispiele für die zweite Kategorie die erwähnten Adtech- und Datenbroker oder generelle Datenanalyseunternehmen. Doch die reine Erkennbarkeit des Drittanbieters erfasst noch nicht die volle Ebene der hier behandelten Prämisse. Zu wissen, *dass* eine Drittpartei eingebunden ist, ermächtigt einen Nutzer noch nicht. Dieser muss zudem wissen, in welchem Ausmaß und für welche Zwecke die betreffende Drittpartei auch Daten verarbeitet. Drittparteien müssen daher nicht bloß als Akteur sichtbar sein, sondern gerade in ihrer Rolle als Datenverarbeiter. Wählt ein App-Nutzer die Möglichkeit, sich mittels *social login* mit seinem Facebook-Account für die Nutzung einer App einzuloggen, ist ihm nicht zwingend bewusst, dass Facebook dabei Daten über sein Verhalten bei der Nutzung dieser App erhält. Nicht umsonst lag bei den beiden EuGH-Urteilen Wirtschaftsakademie und Fashion ID ein großer Schwerpunkt auf der Frage, welcher der beiden Verantwortlichen darüber aufzuklären hat, welche Verarbeitungen Facebook bzgl. der Besucherdaten vornimmt.

Informationen über die Existenz von Drittparteien, das Ausmaß ihres Einbezugs sowie insbesondere die von ihnen verarbeiteten Daten und die Kontexte der Verwendung dieser Daten finden sich daher regelmäßig (und oftmals ausschließlich) in den Datenschutzerklärungen der Diensteanbieter. Hier zeigen

---

access requests?, S. 9 f.: „It is evident from our results that there are no well-established and standardized processes for subject access requests in the mobile app industry. […] Many of the responses we received were not only completely insufficient, but also deceptive or misleading."

[26] Siehe *supra* Kapitel 1 A. II.

sich jedoch gleich mehrere Limitierungen. Zum einen realisiert sich erneut die im vorangegangenen Abschnitt bereits erörterte Problematik des beschränkten Wissens beim Diensteanbieter. Tiefergehende und insbesondere korrekte Informationen über die von ihm einbezogenen Drittparteien kann er nur insoweit angeben, wie sie ihm von diesen mitgeteilt wurden. Ob diese Angaben die Kategorien an zu verarbeitenden Daten sowie die Zwecke und das Ausmaß der Verarbeitung korrekt widerspiegeln, kann er schlicht nicht überprüfen. Noch schwerer wiegt aber die zweite Limitierung: Diensteanbieter legen die Identität und konkreten Verarbeitungszwecke der von ihnen eingebundenen Drittanbieter schlicht nicht immer vollumfänglich offen und müssen dies auch nicht. Selbst bei Vorliegen einer eigenen datenschutzrechtlichen Verantwortlichkeit von Diensteanbietern für die eigenständige Datenerhebung durch Drittanbieter (in Abgrenzung zu der aktiven Übermittlung dieser Daten durch den Diensteanbieter selbst) verlangt Art. 13 Abs. 1 lit. e DSGVO nur die Mitteilung der „Empfänger oder Kategorien von Empfängern der personenbezogenen Daten", nicht aber eine tiefergehende Offenlegung der im Einzelnen verfolgten Zwecke.[27] In der Praxis wird dieses Problem dadurch verschärft, dass die schiere Menge an einbezogenen Drittparteien echte Transparenz und Nachvollziehbarkeit schon aus rein faktischen Gründen auch dort erheblich erschwert, wo Diensteanbieter grundsätzlich alle nötigen Informationen offenlegen. Gut veranschaulicht wird dies anhand des Beispiels einer Analyse des Portals eBay und den auf seiner Website und seinen Apps involvierten Drittanbietern, die hier allerdings meist Empfänger von aktiv übermittelten Daten sind und nicht selbständig die Daten erheben.[28] Die Analyse zeigt, dass bereits die Anzahl involvierter Akteure – im Fall eBay insgesamt 2740 Stück[29] – die Übersichtlichkeit massiv erschwert. Weiter erschwert wird dies dadurch, dass die derzeit gängigste Best Practice-Maßnahme bei der Bereitstellung der Informationen über Drittanbieter und Datenempfänger darin besteht, an einer zentralen Stelle auf deren Datenschutzerklärungen zu verweisen bzw. zu verlinken. Für Datenempfänger bedeutet dies, dass deren aus Art. 14 DSGVO stammende Informationspflicht von eBay bereits miterfüllt wird.[30] Das bereits bei einzelnen Datenschutzerklärungen virulente Problem ihrer überbordenden Länge, aber auch generellen Lesbarkeit, welches das Ideal etwa der informierten Einwilligung in große Zweifel zieht,[31]

---

[27] Vgl. *Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 13 DSGVO Rn. 17; *Paal/Hennemann*, in: Paal/Pauly, DSGVO/BDSG, Art. 13 DSGVO Rn. 18.

[28] Siehe *Kurtz* u. a., Design Goals for Consent at Scale in Digital Service Ecosystems, S. 5 ff. für eine ausführliche Analyse des Falls.

[29] Vgl. *Kurtz* u. a., Design Goals for Consent at Scale in Digital Service Ecosystems, S. 6.

[30] Diese Möglichkeit findet in ähnlicher Form auch Erwähnung bei *Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 14 DSGVO Rn. 2.

[31] Siehe hierzu etwa *McDonald/Cranor*, I/S: A Journal of Law and Policy for the Information Society, 543 (543 ff.); *Utz* u. a., (Un)informed Consent, S. 973 ff.; *Van Alsenoy* u. a., International Review of Law, Computers & Technology 2014, 185 (189 ff.).

wird angesichts dessen, dass es sich nicht mehr nur um einzelne, sondern um tausende Datenschutzerklärungen handelt, geradezu exponentiell verstärkt.[32] Dass dies nur die Spitze des Eisbergs darstellt, zeigt die Studie ebenfalls: Jedenfalls im dort untersuchten Beispiel um eBay können die Datenschutzerklärungen, auf die verwiesen wurde, hinsichtlich ihrer Standards mitunter massiv voneinander abweichen, teilweise also weder auf Deutsch noch auf Englisch,[33] sondern in weiteren Fremdsprechen geschrieben sein; werden Links nicht konstant gepflegt und aktualisiert, drohen Verweise, die ins Nichts gehen oder auf bereits veraltete Versionen der Datenschutzerklärungen verweisen.[34]

Kombiniert man diese faktischen Limitierungen beim Versuch, jede einzelne in einen Dienst einbezogene Drittpartei, die eigenständig Daten verarbeitet (oder übermittelt bekommt), einzeln und im Detail sichtbar zu machen, mit dem legislativen Gedanken hinter der – wie beschrieben in ihrer Reichweite recht limitierten – Informationspflicht des Diensteanbieters, relativiert sich die Problematik zumindest teilweise. Bei der Weitergabe von Daten an (oder, hypothetisch ebenfalls unter die Pflicht subsumiert, der Ermöglichung der Erhebung durch) Drittanbieter muss *deshalb* nur in begrenztem Ausmaß über diese und ihr weiteres Vorgehen mit den Daten informiert werden, weil Drittanbieter als Empfänger von Daten *selbst* Verantwortliche sind und eigenständigen Informationspflichten unterliegen. Die präventive Information über die geplante Weitergabe dient also weniger der späteren Kontrolle als vielmehr der besseren Entscheidungsfindung darüber, ob dem initialen Verantwortlichen überhaupt die Datenverarbeitung erlaubt werden soll (im Falle einer Einwilligung) bzw. ob der Verarbeitung widersprochen werden soll (im Falle der Verarbeitung aufgrund berechtigter Interessen). Die Kontrolle der Datenempfänger soll also stattdessen dadurch gewährleistet werden, dass *sie* ihrerseits als Verantwortliche über die von ihnen verarbeiteten Daten und die damit verfolgten Zwecke aufklären müssen. Hier findet sich letztlich der Kern der Transparenzproblematik: Eine solche Information findet in der Praxis faktisch nicht statt. Nicht unmittelbar mit Betroffenen interagierende Datenempfänger wie Adtech[35]- und

[32] So würde es ca. 123 Stunden dauern, die Datenschutzerklärungen aller von eBay aufgelisteten Drittparteien und Datenempfänger zu lesen. Vgl. *Kurtz* u. a., Design Goals for Consent at Scale in Digital Service Ecosystems, S. 9.

[33] Ob Art. 12 Abs. 1 S. 1 DSGVO zwingend eine Information in der Landessprache des jeweiligen Nutzers voraussetzt, ist nicht endgültig geklärt. Jedenfalls eine Abfassung in einer nicht-englischen Fremdsprache dürfte aber in jedem Fall gegen die Voraussetzungen der Norm verstoßen. Vgl. etwa *Paal/Hennemann*, in: Paal/Pauly, DSGVO/BDSG, Art. 12 DSGVO Rn. 35.

[34] Siehe auch hier die Auflistung bei *Kurtz* u. a., Design Goals for Consent at Scale in Digital Service Ecosystems, S. 6, nach denen zum Zeitpunkt der Untersuchung unter den 906 einzigartigen Drittparteine und Datenempfängern 79 gar nicht abrufbare und 92 in einer nicht-englischen Fremdsprache verfügbare Datenschutzerklärungen waren.

[35] Siehe *Costello*, TechReg 2020, 11 (11 ff.) für einen umfassenden Überblick über Funktionsweise und datenschutzrechtliche Implikationen der Adtech-Branche.

Datenbroker- oder andere Datenanalyseunternehmen geben regelmäßig keine Auskunft darüber, dass und welche Daten sie übermittelt bekommen und was sie damit tun. Das eigentliche Problem ist also eines der Rechtsdurchsetzung, das dazu führt, dass in der Gemengelage der Akteurspluralität die Erkennbarkeit der einzelnen Akteure auf der Strecke bleibt. Dass die Informationspflicht des vorgelagerten Diensteanbieters dieses Defizit ebenso wenig zu kompensieren vermag wie die freiwillige zentrale Auflistung aller Datenschutzerklärungen durch den Diensteanbieter (wie im Fall eBay), ist dann nicht weiter verwunderlich.[36]

3. Der Verantwortliche als einfach zuordenbare Rolle

Eine weitere, den beiden eben beschriebenen Prämissen etwas vorgelagerte, Anforderung an den Akteur, dem das Datenschutzrecht die Rolle des Verantwortlichen zugeschreibt, ist die, dass er sich seiner Rolle stets bewusst, diese also für ihn grundsätzlich einfach zuordenbar ist.[37] Akteuren muss es beim alltäglichen Handeln unmittelbar klar sein, wenn sie dergestalt Einfluss auf die Verarbeitung personenbezogener Daten nehmen, dass dabei die von Art. 4 Nr. 7 DSGVO aufgestellte Einflusshürde überschritten wird. Nur so kann gewährleistet werden, dass etwa auch die der eigentlichen Datenverarbeitung vorgelagerten Organisationspflichten und Instrumente zum Systemdatenschutz durchgängig beachtet werden.

Dass hier grundsätzlich Schwierigkeiten bestehen, als Akteur die Subsumtion des eigenen Lebenssachverhalts nicht nur unter die Voraussetzungen der Rolle des Verantwortlichen, sondern auch der weiteren relevanten Rollen der DSGVO – wie etwa dem Auftragsverarbeiter – zu erreichen, wurde bereits erörtert. Nicht zuletzt die durch den EuGH in ihrer Bedeutung rapide gewachsene gemeinsame Verantwortlichkeit birgt hier grundlegende Abgrenzungsprobleme. Diese der DSGVO bereits inhärenten Schwierigkeiten werden durch die zunehmende Akteurspluralität weiter verstärkt. Je mehr Akteure auf unterschiedlichen Ebenen und zu unterschiedlichen Zeitpunkten Beiträge zu Datenverarbeitungen leisten, desto schwieriger wird es für sie, ihren jeweils eigenen Beitrag im Gesamtkontext korrekt einzuordnen und so eine Einschätzung über die eigene Klassifizierung abzugeben. Letztlich führen so beide Ursprünge zu-

---

[36] So auch *Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, Art. 12 DSGVO Rn. 6: „Insbesondere im Bereich des Tracking sowohl durch den Anbieter auch durch in das Angebot eingebundene Dritte, bspw. über Werbung, hat die transparente Information der betroffenen Person besondere Bedeutung. Gerade aber hier mangelt es häufig an präziser, transparenter und verständlicher Darstellung." *Kurtz* u. a., Design Goals for Consent at Scale in Digital Service Ecosystems, S. 9 ff. machen hier erste konkrete Designvorschläge für eine transparentere und verständlichere Auflistung von Drittparteien und Datenempfängern; einen Überblick über die Designpraxis am Beispiel populärer smarter Haushaltsgeräte liefert *Hoofnagle*, EuCML 2018, 162 (167 ff.).

[37] Siehe *supra* bei Kapitel 2 B. II. 3.

sammen und verstärken sich gegenseitig: Das vom EuGH aufgrund der Beteiligung mehrerer Akteure erweiterte Konzept der Verantwortlichkeit, das eigentlich für klarere Verhältnisse sorgen sollte, bringt letztlich seinerseits eine nochmals erschwerte Einordnung mit sich.

Diese erschwerte Subsumtion zeigt sich auch dann, wenn man die vom EuGH erarbeiteten Kriterien auf die archetypischen Akteurskonstellationen im Bereich digitaler Dienste anwendet: Während hier die Verantwortlichkeit der einzelnen Drittparteien für die unmittelbar von ihnen selbst für eigene Zwecke vorgenommenen Verarbeitungen unstrittig und auch für diese ohne weiteres erkennbar sein dürfte, stellt sich die Einordnung bei den einzelnen Diensteanbietern ungleich schwieriger dar. Mit den im vorangegangenen Kapitel festgehaltenen Erkenntnissen aus der jüngeren EuGH-Rechtsprechung[38] liegt es jedenfalls dogmatisch nahe, hier aufgrund der initialen Ermöglichung der Drittanbieterverarbeitungen durch den Diensteanbieter sowie der regelmäßig kongruenten wirtschaftlichen Zwecke eine gemeinsame Verantwortlichkeit anzunehmen. Doch ist, soviel muss konstatiert werden, diese – im Übrigen ihrerseits nicht unumstrittene – rechtswissenschaftliche Ansicht eine Sache und die faktische Rechtssicherheit auf Seiten potenzieller Verantwortlicher eine gänzlich andere. Ein anhaltender Mangel an Rechtssicherheit aufgrund fehlender Vorgaben durch Aufsichtsbehörden oder übergeordnete europaweite Institutionen wie dem EDSA sorgt dafür, dass an Datenverarbeitungen beteiligte Akteure eine einfache und eindeutige Bestimmung ihrer eigenen Rolle kaum leisten können. Für Diensteanbieter, die zu unterschiedlichen Zwecken Gebrauch von Drittparteien machen, wiegt diese Unsicherheit besonders schwer.

II. Bedeutung

Alle drei der in Kapitel 3 aufgedeckten Prämissen des Verantwortlichkeitskonzepts stehen somit ob der Komplexität von Akteurskonstellationen in modernen Verarbeitungskontexten unter zunehmendem Druck. Von den drei aufgezeigten Akteursgruppen (Plattformbetreiber, Diensteanbieter, Drittanbieter) sind alle von dieser Entwicklung in unterschiedlichem Ausmaße und auf unterschiedliche Weise betroffen. Einerseits unmittelbar, indem in sie gesetzte Erwartungen wie etwa die umfassende Kontrollmöglichkeit und umfängliches Wissen oder die leichte und direkte Erkennbarkeit nach außen nicht mehr ohne weiteres erfüllt werden. Zum anderen mittelbar, indem die in Kapitel 1 beschriebenen Kontrollverluste und -verschiebungen auch dazu führen, dass nun anstelle eines Akteurs eine Vielzahl von Akteuren in unterschiedlichem Maße und unterschiedlichen Stadien Kontrolle über Verarbeitungsumstände ausübt und so als potenzielle Verantwortliche in Betracht kommt, sodass auch das Ideal

[38] Siehe Kapitel 2 C. II. 4.

der leichten Erkennbarkeit der eigenen Rolle stark in Mitleidenschaft gezogen wird.

Ebenfalls zu konstatieren sind weitreichende Auswirkungen für die quer zu den genannten Prämissen liegende Grundvoraussetzung eines Mindestmaßes an Rechtsdurchsetzung.[39] Auch hier zeigt sich, dass die mit der heutzutage vorherrschenden Akteurspluralität verbundenen Praktiken – sowohl hinsichtlich der Arten und Weisen der Kooperation und gegenseitigen Einbindung als auch der typischen Geschäftsmodelle – das ohnehin von einem chronischen Durchsetzungsdefizit gebeutelte Datenschutzrecht weiter strapazieren. Die schiere Anzahl an regelmäßig eingebundenen Akteuren, aber auch ihre verstetigte Praxis, über den Empfang und die Verwendung der Daten nicht zu informieren, macht eine Durchsetzung vonseiten der Betroffenen nahezu unmöglich; Kontrolle und Durchsetzung durch Aufsichtsbehörden ist nur insoweit möglich, als sie losgelöst von konkreten Verarbeitungsvorgängen stattfindet und sich auf den generellen Geschäftszweck und die breitflächig stattfindenden, potenziell datenschutzwidrigen Praktiken konzentriert. Auch dies setzt jedoch voraus, dass ein Akteur einer Aufsichtsbehörde überhaupt bekannt ist oder wird – ohne Beschwerden durch Betroffene oder eigenständige Mitteilungen durch die jeweiligen Verantwortlichen im Rahmen von bspw. Datenschutzfolgenabschätzungen fehlen dafür wichtige Kommunikationsprozesse. Die grassierende Rechtsunsicherheit bei der Frage, wer in welchen Kontexten als (gemeinsamer) Verantwortlicher gilt, erweitert die Problematik der Rechtsdurchsetzung auch auf solche Akteure, die grundsätzlich konformitätswillig wären, sich ihrer Pflichtigkeit aber nicht gewahr sind.

In Anbetracht dieser Erkenntnisse kann nicht mehr davon ausgegangen werden, dass das Konzept der datenschutzrechtlichen Verantwortlichkeit die von ihm erhoffte Effektivität zeitigt. Es droht eine breitflächige Dysfunktionalität des Gesamtkonzepts durch organisierte Verantwortungslosigkeit, wenn die vom gesetzgeberischen Konzept als Erwartung an eine Person formulierte Kontrolle und das erwartete Wissen nicht mehr in der Person, die die Normvoraussetzungen erfüllt, vorhanden ist, und sich stattdessen über eine Vielzahl von Akteuren hinweg verteilt, von denen manche ebenfalls als Verantwortliche qualifiziert werden, während andere unter keine Rolle der DSGVO fallen und bei wiederum anderen große Unklarheit bzgl. ihrer Einordnung besteht.[40]

---

[39] Siehe dazu *supra* Kapitel 2 B. II. 4.

[40] In diese Richtung gehend auch *Tene*, Ohio State Law Journal 2013, 1217 (1219): „[…] in many contexts, such as mobile applications, behavioral advertising, or social networking services, it is not necessarily the controller, but rather an intermediary or platform provider, that wields the most control over information." Ebenso *Mahieu* u. a., jipitec 2019, 85 (88): „[…] will make it increasingly complex to apply the existing linear controller-processor model."

B. Die Ausweitung der Verantwortlichkeit als Lösungsansatz

In Kapitel 2 wurde bereits festgestellt, dass die Stellschrauben für das Konzept der Verantwortlichkeit und seine generelle Wirksamkeit einerseits in der *Auswahl* des Verantwortlichen, andererseits in der *Ausgestaltung* des die Verantwortlichkeit ausmachenden Pflichtenkatalogs bestehen.[41] Mit der nun hinzugewonnenen Erkenntnis um die tatsächlich defizitären Grundprämissen der Verantwortlichkeit soll nun daher ein erster Schritt in Richtung eines Lösungsansatzes unternommen werden. Dieser konzentriert sich primär auf die Komponente der *Auswahl* des Verantwortlichen, betrifft aber nachgelagert auch die Frage einer angepassten *Ausgestaltung* der einzelnen Pflichten. Der Vorgang bei der Annäherung an eine Ausweitung der Verantwortlichkeit ist dabei, angelehnt an das Vorgehen des EuGH, eine schrittweise Entfernung von den unmittelbar an einem Verarbeitungsakt beteiligten Akteuren, um nach und nach auch die Akteure, deren Beteiligungen eine größere Entfernung zur Verarbeitung aufweisen, auf ihre Tauglichkeit zur Verantwortlichkeit hin zu untersuchen. Dabei wird auf die in Kapitel 1 identifizierten typischen Rollen im Rahmen des Angebots digitaler Dienste zurückgegriffen: den Diensteanbieter, die Drittparteien bzw. Drittanbieter und den Plattformbetreiber.[42]

I. Notwendigkeit einer extensiven Verantwortlichkeitszuschreibung

Die generelle Notwendigkeit einer Weiterentwicklung der Verantwortlichkeitszuschreibung ergibt sich aus den bisher festgestellten Erkenntnissen. Wie in Kapitel 2 festgestellt, besteht eine verordnungsgeberische Pflicht, die DSGVO regelmäßig auf ihre Wirksamkeit hin zu evaluieren.[43] Grundlegende Wirksamkeitsdefizite können einerseits dafür sorgen, dass der Verordnungsgeber einer ihn treffenden Schutzpflicht nicht hinreichend nachkommt, andererseits können sie dazu führen, dass die Rechtfertigung für die Eingriffe in die Grundrechte von Datenverarbeitern nicht mehr vorliegt.[44] Unterhalb dieser verfassungsrechtlich relevanten Schwelle verschreibt sich die EU im Großen, wie auch die DSGVO im Kleinen, dem Ideal einer möglichst großen Wirksamkeit. Auch der EuGH hat, beginnend mit seinem Google Spain-Urteil[45] und in konsequenter Fortentwicklung und Konkretisierung in den Wirtschafts-

---

[41] Siehe *supra* bei Kapitel 2 B. II. 5.

[42] Siehe *supra* bei Kapitel 1 A.

[43] Siehe *supra* bei Kapitel 2 B. III. 3. und 4.

[44] Für die Aktivierung einer Schutzpflicht im Rahmen digitaler Dienste plädierend *Weichert*, ZD 2014, 605 (609): „Diese Schutzpflicht ist bei der immer arbeitsteiliger werdenden Internet-Datenverarbeitung von zentraler Bedeutung, da es hier äußerst schwierig ist, effektiv die digitalen Grundrechte durchzusetzen."

[45] EuGH Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317.

akademie-[46] und Fashion ID-Urteilen[47], dieses Leitbild betont und die besondere Bedeutung eines extensiven Verständnisses der Verantwortlichkeit für seine Erreichung herausgestellt. Gerade die Inpflichtnahme zusätzlicher Akteure im Rahmen der DSGVO (und vor ihr der DSRL) kann daher notwendig sein, „damit die darin vorgesehenen Garantien ihre volle Wirksamkeit entfalten können und ein wirksamer und umfassender Schutz der betroffenen Personen, insbesondere ihres Rechts auf Achtung ihres Privatlebens, tatsächlich verwirklicht werden kann."[48]

Aufgrund des defizitären Regulierungskonzepts der datenschutzrechtlichen Verantwortlichkeit ist die grundlegende Wirksamkeit dieses Konzepts in starke Mitleidenschaft gezogen. Dass die Tatsache, dass grundsätzlich für jede Verarbeitung oder jeden Verarbeitungsabschnitt ein Akteur oder mehrere Akteure jeweils die nach bisherigen Maßstäben definierte Schwelle der hinreichenden Einflussnahme auf Zweck- und Mittelbestimmung überschritten haben und als Verantwortliche einzustufen sind, nicht automatisch bedeutet, dass die mit dem Verantwortlichkeitskonzept verknüpften Instrumente auch greifen, hat der Abgleich im vorangegangenen Abschnitt gezeigt. Das OVG Schleswig liegt insofern falsch, wenn es im Zusammenhang mit Facebook-Fanpages behauptet, eine Schutzlücke bestünde schon dann nicht, wenn „es für jede Datenverarbeitung eine verantwortliche Stelle gibt", weil „[u]nverantwortliche Aktivitäten" dann ausgeschlossen seien.[49] Der bloße formelle Akt der Zuordnung eines verantwortlichen Akteurs zu einer Datenverarbeitung garantiert gerade noch nicht, dass dieser Akteur die damit verbundenen Erwartungen auch erfüllt bzw. erfüllen kann; ebenso wenig garantiert er, dass die im gesetzlichen Regelungskonzept vorgesehenen Instrumente zur Rechtsdurchsetzung bei Verstößen gegen die auferlegten Pflichten von den dazu ermächtigten Akteuren durchgesetzt werden können.

Besondere Gefährdungspotentiale für Betroffene bestehen dann, wenn sie sich mit einer Vielzahl verarbeitungsbeteiligter Akteure konfrontiert sehen, zudem schon deshalb, weil häufig eine sehr geringe Erkennbarkeit vorliegt und ein eigenverantwortliches Vorgehen unter Berücksichtigung aller Implikationen und Konsequenzen somit nahezu unmöglich ist. Wie der EuGH in seiner Fashion ID-Entscheidung korrekt festgestellt hat,[50] ist es stets erschwerend zu

---

[46] EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388.

[47] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629.

[48] EuGH Rs. C-131/12 (Google Spain), ECLI:EU:C:2014:317 Rn. 38 zur Begründung der Verantwortlichenstellung von Google im Rahmen der Tätigkeit ihrer Suchmaschine.

[49] OVG Schleswig, ZD 2014, 643 (645).

[50] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 83 mit Verweis auf EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 42. Im hinter dem letztgenannten Urteil stehenden Fall war die Diskrepanz zwischen Mitgliedern und Nicht-Mitgliedern noch größer, da Mitglieder von innerhalb der Plattform die

berücksichtigen, wenn der Besucher einer Website oder Nutzer einer App bereits unmittelbar durch den Besuch oder die Nutzung eine Datenverarbeitung eines Dritten – wie im Entscheidungsfall Facebook durch Einbezug ihres *social plugin* – auslöst, zu dem der Betroffene – wie im Falle Facebooks ein Nichtmitglied – keinen bewussten Bezug hat. Ob die bloße vor Verarbeitungsbeginn erteilte Information über die Existenz und die Verarbeitungsabsichten des Dritten allein ausreichen, um die damit einhergehenden Gefahrenpotentiale ausreichend abzumildern, darf angezweifelt werden. In diese Richtung gingen jedoch die urteilenden Gerichte in den Fällen Wirtschaftsakademie und Fashion ID, die in erster Linie den fehlenden Hinweis auf Facebook*s* Verarbeitungspraktiken und Datenschutzerklärung sowie die Existenz eines Widerspruchsrechts monierten.[51] Hiergegen lässt sich einwenden, dass in typischen Konstellationen einbezogener Drittparteien die Lage für den Betroffenen ungleich schwieriger ist, weil er nicht nur – wie im Falle der beiden EuGH-Urteile – *einem* ihm ggf. unbekannten Akteur wie Facebook, sondern gleich einer *Vielzahl* an Drittanbietern gegenübersteht, deren Einbezug zudem häufig nicht allein durch die Nutzung des Front-Ends des genutzten Dienstes sichtbar wird. Dass der gerichtliche Tenor dahin geht, die bloße Transparentmachung für ausreichend zu erachten, lässt aber auch die jüngere Rechtsprechung des BGH zu Cookie-Bannern vermuten. Dieser zufolge muss zwar bei technisch nicht notwendigen Drittpartei-Cookies zwingend eine Einwilligung des Nutzers vorliegen,[52] es genügt dann zur Datenschutzkonformität aber die Erfüllung der für Einwilligungen grundsätzlich erforderlichen Informationspflichten sowie die Absicherung dessen, dass vor erteilter Einwilligung keine Cookies gesetzt und keine Daten übertragen werden. Gleichzeitig zeigt das Urteil des BVerwG, mit dem die Rechtmäßigkeit der Abschaltungsanordnung gegenüber dem Fanpage-Betreiber als gemeinsamem Verantwortlichen als rechtmäßig bestätigt wurde, dass bei Nichterfüllbarkeit der Erwartungen mit einer Sanktion zu rechnen ist, die, bei Betrachtung der schieren Menge an Fanpages und an in Websites und andere Dienste eingebundenen Drittparteien wie Facebook, kaum ernsthaft global gegenüber allen zuwiderhandelnden „Veranlasserverantwortlichen" durchgesetzt werden kann.[53]

Aus diesen Urteilen grundlegende gerichtliche Festlegungen zur Gefahrenlage bei Multiakteurskonstellationen zu ziehen, wäre dennoch verfehlt. Der

---

infragestehende Fanpage besuchen konnten (was einen geringeren Kontextwechsel bedeuten würde), während Nicht-Mitglieder zwangsläufig von außerhalb (etwa von der Website des Fanpage-Betreibers oder von einer Suchmaschine) zur Fanpage und damit auf das soziale Netzwerk gelangen mussten.

[51] Vgl. BVerwG, Urt. v. 11.09.2019, Az. 6 C 15.18 (Wirtschaftsakademie Schleswig-Holstein) Rn. 2.

[52] Vgl. BGH, Urt. v. 28.05.2020, Az. I ZR 7/16 (Cookie-Einwilligung II) Rn. 55.

[53] Zu der Widersprüchlichkeit der an die vom EuGH identifizierten gemeinsamen Verantwortlichen gestellten Erwartungen siehe *supra* in Kapitel 2 C. II. 4. c) cc).

BGH entschied allein die materiellrechtliche Frage der Reichweite dessen, was die bisherigen Pflichten nach bestehender Rechtslage vom bisherigen Verantwortlichen verlangen. Auch die Urteile von EuGH und BVerwG bezogen sich hinsichtlich dieser Frage konkret auf die vorliegenden Konstellationen, in denen die neu als gemeinsame Verantwortliche herangezogenen Website- und Fanpage-Betreiber, wie mehrfach betont, nur begrenzte Handlungsmöglichkeiten hatten. Die – zudem nicht abschließend beurteilte – Reichweite der diese Verantwortlichen treffenden Pflichten folgte daher in erster Linie Zumutbarkeitserwägungen. Gleichzeitig zeugt allein die Tatsache, dass hier bisher nicht berücksichtigte Akteure in den Kreis der (gemeinsamen) Verantwortlichkeit einbezogen wurden, unbestreitbar davon, dass eine Notwendigkeit zum Handeln erkannt wurde. Mit anderen Worten: Dass in den vorliegenden Fällen die Möglichkeit dieser Verantwortlichen, auf die durch sie ermöglichten Verarbeitungen durch Facebook jedenfalls hinzuweisen, als zentrale Pflicht betont und dies zunächst als ausreichend erachtet wurde, erlaubt noch nicht den weiteren Schluss, die unbestritten erkannte Gefahrenlage wäre damit bereits hinreichend abgemildert; es zeigt einzig, dass nach Ansicht von EuGH und BVerwG von *diesen* Verantwortlichen im Rahmen ihrer Möglichkeiten und in *diesen* konkreten Konstellationen nicht mehr als die Information des Betroffenen verlangt werden kann. Über einerseits die Pflichtenreichweite derselben Verantwortlichen in anderen Konstellationen und andererseits die verbleibende Gefahrenlage für Betroffene in diesen und anderen Konstellationen ist damit noch nichts gesagt. Insbesondere der EuGH war in seinen Urteilen gebunden durch die konkrete Vorlagefrage,[54] aber auch die grundlegenden Limitierungen der richterlichen Rechtsfortbildung.[55]

Es ist demnach jedenfalls einer von mehreren möglichen gangbaren Wegen, die Verantwortlichkeit auf solche Akteure auszweiten, die nach bisheriger Rechtslage bzw. bisherigem Verständnis dieser noch nicht als solche in Betracht kamen, sich aber aufgrund ihrer Einfluss- und Kontrollmöglichkeiten und Expertise anbieten. Vereinzelt wurde ein solcher Perspektivenwechsel – oder genauer: eine solche Perspektivenerweiterung – in der Literatur bereits gefordert.[56] Damit einher geht eine Inpflichtnahme von Akteuren zur Eindämmung

[54] Während es in der Wirtschaftsakademie-Entscheidung alleine um die Frage der Verantwortlichkeit des Fanpage-Betreibers ging, waren die Vorlagefragen 5 und 6 im Fall Fashion ID explizit darauf bezogen, ob ein Websitebetreiber hinsichtlich der Verarbeitungen durch einbezogene Dritte wie Facebook als Empfänger der Nutzereinwilligungen in Betracht kommt und von der Informationspflicht des Art. 10 DSRL (nun Art. 13 DSGVO) getroffen wird. Siehe EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 42.

[55] Zu diesem Thema im deutschen Verfassungsrecht siehe *Kruse*, Die verfassungsrechtlichen Grenzen richterlicher Rechtsfortbildung; *Wank*, Grenzen richterlicher Rechtsfortbildung; umfassend zu den Grenzen auf unionsrechtlicher Ebene *Walter*, Rechtsfortbildung durch den EuGH – Eine rechtsmethodische Untersuchung ausgehend von der deutschen und französischen Methodenlehre.

[56] Siehe etwa, bezugnehmend auf den technischen Wissensvorsprung von Cloud-Provi-

von Gefahren im Zusammenhang mit Datenverarbeitungen bei gleichzeitiger Entfernung von der bzw. den jeweiligen als Anknüpfungspunkt dienenden Datenverarbeitung(en). Die damit verbundene Hoffnung bezieht sich auf mehrere Ebenen: Einerseits wäre zu erwarten, dass die neu erfassten Akteure ihrerseits die an sie gerichteten Erwartungen, also unter anderem die ihnen auferlegten materiellen Pflichten, erfüllen können. Darüber hinaus müsste ihre Verantwortlichkeit aber auch dafür sorgen, dass über den eigenen Raum hinaus das gesamte regulatorische und faktische Umfeld der in Betracht stehenden Datenverarbeitung(en) einen Zugewinn an Wirksamkeit erfährt. Es müssten also auch die Erwartungen an die im jeweiligen Einzelfall bereits vorher in die Pflicht genommenen Akteure besser erfüllt und der Schutz der jeweiligen Betroffenen insgesamt verstärkt werden. Das jedoch kann – mit der eben beschriebenen Unzulänglichkeit bloßer isoliert nebeneinander bestehender Verantwortlichkeiten – nur erreicht werden, wenn die verschiedenen auf einen einheitlichen Lebenssachverhalt gerichteten Verantwortlichkeiten reflexiv aufeinander bezogen sind. Nur so erscheint es möglich, durch neu in die Pflicht genommene Akteure zu gewährleisten, dass die bei den unterschiedlichen Typen bereits bekannter Verantwortlicher aufgezeigten Defizite wie die fehlende Kontrollfähigkeit von Diensteanbietern gegenüber Drittparteien oder die aus Perspektive Außenstehender meist fehlende Erkennbarkeit der einbezogenen Drittparteien ausgeglichen werden, also eine gesteigerte Befähigung[57] sowohl der „klassischen" Verantwortlichen als auch der zur Durchsetzung aufgerufenen Akteure (primär Betroffene und Aufsichtsbehörden) erreicht wird. Der Ansatz ähnelt insofern dem von *Helberger u. a.* vorgeschlagenen Konzept einer kooperativen Verantwortung („*cooperative responsibility*"[58]), nach dem soziale Netzwerke, Inhalte generierende Nutzer und öffentliche Institutionen in einem dynamischen Austausch jeweils unterschiedliche Verantwortungsrollen einnehmen und so ihre jeweiligen Handlungsfähigkeiten verstärken, wobei insbesondere Plattformen die Rolle zukommen sollte, das konforme Handeln von Nutzern zu unterstützen und anzuregen.[59]

---

dern gegenüber ihren Nutzern, *Sydow/Kring*, ZD 2014, 271 (275): „Die effizientere datenschutzrechtliche Strategie ist, das IT-Marktgeschehen auf der Angebotsseite in den Blick zu nehmen."

[57] Dergestalt, dass diese stärker befähigten Akteure in eine Lage versetzt werden, aus der heraus sie ihre Pflichten und Aufgaben wirksamer erfüllen können.

[58] *Helberger* u. a., The Information Society 2018, 1 (3 ff.).

[59] Siehe *Helberger* u. a., The Information Society 2018, 1 (10): „We have indicated that the latter can take various forms, from educating users and taking up prospective design responsibility in platform architectures, to governments creating a framework for more transparent and publicly responsible forms of content curation and service delivery."

II. Legitimation der jeweiligen Zusatzbelastung

Doch wie lässt sich die Zusatzbelastung für die bisher nicht in die Pflicht genommenen Akteure legitimieren? Allgemein lässt sich hierzu auf das bereits mehrfach Geschilderte verweisen: Da die Effektivität des Regelungskonzepts insgesamt Voraussetzung für seine verfassungsrechtliche Legitimität ist, sind verhältnismäßige Zusatzbelastungen bzw. ist die Ausweitung des Kreises der Normunterworfenen als Kehrseite der Medaille dann legitim, wenn dies insgesamt zu einer höheren Wirksamkeit des Regelungskonzepts beiträgt und die einzelnen Normunterworfenen gleichzeitig nicht unzumutbar belastet. Darunter lassen sich zwei Voraussetzungen bilden, die vorliegen müssen, um die Zusatzbelastung eines Akteurs bzw. einer Akteursgruppe konkret zu legitimieren: Einerseits die oben beschriebene Fähigkeit zur wirksamen Erfüllung der jeweiligen materiellrechtlichen Pflichten, aber auch zur Leistung der grundlegenderen Steuerungseffekte auf die weiteren Verantwortlichen sowie die zur Durchsetzung des Rechts berufenen Akteure in Form von Betroffenen und Aufsichtsbehörden (1.).[60] Außerdem ein hinreichender Zurechnungstatbestand, durch den ein kausaler Zusammenhang des die Verantwortlichkeit auslösenden Handelns mit der infragestehenden Gefahr – hier also der Datenverarbeitung als vom Datenschutzrecht definierter Anknüpfungspunkt – sichergestellt wird (2.).

1. Fähigkeit zur Pflichtenerfüllung/Zielerreichung

Wie im letzten Abschnitt bereits festgestellt wurde, kommen für die zusätzliche Inpflichtnahme Plattformbetreiber (a)) und Diensteanbieter (b)) als typisierte Akteursgruppen in Betracht. Die folgenden Überlegungen folgen der bereits erwähnten Zweiteilung und betreffen einerseits die Fähigkeit zur Erfüllung eigener materiellrechtlicher Pflichten, andererseits die damit verknüpfte, aber weiterreichende Erwartung der gesteigerten Befähigung bestehender Verantwortlicher zur Erfüllung ihrer Pflichten sowie die Unterstützung der zur Durchsetzung vorgesehenen Akteure in Person von Betroffenen und Aufsichtsbehörden – und damit insgesamt die Steigerung des Schutzniveaus für Betroffene. Da die konkreten materiellen Pflichten, die mit einer Verantwortlichkeit dieser Akteure einhergehen würden, von der konkreten *Ausgestaltung* einer solchen Verantwortlichkeit abhängen und damit erst in den folgenden Abschnitten im Detail erörtert werden, sind die folgenden Überlegungen (jeweils aa)) auf dieser ersten Ebene notwendigerweise eher typisiert und abstrakt. Hier bietet sich eine Trennung zwischen unmittelbar auf Datenverarbeitungen durch bisherige Verantwortliche bezogene Pflichten einerseits und generelle, auf die Gestaltung des eigenen Systems gerichtete, Pflichten andererseits an. Die Fähigkeit zur

[60] Zu der zuletzt genannten Gruppe müssen in begrenztem Umfang auch Mitbewerber und Verbraucherschutz- und andere Interessenverbände gezählt werden.

Kompensation der derzeitigen Defizite im Zusammenhang mit den bisherigen Verantwortlichen (jeweils bb)) ist dann eine nachgelagerte Frage, die sich an den diese Verantwortlichen treffenden Pflichten sowie den dahinter stehenden Grundprämissen zu messen hat.

a) Plattformbetreiber

„Regulation by the platform can potentially be superior to regulation by state or federal governments. […] Platforms often have considerably greater visibility into user behaviour than public regulators, providing an opportunity to sanction behaviour earlier and with greater accuracy."[61]

Wie in Kapitel 2 erörtert wurde, haben Plattformbetreiber eine herausgehobene Stellung bei der Bildung und Durchsetzung von Regeln sowie der Bereitstellung von handlungsraumeröffnenden und -begrenzenden Infrastrukturen auf ihren Plattformen.[62] Bereits die Tatsache, dass sie plattformweit entsprechende *boundary resources* entwickeln, bereitstellen und durchsetzen, zeigt, dass sie ein Ausmaß an Einfluss ausüben können und tatsächlich ausüben, durch welches einerseits das Verhalten des einzelnen datenverarbeitenden Plattformnutzers weitgehend gesteuert und andererseits eine große Anzahl solcher Plattformnutzer erreicht werden kann.

aa) Eigene materielle Pflichten

Die Datenverarbeitungen, auf die Plattformbetreiber mittelbar Einfluss nehmen können, sind die der Diensteanbieter einerseits und die der von diesen einbezogenen Drittparteien andererseits.[63] In beiden Fällen sind Plattformbetreiber in der Lage, solchen Pflichten wirksam nachzukommen, die unmittelbar diese Datenverarbeitungen betreffen, also bspw. darauf bezogen sind, wann und unter welchen Umständen Diensteanbieter und Drittparteien Daten verarbeiten (dürfen), welche Zwecke festgelegt und ob die Verarbeitungen tatsächlich auf diese begrenzt werden. Auch das Vorliegen einer Rechtsgrundlage, etwa das rechtzeitige Einholen einer nicht offensichtlich unwirksamen Einwilligung oder die Vorlage einer jedenfalls grundsätzlich nachvollziehbaren Interessenabwägung im Rahmen von Art. 6 Abs. 1 lit. f DSGVO kann im Rahmen von als *bounda-*

---

[61] *Parker/Van Alstyne*, in: Augier/Teece, The Palgrave encyclopedia of strategic management, S. 1290 (1295).

[62] Vgl. auch *Helberger* u. a., The Information Society 2018, 1 (4): „As laws, directives and procedures allocate and distribute responsibility in institutions, we argue that in the case of platforms, the architectural design choices play a similar role."

[63] Hinzu kommen die von Plattformbetreibern selbst vorgenommenen Verarbeitungen, die hier aber nicht im Fokus stehen sollen, da hier eine originäre Verantwortlichkeit der jeweiligen Plattformbetreiber stets ohne weiteres gegeben ist und – nicht zuletzt bedingt durch die Machtstellung eines Plattformbetreibers – keine relevante Beteiligung anderer Akteure die Lage verkompliziert.

ry resources ausgestalteten Kontrollmechanismen überprüft werden. Durch bewusstes Verengen von Möglichkeitsräumen können Plattformbetreiber neben dieser Überprüfung der Einhaltung von Pflichten auch absichern, dass Diensteanbieter sich nur so verhalten können, dass die Einhaltung ihrer Pflicht möglich ist und bleibt. So gesehen kann, bei geschickter und gesetzlich und behördlich angeleiteter Gestaltung der Plattforminfrastruktur, im Idealfall bereits proaktiv verhindert werden, dass sich einzelne Praktiken entwickeln, die sich zunehmend von den datenschutzrechtlichen Vorgaben entfernen. Gleichzeitig könnten spätere Nachjustierungen dafür sorgen, dass als problematisch erkannte Praktiken erschwert oder verunmöglicht werden.[64] Ein solches Vorgehen könnte als eine Art angeleiteter Weg in Richtung *privacy by design* hinsichtlich der datenverarbeitenden Nutzung der Plattforminfrastruktur verstanden werden.

Durch ihre Vermittlerrolle zwischen Diensteanbieter und Nutzer sowie ihre generelle Gatekeeperfunktion sind Plattformbetreiber zudem in besonderem Maße dazu geeignet, auch konkreten Verarbeitungen vorgelagerte und auf Systemgestaltung gerichtete Pflichten zu erfüllen.[65] Betreffen diese etwa die Gestaltung der plattformeigenen Schnittstellen, die Regelbildung bei der Aufnahme auf die Plattform oder in den primären bzw. einzigen Distributionskanal, oder die kursorische Prüfung der Seriosität einbezogener Drittparteien, kann das weitreichende Auswirkungen auf die grundlegenden Gestaltungen der Dienste auf der Plattform haben. Auch hier kann somit wieder unterschieden werden zwischen Kontrolle einerseits und vorgezogener Absicherung andererseits. Zur erstgenannten Kategorie kann es etwa gehören, zu überprüfen, ob, in welcher Form und mit welchem Inhalt Datenschutzerklärungen bereitgestellt wurden. Auch Pflichten gerichtet auf nachträgliche Maßnahmen, die Diensteanbieter, ähnlich einem abgestuften *notice and takedown*-Verfahren, bei Bekanntwerden von Verstößen im Rahmen ihrer Präsenz auf der Plattform sanktionieren, erscheinen denkbar. So könnten erkennbar datenschutzwidrig handelnde Diensteanbieter in Distributionskanälen weniger sichtbar gemacht werden, sodass sie in Suchergebnissen niedriger gelistet werden, während sich durch zuverlässige oder gar überobligatorische Bemühungen um Datenschutz auszeichnende An-

[64] Die Auswirkungen solcher Entscheidungen auf mitunter ganze Branchen lassen sich einmal mehr gut am Beispiel Apple verdeutlichen. Durch Anstrengungen, Nutzern von iOS mehr und präzisere Möglichkeiten zur Limitierung des Zugriffs auf Standortdaten an die Hand zu geben, sowie durch die generelle Beschränkung des Zugriffs auf bloß Daten geringerer Qualität (im Sinne von geringerer Aussagekraft und Genauigkeit) wurden insbesondere Datenflüsse an Adtech- und Datenbrokerunternehmen massiv eingeschränkt. Siehe *Malcolm Owen*, App tracking alert in iOS 13 has dramatically cut location data flow to ad industry, AppleInsider vom 13.01.2020 (https://appleinsider.com/articles/20/01/13/app-tracking-alert-in-ios-13-has-dramatically-cut-location-data-flow-to-ad-industry). Zuletzt abgerufen am 14.01.2022.

[65] Vgl. auch *Eifert*, NJW 2017, 1450 (1450), nach dem sie als Intermediäre einen „relativ effektiven Ansatzpunkt für den regulatorischen Zugriff in dem durch seine Unübersichtlichkeit und Fragmentierung sonst nur schwer adressierbaren digitalen Kommunikationsraum" darstellen.

bieter höher gerankt werden. Je nach Schwere, Offensichtlichkeit und Dauerhaftigkeit des infrage stehenden Verstoßes kämen hier unterschiedlich schwere Sanktionen in Betracht. *Ultima ratio* wäre hier sicherlich der völlige Ausschluss aus der Plattform, bei besonders schwerwiegenden Verstößen ggf. verbunden mit der Löschung bereits installierter bzw. genutzter Apps auf Nutzerendgeräten.[66]

Nicht zu vernachlässigen ist dabei zudem die Tatsache, dass viele dieser Ausgestaltungsentscheidungen von Plattformbetreibern als Teile ihrer *boundary resources*, wenngleich in variierender Form und Kontrolltiefe, sowieso getroffen werden. Entsprechende Pflichten zur normativ angeleiteten und reflektierten Steuerung und Änderung dieser *resources* würden daher aus pragmatischer Betrachtungsweise schon deshalb den bestehenden Fähigkeiten der Plattformbetreiber entsprechen, weil diese in vielen Fällen bloß Anpassungen von Prozessen vornehmen müssten, die ohnehin existieren, was effizienter erscheint, als vollkommen neue Handlungen zu verlangen.

bb) Kompensation bestehender Defizite

Unter diesen Stichpunkt fallen Erwartungen an den Plattformbetreiber, im Falle seiner Verantwortlichkeit durch das Nachkommen seiner Pflichten mittelbar einerseits die oben aufgezeigten Defizite der Grundprämissen der datenschutzrechtlichen Verantwortlichkeit abzumildern und andererseits dafür zu sorgen, dass die in Kapitel 2 festgestellten Kontrollverluste insbesondere der Diensteanbieter in Teilen kompensiert werden.

Hier lässt sich zunächst anführen, dass Plattformbetreiber ob ihres naturgemäßen Überblicks über und Einblicks in die auf der Plattform agierenden Akteure einen Wissens- und Transparenzvorsprung gegenüber Betroffenen, aber auch Aufsichtsbehörden haben, wenn es um das Handeln von Diensteanbietern und Drittparteien auf der Plattform geht. Durch die regelmäßig vor Aufnahme auf die Plattform erfolgende Überprüfung der aufnahmeersuchenden Dienste und Apps können grundlegende Parameter wie die verlangten Datenzugriffe oder die einbezogenen Drittparteien bereits überprüft werden. Gleiches gilt für einzelne Datenerhebungen durch Diensteanbieter und Drittparteien, die von Plattformbetreibern grundsätzlich protokolliert werden können. Eine Normierung von Pflichten zu solchen Protokollierungen und zur Auskunft gegenüber Aufsichtsbehörden, aber auch Diensteanbietern selbst, hinsichtlich der Aktivitäten der von ihnen genutzten Drittparteien, könnte bestehende Transparenzdefizite abmildern.

[66] So bereits vorgenommen von Google, siehe *Claudine Beaumont*, Google remotely deletes Android apps, The Telegraph vom 25.06.2010 (https://www.telegraph.co.uk/technology/google/7854560/Google-remotely-deletes-Android-apps.html). Zuletzt abgerufen am 14.01.2022.

Auch die Stellung der Nutzer (und damit potenziellen Betroffenen) kann durch erhöhte Transparenz, aber auch verstärkte Möglichkeiten zur Einflussnahme unterstützt und abgesichert werden. Transparenzfördernd auswirken können sich etwa zwingende Anforderungen an die Ausgestaltung, Verständlichkeit und Art der Anzeige von Datenschutzerklärungen oder klarere Vorgaben bzgl. des Aufzeigens von Drittparteien und ihren verfolgten Zwecken und geplanten Verarbeitungen. Beispiele für Maßnahmen zur Steigerung der Nutzerkontrolle finden sich in der jüngeren Vergangenheit gleich mehrfach. Der Übersichtlichkeit halber soll hier abermals auf Apple und Google mit den dazugehörigen mobilen Plattformen iOS und Android eingegangen werden. Durch zahlreiche Veränderungen daran, wie feingranular Nutzer in den Abruf bestimmter Datenkategorien einwilligen können (von dem ursprünglichen pauschalen systemweiten Ein- und Ausschalten der jeweiligen Sensoren wie GPS und Bluetooth über pauschale Berechtigungen für einzelne Apps bis hin zu den heute üblichen Optionen, die Mittelwege[67] wie die einmalige Erlaubnis oder die auf den Abruf bei aktiver Nutzung der App beschränkte Erlaubnis vorsehen),[68] wie sie die für den ordnungsgemäßen Betrieb einer App notwendigen Berechtigungen und geplanten Verarbeitungen und Zusammenführungen von Daten vor der ersten Nutzung angezeigt bekommen[69] oder wie sie im Falle von Apple eine vom Plattformbetreiber selbst angebotene datenschutzfreundliche *single sign-on*-Methode[70] nutzen können, um nicht auf datenhungrige Plugins von Google oder Facebook zurückgreifen zu müssen, wurde die Kontrolle von Nutzern teils weitreichend gestärkt, was bereits messbare Auswirkungen mit sich brachte.[71]

Auch eine Unterstützung der Diensteanbieter bei deren Erfüllung der ihr eigenen Pflichten ist als Effekt einer Inpflichtnahme von Plattformbetreibern denkbar. Neben der bereits genannten Verengung von Handlungsräumen zum

---

[67] So erlaubt Apple neuerdings sogar die Auswahl, ob einer App der genaue oder bloß der approximierte Standort mitgeteilt werden soll. Vgl. *Benjamin Mayo*, iOS 14 lets users grant approximate location access for apps that don't require exact GPS tracking, 9to5mac vom 12.08.2020 (https://9to5mac.com/2020/08/12/ios-14-precise-location/). Zuletzt abgerufen am 14.01.2022.

[68] Zur Evolution des Berechtigungsmanagements unter Android siehe etwa *Alepis/Patsakis*, in: Ali/Danger/Eisenbarth, Security, Privacy, and Applied Cryptography Engineering, S. 53 (53 ff.).

[69] Siehe *Nick Statt*, Apple launches new App Store privacy labels so you can see how iOS apps use your data, The Verge vom 14.12.2020 (https://www.theverge.com/2020/12/14/22174017/apple-app-store-new-privacy-labels-ios-apps-public). Zuletzt abgerufen am 14.01.2022.

[70] Siehe hierzu *Lily Hay Newman*, ‚Sign In With Apple' Protects You in Ways Google and Facebook Don't, Wired vom 04.06.2019 (https://www.wired.com/story/sign-in-with-apple-sso-google-facebook/). Zuletzt abgerufen am 14.01.2022.

[71] Vgl. erneut *Malcolm Owen*, App tracking alert in iOS 13 has dramatically cut location data flow to ad industry, AppleInsider vom 13.01.2020 (https://appleinsider.com/articles/20/01/13/app-tracking-alert-in-ios-13-has-dramatically-cut-location-data-flow-to-ad-industry). Zuletzt abgerufen am 14.01.2022.

Zwecke der Erschwerung oder Verunmöglichung datenschutzwidriger Verhaltensweisen wären unter diesem Stichwort auch konstruktive Unterstützungsleistungen, etwa beim Anfertigen von Verzeichnissen von Verarbeitungstätigkeiten gem. Art. 30 Abs. 1 S. 1 DSGVO oder hinsichtlich der Schaffung einer generellen Sensibilität für datenschutzfreundliche Gestaltungen[72], ein weiterer möglicher Weg.[73]

Auch hier ist zudem erneut zu konstatieren, dass ein Großteil dieser kompensierenden Maßnahmen bereits existierenden *boundary resouces* entspräche, wie die genannten Beispiele um Googles und insbesondere Apples Plattformen zeigen.

cc) Zwischenergebnis

Es lässt sich festhalten, dass Plattformbetreiber ob ihrer herausgehobenen Machtposition gegenüber den auf ihrer jeweiligen Plattform aktiven Diensteanbietern und Drittparteien strukturell in der Lage wären, die mit ihrer Inpflichtnahme einhergehenden Pflichten wirksam zu erfüllen und gleichzeitig, bei entsprechender Ausgestaltung dieser Pflichten, zu einer Kompensation der durch die Akteurskonstellationen heraufbeschworenen Defizite beizutragen.

Solche kompensationsfördernden Effekte könnten unmittelbar durch materielle Pflichten und mittelbar durch deren Effekte das Verhalten der Diensteanbieter und der von ihr einbezogenen Drittparteien betreffen, indem diesen gegenüber datenschutzkonformes Verhalten unmittelbar durchgesetzt bzw. „erzwungen“ wird, wenn eine kursorische Überprüfung der Konformität der einzelnen Akteure durchgeführt und konstruktive Unterstützung bei aktiven Datenschutzbemühungen geleistet wird und (bspw. ökonomische) Anreize zu konformem oder überobligatorischem Handeln gesetzt werden. Dies kann zu einer Verringerung des insbesondere nach erstmaligem Einbezug auftretenden Macht- und Informationsungleichgewichts zwischen Diensteanbietern und Drittparteien[74] beitragen. Plattformbetreiber können aber auch aktiv Transparenz- und Kontrolldefizite bei Betroffenen und Aufsichtsbehörden verringern, indem sie ihre eigenen tiefreichenden Einsichtsmöglichkeiten nutzbar machen und in Teilen zur Verfügung stellen.

Diese Fähigkeit der Plattformbetreiber verdeutlichen die von ihnen genutzten *boundary resources* in zweierlei Hinsicht: durch ihre reine Existenz und

---

[72] Vgl. hinsichtlich einer solchen Aufklärungsrolle *Greene/Shilton*, New Media & Society 2018, 1640 (1642): „Developers learn what privacy means through their everyday work practices, as they interact with iOS or Android's technical features, its human representatives, and other developers working through similar products and problems.“

[73] Hier müsste freilich Wert darauf gelegt werden, dass derartige Unterstützungsleistungen nicht dazu führen, dass Plattformbetreiber ihrerseits Zugriff auf mehr Nutzerdaten erlangen. Zu dieser grundlegenden Problematik ausführlich *infra* bei D. IV. 3.

[74] Siehe dazu *supra* bei Kapitel 1 B. I.

Charakteristik als plattformweit Geltung beanspruchende und Handlungsräume ermöglichende wie begrenzende Gestaltungsentscheidungen, aber auch durch die Tatsache, dass viele von ihnen konkret bereits existieren und durch entsprechende Pflichten „nur" im Detail verändert, also bspw. verschärft werden müssten. Doch auch dort, wo noch keine entsprechende Ressource existiert, zeigen die in Kapitel 1 gewonnenen Erkenntnisse, dass Plattformbetreiber die strukturelle Befähigung aufweisen, solche auf Basis emergent aufkommender und sich teils dynamisch entwickelnder Notwendigkeiten neu zu gestalten und kontinuierlich nachzujustieren.[75] Pflichten, die hier auf Neugestaltung von *boundary resources* gerichtet wären, würden sich daher grundsätzlich organisch in das bestehende System an externen und internen Einflüssen einfügen, das die Ausgestaltungsentscheidungen der Plattformbetreiber prägt.[76]

b) Diensteanbieter

Als zweite typisierte Akteursgruppe, die zusätzlich in die Pflicht genommen werden könnte, kommen einzelne Diensteanbieter in Betracht. Hinsichtlich der von ihnen selbst, gewissermaßen „eigenhändig" und zu eigenen Zwecken verarbeiteten Daten bedarf es keiner neuen Inpflichtnahme – hier besteht bereits jetzt eine datenschutzrechtliche Verantwortlichkeit und, mit dem eben Gesagten, ggf. eine zusätzliche Verantwortlichkeit eines Plattformbetreibers. Relevant ist hier hingegen eine etwaige Verantwortlichkeit mit Pflichten, deren Anknüpfungspunkt die von einbezogenen Drittparteien vorgenommenen Datenverarbeitungen sind. Da hier eine sehr große strukturelle Ähnlichkeit zu den vom EuGH in seiner Fashion ID-Entscheidung festgehaltenen Kriterien[77] besteht – Ermöglichung der Verarbeitung(en) eines dritten Akteurs durch dessen bewusste Einbindung bei damit einhergehenden Vorteilen für beide Parteien – und nach hier vertretener Ansicht die dort erfolgte Auslegung auch auf die Konstellation zwischen Diensteanbietern und Drittparteien anwendbar ist,[78] orientiert sich dieser Abschnitt lose an den vom Gerichtshof vorgenommenen Ausführungen.

aa) Eigene materielle Pflichten

Da der EuGH sich zumindest einige Gedanken zu der Frage, welche Pflichten einen Websitebetreiber oder (in etwas abgewandelter Form) den Betreiber einer Facebook-Fanpage treffen, gemacht hat, kann sich dieser Abschnitt zunächst auf konkretere Pflichten beziehen, als dies vorangehend für Plattformbetreiber

---

[75] Siehe dazu *supra* bei Kapitel 1 B. II. 1.

[76] Vgl. hierzu, sehr instruktiv die verschiedenen Einflusssphären aufzeigend *Ghazawneh/Henfridsson*, Governing third-party development through platform boundary resources, S. 13 f.; *dies.*, Information Systems Journal 2013, 173 (176 f.).

[77] EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 75, 80.

[78] Siehe die Ausführungen in Kapitel 2 C. II. 4. c).

der Fall war. Da die vom EuGH gemachten Ausführungen aber erstens nicht abschließend sind und zweitens noch zu klären sein wird, ob die Anwendung der gemeinsamen Verantwortlichkeit auf Diensteanbieter nicht nur der EuGH-Dogmatik nach *de lege lata* notwendig, sondern auch hinreichend zielführend ist, sollen aber auch darüber hinausgehende Gedanken angestellt werden.

Blickt man auf die Ausführungen des EuGH und die in der Rezeption des Urteils als zentral angesehenen Punkte, zeigt sich eine Dichotomie: Website- und Fanpage-Betreiber haben zwar zu Beginn eine weitreichende Handlungsmacht, wenn sie die Entscheidung für oder gegen den Einbezug eines bestimmten Plugins oder die Eröffnung einer Fanpage treffen. Ist diese Entscheidung aber erst einmal getroffen, liegt die Handlungsmacht allein bei der einbezogenen Drittpartei und besteht kein Einfluss des Betreibers mehr auf das datenverarbeitungserhebliche Verhalten – Daten können ohne sein Zutun durch die Drittpartei unmittelbar beim Nutzer erhoben werden. Durch die technische Realisierung mittels vorgefertigter Plugins ist eine Einflussnahme darauf, welche Daten unter welchen Umständen und in welchem Ausmaß verarbeitet werden, nur sehr begrenzt möglich. Gleiches gilt für vorherige Verhandlungen, da die Bedingungen – jedenfalls in den stets Facebook als besonders mächtigen Akteur betreffenden EuGH-Urteilen – typischerweise einseitig gestellt werden und den Betreiber so in eine *take it or leave it*-Situation versetzen.

Abgesehen vom in diesen Fällen besonders virulenten Machtgefälle treffen dieselben Überlegungen auch auf die hier in den Blick genommenen auf Plattformen aktiven Diensteanbieter im Verhältnis zu den von ihnen einbezogenen Drittparteien zu. Die Möglichkeit nachträglicher Einflussnahme ist hier im Zweifel als noch geringer zu bewerten, weil insbesondere der Einbezug von SDKs in Apps dazu führt, dass die gleichen Zugriffsmöglichkeiten auf Nutzerdaten bestehen, die auch der jeweiligen App offenstehen.[79] Eine wirksame Fähigkeit, die Nutzung dieser Zugriffsmöglichkeit zu kontrollieren oder überhaupt zu bemerken, besteht nicht. Einzig im Vorfeld könnten auf vertraglicher Ebene klare Grenzen definiert werden, deren Überschreiten mit Vertragsstrafen oder Ähnlichem sanktioniert werden könnte. Ihre Durchsetzung erfordert wiederum Kenntnis von möglichen Verstößen, die mangels Transparenz schwer zu erlangen sein dürfte. Hier könnte die im vorangegangenen Abschnitt beschriebene transparenzfördernde Fähigkeit von Plattformbetreibern ein mögliches Kompensationsmittel sein.

Da der EuGH in seinen Urteilen eine gemeinsame Verantwortlichkeit im Rahmen der bestehenden Möglichkeiten der DSGVO annahm, kommen grundsätzlich die existierenden Verantwortlichenpflichten in Betracht. Diese sind jedoch klassischerweise insofern auf *eigene* Datenverarbeitungen bezogen, als der pflichtige Akteur für viele von ihnen Zugriff auf die Daten sowie weit-

[79] Siehe dazu ausführlich *supra* in Kapitel 1 A. I. 2. und in diesem Kapitel bei A. I. 1.

gehende Kontrolle und umfassendes Wissen benötigt: Kontrolle über die verfolgten Zwecke, die ergriffenen Sicherheitsmaßnahmen und die Art und Weise der Speicherung, Wissen über Verarbeitungsumfang, Datenflüsse und etwaige Risiken. Dass der EuGH nun explizit keinen Zugriff auf die infrage stehenden Daten mehr voraussetzt, entspricht zunächst insofern der bereits immer bestehenden Dogmatik, als die Fremdspeicherung auch in Fällen der Auftragsverarbeitung nichts an der Verantwortlichkeit ändert. Im Unterschied zu jenen Fällen ist der Einfluss eines gemeinsamen Verantwortlichen aber generell – und insbesondere in den hier beschriebenen Fällen – weitaus geringer und ungleichmäßiger, da der gegenpolige Mitverantwortliche seinerseits ebenfalls Einfluss ausübt, und zwar regelmäßig stärker und mit größerer Nähe zu den betroffenen Daten. Dieser Tatsache trug der EuGH in seinen Urteilen insofern Rechnung, als er generell auf die Notwendigkeit abstellte, stets anhand der Spezifika des Einzelfalls zu beurteilen, wie die gemeinsamen Verantwortlichen im Rahmen ihrer Vereinbarung gem. Art. 26 Abs. 1 S. 2 DSGVO die verschiedenen Pflichten untereinander aufgeteilt haben. Letztlich, so der EuGH, käme es aber darauf an, wer welche Pflichten *faktisch* durch nähere Beteiligung am jeweiligen Verarbeitungsprozess überhaupt oder besser erfüllen könne,[80] sodass privatautonome Vereinbarungen nur solange wirksam seien, wie sie diese Realität widerspiegeln.[81] *In concreto* bezog der EuGH allein Stellung zu der Informationspflicht gegenüber dem Betroffenen gem. Art. 13 f. DSGVO, die in den vorliegenden Fällen nicht erfüllt worden war und deren Erfüllung dem EuGH zufolge dem jeweiligen Betreiber kraft seiner unmittelbaren Kommunikation mit dem Betroffenen obliegen hätte.[82] Dass auch die Erfüllung dieser Pflicht vom Betreiber, aber auch von anderen Diensteanbietern, nicht aus eigener Kraft heraus möglich ist, sondern von der Mithilfe Facebooks[83] bzw. möglicher Drittparteien abhängt, macht die Problematik offensichtlich.

Bei näherer Betrachtung der restlichen Pflichten wird offenbar, dass auch nur ein Bruchteil dieser daneben überhaupt in Betracht kommt. Die meisten Pflich-

---

[80] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 102 f.

[81] Siehe ebenfalls EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 102 f., wonach nur dann von einer „wirksamen und rechtzeitigen Wahrung der Rechte der betroffenen Person" ausgegangen werden könne. Dies ergibt sich genau genommen auch schon unmittelbar aus Art. 26 Abs. 2 S. 1 DSGVO.

[82] Daneben stellte der EuGH auch klar, dass jeder Verantwortliche eine eigenständige Rechtsgrundlage für die Verarbeitung, vorliegend also ein jeweils eigenes berechtigtes Interesse iSv Art. 6 Abs. 1 lit. f DSGVO benötigt, sodass hier genau genommen eine weitere den Betreiber treffende Pflicht zu sehen ist. Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 97.

[83] Hier kann einmal mehr darauf verwiesen werden, dass die von Facebook bereitgestellten Informationen iSd Art. 26 DSGVO, die unter anderem dem hier beschriebenen Zweck dienen sollen, nach behördlicher Ansicht nicht den gesetzlichen Ansprüchen genügen. Vgl. *Datenschutzkonferenz (DSK)*, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit.

ten knüpfen, wie bereits geschildert, an die Einflussnahme auf die unmittelbare Verarbeitungsumgebung an.[84] Während ein Websitebetreiber wie im Fashion ID-Urteil einen Teil dieser Umgebung – namentlich seine Website – selbst gestaltet, ist die eigentlich relevante Umgebung – namentlich das Plugin – eine Art fremdbeherrschte Insel, die ihre eigene Umgebung darstellt. Noch stärker gilt dies für Fanpage-Betreiber wie im Wirtschaftsakademie-Urteil, bei der letztlich die genutzte Infrastruktur in ihrer Gänze von Facebook beherrscht wird, aber auch für Diensteanbieter auf anderen Plattformen, bei denen zur Insel der Drittpartei noch hinzu kommt, dass die übrige Umgebung gewissermaßen vom Plattformbetreiber „geliehen" ist und dessen Regeln unterliegt.

Denkbar erscheint daher allein die Anwendung besonders abstrakter, in ihrer Zielrichtung in Teilen vom Einzelfall abhängiger Pflichten wie der zur Ergreifung von *privacy by design*-Maßnahmen gem. Art. 25 Abs. 1 DSGVO, die hier darauf gerichtet sein könnten, den Einbezug des Dritten oder die Nutzung der fremden Infrastruktur im Rahmen der eigenen Möglichkeiten inhärent datenschutzfreundlicher zu gestalten. Wie genau eine solche Gestaltung unter den beschriebenen Einflussgrenzen aussehen könnte, erscheint aber wiederum fraglich. Letztlich gelangt man erneut zum Ausgangspunkt einer begrenzten Kontrolle und Verhandlungsmacht, die die wirksame Erfüllung existierender DSGVO-Pflichten für Diensteanbieter schwer bis unmöglich macht. Ob diese ob ihrer Abstraktheit im Einzelfall so skaliert und angepasst werden können, dass – nicht zuletzt durch Unterstützung von Plattformbetreibern – doch noch wirksame Beiträge möglich werden, soll unten im Abschnitt zur Weiterentwicklung der gemeinsamen Verantwortlichkeit (C.) erörtert werden.

bb) Kompensation bestehender Defizite

Aufgrund der geringen Eignung zur Erfüllung eigener materieller Pflichten liegt ein umso größeres Augenmerk auf der Frage, ob ein Handeln von Diensteanbietern denkbar erscheint, welches die bestehenden Defizite insbesondere der zur Durchsetzung berufenen Akteure gegenüber Drittparteien teilweise zu kompensieren vermag. Diese Überlegung entspricht der oben hergeleiteten Interpretation dessen, was der EuGH sich von der Inpflichtnahme faktisch nur bedingt mächtiger und entscheidungsfähiger Akteure erhofft haben mag: Nicht die Fähigkeit zur Erfüllung einzelner materieller Pflichten steht letztlich im Vordergrund, sondern der Druck, der damit auf ansonsten schlecht greifbare Akteure – in den EuGH-Fällen konkret Facebook – ausgeübt werden kann.[85] So wie das Fazit bereits beim Resümee zu der entsprechenden Entscheidung eher gemischt

[84] So etwa die Pflichten zur Implementierung technischer und organisatorischer Maßnahmen zur Datensicherung gem. Art. 32 Abs. 1 bzw. zur Sicherstellung der Einhaltung der Datenschutzgrundsätze gem. Art. 25 Abs. 1, aber auch die Pflicht zur Anfertigung eines Verarbeitungsverzeichnisses gem. Art. 30 Abs. 1 DSGVO.

[85] Siehe die Analyse der EuGH-Urteile in Kapitel 2 C. II. c) cc) sowie die prägnanten

ausfiel, muss auch hier konstatiert werden, dass der Spagat zwischen der Inpflichtnahme nur begrenzt handlungsfähiger Akteure einerseits und der damit verbundenen Erwartung weitreichender Auswirkungen andererseits schwierig zu bewerkstelligen sein dürfte. Erschwerend hinzu kommt, dass es hier in Abgrenzung zu den EuGH-Fällen nicht um einen einzelnen, großen Akteur geht, sondern um eine unüberschaubare Menge von Drittparteien, mithin also um eine verfestigte Praxis und ein breites, etabliertes Geschäftsmodell mit vielzähligen ähnlich agierenden Akteuren. Zu hoffen, die Inpflichtnahme von Diensteanbietern mitsamt der Androhung von Haftung und Sanktionen könnte diese zum Verzicht der Nutzung datenschutzwidriger Drittparteien bewegen und jene dadurch mittelbar zu datenschutzkonformem Handeln „zwingen", wäre daher aus zwei Gründen verfehlt: aufgrund der verfestigten Praxis, die bisher kaum gangbare Alternativen bereithält,[86] sowie aufgrund der Menge, Heterogenität und Intransparenz der Drittparteien. Da Drittanbieter zu unterschiedlichsten Zwecken eingebunden werden[87] und da ob ihres gerade kumulativ kaum zu überblickenden (Verarbeitungs-)Handelns kaum festzustellen ist, wer von ihnen sich datenschutzkonform verhält und wer als „schwarzes Schaf" agiert, werden Diensteanbieter regelmäßig nicht in der Lage sein, ihr Handeln selbst bei besten Absichten entsprechend auszurichten und bspw. den Einbezug „schwarzer Schafe" zu vermeiden, Betroffene umfassender und früher zu informieren oder Aufsichtsbehörden bei ihren Kontrollbemühungen zu unterstützen.

Ohne externe Mechanismen ist demnach nur begrenzt zu erwarten, dass Diensteanbieter infolge ihrer Inpflichtnahme eigenständig in der Lage sind, bestehende Defizite hinsichtlich der Kontrolle von Drittanbietern sowie der Handlungs- und Kontrollfähigkeit von Betroffenen und Aufsichtsbehörden zu kompensieren. Ein denkbarer Ansatz könnte sich aber aus der im vorangegangenen Abschnitt beschriebenen Rolle der Plattformbetreiber ergeben. Würden diese zielgerichtet als Verantwortliche in die Pflicht genommen, könnte so eine unmittelbare Defizitkompensierung durch Befähigung von Diensteanbietern erreicht werden, indem etwa bereits auf Plattformebene (z. B. bei Aufnahme in den entsprechenden Distributionskanal) eine Durchleuchtung der einbezogenen Drittanbieter (ggf. verbunden mit einem Abgleich mit einer Liste bereits bekannter „schwarzer Schafe") vorgenommen oder die später von diesen vorgenommenen Datenerhebungen protokolliert und den Diensteanbietern mitgeteilt werden. Dies könnte eine weitere, mittelbare, Defizitkompensierung bedingen, indem derart unterstützte Diensteanbieter – gewissermaßen „zu ihrem Glück gezwungen" – ihre hinzugewonnenen Einblicke und Handlungs-

---

Ausführungen von *Globocnik*, IIC 2019, 1033 (1042), der treffend von „enforcement against Big Tech by the back door" spricht.

[86] Wie es auch für Unternehmen, Vereine und andere werbende Akteure kaum ernsthafte Alternativen gibt, die eine ähnliche Reichweite wie Facebook bieten können.

[87] Siehe hierzu die Erläuterung *supra* bei Kapitel 1 A.

möglichkeiten im Rahmen ihres Verhältnisses gegenüber Nutzern (sowie ggf. Aufsichtsbehörden) fruchtbar machen und zugunsten eines bewussteren Auswahlprozesses von Drittparteien einfließen lassen könnten. Ist eine solche reflexive Wirkung von Verantwortlichkeiten regulatorisch abgesichert – und nur, wenn dies sichergestellt ist – kann auch bzgl. der eigenen Verantwortlichkeit von Diensteanbietern darüber nachgedacht werden, Pflichten zu etablieren, die konkrete Anforderungen an die Sorgfalt stellen, die bei der Auswahl von Drittanbietern an den Tag gelegt wird.

cc) Zwischenergebnis

Die Fähigkeit von Diensteanbietern zur Pflichtenerfüllung hängt stark mit ihrer nur begrenzten Entscheidungsmacht zusammen. Da diese sich häufig in der Entscheidung *pro* oder *contra* Einbeziehung einer konkreten Drittpartei erschöpft, liegt jedenfalls eine generelle Befähigung zur sorgfältigen Auswahl von Drittparteien vor. Gleichzeitig mangelt es Diensteanbietern an der nötigen Transparenz und Verhandlungsstärke, um auch nach dieser einmaligen Entscheidung Drittanbieter zu kontrollieren und ggf. zu sanktionieren sowie Nutzer tiefgreifend zu informieren und ggf. zu warnen. Vertragliche Limitierungen sind möglich, ihre Durchsetzung ist aber zweifelhaft. Hinzu kommt, dass es vielen Diensteanbietern bei sehr geringer Aufdeckungswahrscheinlichkeit und entsprechend geringen Haftungsrisiken regelmäßig am nötigen Normbefolgungswillen mangeln dürfte.[88]

Die tatsächliche Fähigkeit ist daher grundsätzlich gegeben, hängt aber in ihrer Reichweite in starkem Maße von externen Mechanismen ab. Ein solcher Mechanismus könnte die Inpflichtnahme von Plattformbetreibern mit der teilweisen Zielrichtung einer Unterstützung der Diensteanbieter sein. So könnte ebenfalls sichergestellt werden, dass die Inpflichtnahme der Letztgenannten auch weitergehende Defizite etwa auf Seiten der Nutzer und Aufsichtsbehörden teilweise kompensiert.

2. Zurechnungstatbestände

Eine besondere Befähigung zur Pflichtenerfüllung allein kann, mit Blick auf mögliche Sanktionen und Haftungsrisiken, regelmäßig nicht ausreichen, um die Belastung eines privaten Akteurs mit Pflichten zu legitimieren. Ist, wie hier, das Ziel der Inpflichtnahme der Schutz Betroffener, bedarf es zudem eines hinreichenden Zurechnungstatbestands: einer Verknüpfung zwischen dem Handeln oder eines sonstigen aus der „Sphäre“ des in die Pflicht zu nehmenden Akteurs stammenden Impulses einerseits und der Gefahren, vor denen Betroffene geschützt werden sollen, andererseits:

[88] Siehe hierzu *supra* in Kapitel 2 B. II. 4. sowie grundlegend bei *Hoffmann-Riem*, Innovation und Recht, Recht und Innovation, S. 142 ff.

„Die Inanspruchnahme Privater zur Erfüllung öffentlicher Aufgaben bedient sich also der Zurechnung als Rechtfertigung: Negatives Vorverhalten und/oder positive Folgen sollen die Inanspruchnahme rechtfertigen."[89]

Aus dem zumindest oberflächliche Ähnlichkeiten zum Datenschutzrecht aufweisenden[90] allgemeinen Gefahrenabwehr- und Polizeirecht bekannt ist etwa das Anknüpfen an das gefahrenverursachende Handeln oder Unterlassen (sog. Handlungs- oder Verhaltensstörer[91]) und die Sachherrschaft über eine gefahrenverursachende Sache (sog. Zustandsstörer[92]).[93] Auch hier sind die Überlegungen zu einem gewissen Grad noch abstrakt, da die Frage der genauen Verantwortlichkeit sowie der Ausgestaltung und Reichweite ihrer Pflichten erst später geklärt werden soll. Klar ist aber bereits, dass es um die Frage der gegenseitigen Zurechnung verschiedener Beiträge unterschiedlicher Akteure (Plattformbetreiber, Diensteanbieter, Drittpartei) geht und die jeweilige Verantwortlichkeit Pflichten beinhalten wird, die reflexiv aufeinander bezogen sind und sich in ihrer Wirkung gegenseitig unterstützen und verstärken sowie positive Externalitäten für unter anderem die zur Rechtsdurchsetzung aufgerufenen Akteure (Betroffene, Aufsichtsbehörden) zeitigen sollen.[94]

a) Klassische Zurechnung im Datenschutzrecht

Der Zurechnungstatbestand des datenschutzrechtlichen Verantwortlichen knüpft diesbezüglich an den konkreten Vorgang bzw. die konkrete Vorgangsreihe[95] der Datenverarbeitung an. Die unstrukturierte und ungeregelte Datenverarbeitung ist in der Dogmatik des Datenschutzrechts der Akt, dessen Durchführung, insbesondere aber dessen schwer abzusehende und in ihren Folgen weitreichend offene nachfolgende Handlungen und Entscheidungen, eine gewisse Gefahr zugeschrieben wird und daher rechtlich strukturiert und in geordnete Bahnen gelenkt werden soll.[96] Deshalb stellt Art. 4 Nr. 7 DSGVO zur Be-

---

[89] *Lennartz*, DÖV 2019, 434 (435); siehe auch *Hofmann*, JZ 2018, 746 (749), der in seiner Analyse von Tatbeständen mittelbarer Verantwortlichkeit ausführt: „Übergreifend findet sich also der Gedanke, dass nicht jede Handlung, die mit einer Rechtsverletzung in mehr oder weniger engem Zusammenhang steht, rechtlich zu missbilligen ist."

[90] So auch *Martini/Fritzsche*, NVwZ-Extra 2015, 1 (10 f.). Auch das BVerwG zog in seinem Urt. v. 11.09.2019, Az. 1 C 28.14 (Wirtschaftsakademie Schleswig-Holstein) Rn. 31 das Gebot einer „effektiven und wirkungsvollen Gefahrenabwehr" heran, um die Ermessensfehlerfreiheit der Maßnahme gegenüber der Wirtschaftsakademie zu begründen.

[91] Siehe etwa § 8 hambSOG, Art. 7 bayPAG, § 5 bbgPolG, § 6 bwPolG.

[92] Siehe etwa § 9 hambSOG, Art. 8 bayPAG, § 6 bbgPolG, §7 bwPolG.

[93] Vgl. *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 135.

[94] Siehe hierzu die vorangegangenen Ausführungen unter I und II. 1.

[95] Art. 4 Nr. 2 umfasst hier explizit auch die Vorgangsreihe, solange deren Vorgänge einen hinreichend engen Zusammenhang aufweisen. Vgl. *Roßnagel*, in: Simitis u. a., DSGVO/BDSG Art. 4 Nr. 2 DSGVO Rn. 11; *Herbst*, in: Kühling/Buchner, DSGVO/BDSG, Art. 4 Nr. 2 DSGVO Rn. 15.

[96] Vgl. *Marsch*, Das europäische Datenschutzgrundrecht, S. 269 sowie die Ausführungen *supra* in Kapitel 2 A. III.

stimmung des Verantwortlichen auf die Entscheidung über Zwecke und Mittel der Verarbeitung ab und formuliert (implizit) die erste Grundprämisse der Verantwortlichkeit, dass die DSGVO stets den zentralen und alle Umstände einer konkreten Verarbeitung oder Verarbeitungsreihe kennenden Akteur als Verantwortlichen qualifizieren muss.[97]

Neben diesen strukturellen Ähnlichkeiten zum Polizeirecht gibt es aber auch tiefgreifende Unterschiede: Der dortige Gefahrenbegriff ist weitaus enger als die – wie in Kapitel 2 A. erörtert – bloß sehr abstrakte und vorgelagerte Gefahr, die mit einer einzelnen, pauschalen Datenverarbeitung einhergeht und in diesem Stadium eher einem Risiko entspricht.[98] Zwar lässt auch das Polizeirecht für bestimmte Maßnahmen – insbesondere für Polizeiverordnungen – *abstrakte* Gefahren ausreichen; doch liegt hier ein anderes Verständnis der Abstraktheit zugrunde: Im Polizeirecht bezeichnet der Begriff in Abgrenzung zu einer im *Einzelfall* vorliegenden Gefahr eine Gefahr, die *generell* und nach allgemeiner Lebenserfahrung *typischerweise* durch eine Sachlage oder ein Verhalten verursacht wird.[99] Das geschützte Rechtsgut, dessen Gefährdung droht, muss hingegen in beiden Fällen bereits konkret feststehen.[100] Die Unterscheidung ist somit eine Frage der Allgemeinheit der Gefahr, nicht aber ihrer Intensität: „Die konkrete Gefahr ist nicht eine intensivere Gefahr als die abstrakte, sondern eine andere."[101] Im Datenschutzrecht hingegen ist die im Zusammenhang mit einer Datenverarbeitung entstehende Gefahr zunächst in der Hinsicht abstrakt, dass weder eine konkrete Eintrittswahrscheinlichkeit noch das im (generalisierten) Einzelfall bedrohte Schutzgut bereits konkret benannt werden kann. Dazu passt, dass der Verordnungsgeber die grundlegende Einschätzung des Vorliegens einer „Gefahr" (genauer: eines Risikos) bereits getroffen hat: Jede Verarbeitung personenbezogener Daten führt – das Vorliegen der restlichen Voraussetzungen des sachlichen und örtlichen Anwendungsbereichs vorausgesetzt – zur Anwendung der DSGVO. Im Polizeirecht hingegen muss das Vorliegen einer Gefahr, das heißt einer Situation, in der bei ungehindertem Ablauf des zu erwartenden Geschehens mit hinreichender Wahrscheinlichkeit eine Schädigung eines geschützten Rechtsguts zu erwarten ist,[102] aufgrund der Vielzahl unterschiedlichster Fälle und Szenarien stets im Einzelfall von der handelnden Behörde festgestellt werden.

---

[97] Vgl. dazu die Ausführungen *supra* bei Kapitel 2 B. II. 1.

[98] Dass das Vorliegen eines bloßen Risikos als Eingriffsschwelle ausreicht, wäre zwar im allgemeinen Polizeirecht unverhältnismäßig, kann aber in Spezialgesetzen grundsätzlich zulässig sein. Vgl. *Di Fabio*, JURA 1996, 566 (570 ff.).

[99] *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 115: „Die konkrete Gefahr bezieht sich also auf den Einzelfall, die abstrakte hingegen auf den typischen Fall."

[100] Vgl. *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 99: „[…] erst wenn das betroffene Schutzgut bestimmt wurde, kann festgestellt werden, ob für dieses eine Gefahr besteht."

[101] *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 116.

[102] Vgl. statt vieler *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 113; siehe auch den kurzen Abriss zur Geschichte des Begriffs m. w. N. bei *Heun*, RW 2011, 376 (377 f.).

Diese Unterscheidung setzt sich auch auf Rechtsfolgenebene fort: Wo das Polizeirecht im klassischen Sinne Störer durch konkrete Maßnahmen dazu verpflichtet, die von ihnen oder den unter ihrer Sachherrschaft stehenden Sachen ausgehende Gefahr abzustellen oder die polizeilich vorgenommene Abstellung hinzunehmen[103] sowie ggf. die entstandenen Kosten zu tragen[104], geht mit der datenschutzrechtlichen Verantwortlichkeit ein ganzes Bündel an Pflichten einher, das präventive Vorsorgepflichten ebenso beinhaltet wie das Hinnehmen von Untersagungs- und anderen Verfügungen in Fällen datenschutzrechtswidriger Praktiken.[105] Die polizeirechtliche Verantwortlichkeit als Störer betrifft daher richtiger Weise einzig die Pflicht zum Abstellen einzelner, gefahrenträchtiger Handlungen oder Zustände sowie ggf. zum Kostenersatz infolge behördlicher Inanspruchnahme,[106] während das Datenschutzrecht ubiquitäre, alltägliche Handlungen unabhängig von behördlichem Einschreiten rechtlich einrahmt und – trotz Ausgestaltung als Verbotsprinzip mit Erlaubnisvorbehalt – damit nicht zu ihrem Unterlassen, sondern zu ihrer möglichst risikoarmen und betroffenenfreundlichen Ausübung sowie zu einer entsprechenden Gestaltung der Verarbeitungsumgebung verpflichtet.[107] Der bereits vom Verordnungsgeber getroffenen Zuschreibung eines gewissen Risikos zur Verarbeitung personenbezogener Daten folgt daher nachgelagert im Rahmen der einzelnen Pflichten eine Risiko- und Gefahrenbeurteilung durch die Verantwortlichen selbst sowie durch Aufsichtsbehörden.[108] Diese kann dann je nach Ergebnis der Beurteilung unterschiedliche Handlungspflichten nach sich ziehen. Während also die polizeirechtliche Verantwortlichkeit eine simple Umschreibung für die legitime Inanspruchnahme durch Polizei- und Ordnungsbehörden ist, beschreibt die datenschutzrechtliche Verantwortlichkeit eine komplexe Pflichtenübertragung, die – bei Verstoß gegen Pflichten – eine Einzelfallinanspruchnahme sowie eine

---

[103] Vgl. *Schoch*, in: Schoch, Besonderes Verwaltungsrecht, S. 11 (15): „[…] Abwehr konkreter Gefahren für ein Schutzgut durch die Polizei- und Ordnungsbehörden mittels Maßnahmen, die an die Verantwortlichen der Gefahrenlage adressiert sind[…]."

[104] Siehe *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 389 ff. zu den Voraussetzungen dafür.

[105] Vgl. die Abhilfebefugnisse der Aufsichtsbehörden in Art. 58 Abs. 2 DSGVO sowie die diese betreffenden Ausführungen *supra* in Kapitel 2 B. I. 1. e) aa).

[106] Siehe *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 136; eine von Stimmen wie *Martensen*, DVBl 1996, 286 (286 f.) vertretene materielle Polizei- oder Nichtstörungspflicht, die auch vor Inanspruchnahme durch Ordnungsbehörden dazu verpflichten soll, aus dem eigenen Verhalten oder Zustand eigener Sachen keine Gefahren erwachsen zu lassen, stünde dieser Aussage nur scheinbar entgegen: Sie bezöge sich letztlich auch nur auf geltendes Recht und somit bereits existierende Pflichten.

[107] Zur Unterscheidung des Risikobegriffs im Rahmen der Verantwortlichtenpflichten einerseits und dem Polizeirecht andererseits siehe *Schröder*, ZD 2019, 503 (504 f.). Grundlegend zum risikobasierten Ansatz der DSGVO zudem *Gellert*, The risk-based approach to data protection.

[108] Vgl. *Schröder*, ZD 2019, 503 (503 ff.); *Gellert*, EDPL 2016, 481 (481 ff.) sowie die Ausführungen in Kapitel 2 B. I. 2. a) cc).

Haftung des Verantwortlichen nach sich ziehen kann. Sie ist damit gleichzeitig niedrigschwelliger (weil ihr Vorliegen noch keine Inanspruchnahme nach sich zieht) und umfassender (weil sie eine Vielzahl von, auch präventiv zu erfüllenden, Pflichten beinhaltet, die zu teils kostenintensiven Maßnahmen verpflichten) als die polizeirechtliche Verantwortlichkeit. Nichtsdestotrotz ist die Tür mit der erstmaligen Zurechnung einer Verarbeitung zu einem Akteur bereits unwiderruflich aufgestoßen. Die nachgelagerten Fragen des Ausmaßes der vom Verantwortlichen erwarteten Maßnahmen betreffen dann eben nur das Ausmaß, nicht die Existenz der Pflichtigkeit.[109] Trotz im Detail teils größerer Unterschiede bei der Begründung der Inpflichtnahme Verantwortlicher kann daher für das Datenschutzrecht, das nach hiesigem Verständnis ja in der Sache besonderes Gefahrenabwehr- bzw. Risikovorsorgerecht darstellt,[110] ein Abgleich mit den Zurechnungstatbeständen des allgemeinen Polizeirechts fruchtbar sein für die Beantwortung der Frage, welcher Maßstab für die Zurechnung bei der Erweiterung der Verantwortlichkeit anzulegen sein sollte.

Ähnlich wie ein Störer im Polizeirecht eine Gefahr *verursachen* muss, muss ein Akteur im Datenschutzrecht Daten *verarbeiten*, um als Verantwortlicher für die betreffenden Verarbeitungen zu gelten. Das führt leicht zu terminologischen Verwirrungen, weil das Substantiv der *Verarbeitung* einerseits den Gegenstand der Regulierung, andererseits aber auch die Verursachungshandlung des Verantwortlichen (indem dieser Daten verarbeitet) beschreibt. Verantwortlich ist ein Akteur also stets dann für Datenverarbeitungen, wenn *er* sie durchführt, die Datenverarbeitung also *seine* ist.[111] Versucht man sich mit dem oben in Kapitel 2 Erarbeiteten zu den Voraussetzungen der Verantwortlichkeit an einer Einordnung in die Systematik des Polizeirechts, so würde sich der datenschutzrechtliche Verantwortliche sowohl als Handlungs- als auch als Zustandsstörer beschreiben lassen. Eine eigene, die Verantwortlichkeit auslösende Verarbeitung ist gerade nicht nur in Form einer eigenen (oder gar eigenhändigen) Verarbeitung – die ja im Bereich des Digitalen und damit des stets nur mittelbaren Handelns durch Hilfsmittel hindurch ohnehin schwer zu definieren wäre –, sondern insbesondere auch durch Ausübung der Entscheidungs- oder Sachherrschaft möglich. Das wird schon anhand der Tatbestandsmerkmale in Form der Beeinflussung von *Zwecken* und *Mittel* der Verarbeitung deutlich. Ein besonders plastisches Beispiel hierfür ist die Möglichkeit des Einsatzes eines Auftragsver-

[109] Dass es keine weitreichende Skalierung von Verantwortlichenpflichten gibt, sondern alle Pflichten zunächst dem Grunde nach auf alle Verantwortlichen anwendbar sind, wurde *supra* bei Kapitel 2 C. II. 4. c) cc) erörtert.

[110] Siehe dazu ausführlich *supra* in Kapitel 3 A. III. In eine ähnliche Richtung gehend auch *Martini/Fritzsche*, NVwZ-Extra 2015, 1 (10 f.), die von Datenschutzrecht als Sonderordnungsrecht sprechen.

[111] Ausführlich zu den Voraussetzungen des Art. 4 Nr. 7 DSGVO, wonach der Verantwortliche die *Mittel* und *Zwecke* der Verarbeitung beeinflussen muss, um iSd DSGVO Daten zu verarbeiten, siehe *supra* bei Kapitel 2 C. II.

arbeiters, der eigenständig, aber weisungsgebunden die Verarbeitung *für* den Verantwortlichen vornimmt. Die Verarbeitung ist zudem das Bezugsobjekt der Verantwortlichkeit: Der Verantwortliche muss dafür Rechnung tragen, dass die Verarbeitung an sich rechtmäßig abläuft. Voraussetzung dafür ist, dass er eine Vielzahl an Pflichten erfüllt, die teilweise eng mit der Verarbeitung zusammen hängen und teilweise ihr Umfeld betreffen.[112]

Dieser Zurechnungstatbestand, der hinter der klassischen datenschutzrechtlichen Verantwortlichkeit steht, könnte auch die Ausweitung der Verantwortlichkeit auf Diensteanbieter legitimeren. Der für die Zurechnung nötige Verursachungszusammenhang bestünde dann darin, dass diese einen eigenständigen und ausreichenden Beitrag zur Verursachung einer Datenverarbeitung setzen. In diese Richtung lässt sich die Linie des EuGH interpretieren, nach der die *Ermöglichung* der Verarbeitung in Verbindung mit einer (irgendwie gearteten) Zweckkongruenz des näher an der Verarbeitung befindlichen Verantwortlichen für eine (gemeinsame) Verantwortlichkeit genügt.[113] Nach diesem Verständnis liegt also trotz offensichtlicher qualitativer Unterschiede auch in diesen Fällen eine hinreichende Nähe zur Datenverarbeitung als „Gefahrenquelle" vor, um die Inpflichtnahme zu legitimieren. Verantwortlich ist der Diensteanbieter dementsprechend gemeinsam mit dem Drittanbieter (so wie Fanpage- und Websitebetreiber in den EuGH-Urteilen) unmittelbar für die Datenverarbeitung, die sich als – *auch* – die Seine darstellt.[114] Die Verursachung der Datenverarbeitung in Verbindung mit der beschriebenen Zweckkongruenz ist daher bereits eine dem Grunde nach verbotene Handlung, die einer Rechtsgrundlage bedarf – wie auch der EuGH letztlich unmissverständlich klarstellt, indem er festlegt, dass gemeinsame Verantwortliche ihre Verarbeitungsbeiträge *jeweils* auf eigene Rechtsgrundlagen stützen können müssen, es also nicht genügt, dass der verarbeitungsnähere Verantwortliche eine solche vorweisen kann. Einer dogmatischen Modifikation oder Erweiterung des legitimierenden Zurechnungstatbestandes braucht es nach Ansicht des EuGH damit nicht. Eine griffige Definition der konkreten Schwelle des Verursachungszusammenhangs, der für die Zurechnung ausreicht, erlaubt dies wohlgemerkt nicht.[115] Anders als im Polizeirecht, wo zur Lösung dieser Frage vielerorts mit der Rechtswidrigkeitslehre darauf abgestellt wird, ob eine konkrete rechtliche Handlungs- oder Unterlassungspflicht verletzt wird,[116] kann hier der Blick in andere Rechtsgebiete

[112] Siehe zu den einzelnen Pflichten *supra* in Kapitel 2 B. I. 1.

[113] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 77 ff. Siehe außerdem die ausführlichen Ausführungen *supra* in Kapitel 2 C. II. 4. b).

[114] Daran ändert auch die Tatsache nichts, dass der EuGH explizit eine unterschiedliche Gewichtung bzw. unterschiedliche „Grade der Verantwortlichkeit" definiert und somit auf Ebene der einzelnen Pflichten und der konkreten Haftbarkeit letztlich anerkennt, dass auch bei eigenen Verarbeitungen eine Existenz von nur begrenzten Einflussmöglichkeiten denkbar ist.

[115] Siehe dazu bereits die Ausführungen in Kapitel 3 C. II. 4. d).

[116] Siehe hierzu ausführlich *Poscher*, Jura 2007, 801 (803 ff.).

keinen Erkenntnisgewinn bieten, da das Datenschutzrecht gerade nicht auf die restliche Rechtsordnung verweist, sondern vielmehr seine eigenen Maßstäbe aufstellt. Fraglich ist daher, ob andere Zurechnungstatbestände infragekommen, die klarere Grenzen setzen.

b) Parallelen zum Polizeirecht: Nichtstörer und Zweckveranlasser

Das Polizeirecht kennt neben dem Störer weitere Verantwortlichkeitsrollen, deren belastende Wirkung sich aus unterschiedlichen Anforderungen an Zurechnungstatbestände legitimiert.

Die umstrittene[117] Figur des *Zweckveranlassers* beschreibt einen Akteur, dessen Verantwortlichkeit sich daraus ergibt, dass er eine an sich neutrale Handlung vornimmt, die zurechenbar die nachfolgende Störung durch eine oder mehrere Handlungs- oder Zustandsstörer veranlasst.[118] Während die Handlung des Zweckveranlassers die für die Verantwortlichkeit notwendige Gefahrenschwelle also ihrerseits nicht überschreitet, steht sie in einem solch engen Zusammenhang mit dem unstreitig gefahrauslösenden Verhalten oder Zustand des unmittelbaren Störers, dass sie bei wertender Betrachtung als wesentlicher und ausschlaggebender Faktor für die Gefahrverursachung angesehen werden kann.[119] Dogmatisch wird die Figur damit verbreitet als Unterfall des Handlungsstörers verstanden.[120] Ob dadurch das nach herrschender Meinung zentrale Unmittelbarkeitserfordernis durchbrochen wird[121] oder nicht[122], ist bis heute umstritten. Ein prägnanter Beispielsfall, der im Zusammenhang mit dieser Figur diskutiert wird, ist die Verantwortlichkeit von Fußballvereinen für Gefahren durch rivalisierende Fangruppen sowie für die Kosten der Polizeiaufgebote, die als Reaktion darauf von Gemeinden aufgeboten werden müssen.[123] Auch aus dieser polizeirechtlichen Figur lassen sich grundlegende Überlegungen zu Zurechnungskriterien abstrahieren, die über das Polizeirecht hinausgehen.[124] So lässt sich der Gedanke einer Zurechnung unmittelbar gefahrträchtigen dritten Verhaltens zu einem auf den ersten Blick von dieser Gefahr weiter entfernten Akteur ebenfalls gut auf die beiden EuGH-Fälle und auf die Konstellationen von Diensteanbietern und Drittparteien übertragen. Während Dritt-

---

[117] Zu den breit diskutierten verfassungsrechtlichen Bedenken siehe etwa *Beaucamp/Seifert*, JA 2007, 577 (579 f.). Die Einwände gegen Notwendigkeit und Zulässigkeit der Figur systematisch adressierend und größtenteils überzeugend widerlegend *Lange*, Zweckveranlassung, S. 43 ff.

[118] *Schoch*, JURA 2009, 360 (361).

[119] Siehe statt vieler *Lange*, Zweckveranlassung, S. 16 f. m. w. N.

[120] Vgl. *Schoch*, JURA 2009, 360 (361).

[121] So etwa *Poscher*, JURA 2007, 801 (807); *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 145.

[122] So etwa *Schoch*, JURA 2009, 360 (361).

[123] Siehe hierzu ausführlich *Lange*, Zweckveranlassung, S. 23 ff.

[124] So auch *Lange*, Zweckveranlassung, S. 33 ff.

parteien unstrittig Daten als Verantwortliche verarbeiten, leisten Diensteanbieter nur einen vorgelagerten, zunächst neutralen Handlungsbeitrag in Form des Einbezugs dieser Drittparteien. Auch die Motivation hinter dem Bedürfnis einer zusätzlichen verantwortlichen Person ähnelt sich in beiden Konstellationen: dort eine zusätzlichen Akteur in Anspruch nehmen zu können, wo der unmittelbar Verantwortliche nicht, zu umständlich oder weniger erfolgversprechend in Anspruch genommen werden kann.[125] Gedanken zur unmittelbaren Anwendbarkeit der Figur des Zweckveranlassers als datenschutzrechtliche Verantwortlichkeitskategorie wurden im Vorfeld der Wirtschaftsakademie-Entscheidung des EuGH in der Literatur teilweise bereits angestellt.[126] Galt dort noch als Fazit, dass der abschließende Charakter der eigenständigen Verantwortlichkeitsregelungen des Datenschutzrechts eine solche unmittelbare Übertragung verbietet,[127] muss dies heute nicht absolut gelten. Zum einen geht es nicht um eine unmittelbare Anwendung der polizeirechtlichen Figur, sondern um eine Übertragung der dahinterstehenden Zurechnungsgedanken. Zum anderen ist die Ausgangslage eine andere: Ging es *Martini* und *Fritzsche* noch darum, vor dem Grundsatzurteil des EuGH einen dogmatisch gangbaren Weg zu finden, den betreffenden Fanpage-Betreiber trotz (vermeintlich) fehlender datenschutzrechtlicher Verantwortlichkeit in die Pflicht zu nehmen, ist die Verantwortlichkeit selbst heute bereits abschließend festgestellt und geht es daher nur noch um die Offenlegung der diese legitimierenden Zurechnung. Nichtsdestotrotz sprechen bei näherer Betrachtung andere Gründe gegen eine Legitimierung über diesen Weg. Da es sich bei der Verantwortlichkeit als Zweckveranlasser um eine Verantwortlichkeit allein für die *eigene* Handlung handelt,[128] der die nachfolgende, durch diese Handlung verursachte Gefährdungshandlung zugerechnet wird, legitimiert sie auch nur Pflichten, die sich auf die eigene Handlung beziehen. Für den polizeirechtlichen Zweckveranlasser genügt dies, weil er nur zur Abstellung des eigenen Verhaltens bzw. zur Hinnahme der Ersatzhandlung oder des unmittelbaren Zwangs (sowie ggf. zur Erstattung angefallener Kosten) verpflichtet werden muss. Eine solche isolierte Pflicht – die für Diensteanbieter darauf hinauslaufen würde, eine Drittpartei schlicht nicht mehr einzubinden – wäre für die Zwecksetzung des Datenschutzrechts aber zu unterkomplex. Entsprechend der oben bereits angesprochenen unterschiedlichen Zieldimensionen von Polizei- und Datenschutzrecht wären auch hier mehrschichtige Pflichten, die – getreu der Figur der *gemeinsamen* Verantwortlichkeit – beide Verarbei-

---

[125] Vgl. *Schoch*, JURA 2009, 360 (366): „Oftmals wird ein Vorgehen gegen mehrere ‚Vorderleute', die der Behörde vielleicht nicht einmal alle bekannt sind, wenig erfolgversprechend sein." Ebenso *Poscher*, JURA 2007, 801 (807).

[126] *Martini/Fritzsche*, NVwZ-Extra 2015, 1 (10).

[127] *Martini/Fritzsche*, NVwZ-Extra 2015, 1 (11).

[128] Vgl. *Schoch*, JURA 2009, 360 (363), wonach es „bei der Zweckveranlassung um die Bewertung eigenen Verhaltens des (potenziell) Pflichtigen" geht.

tungsbeiträge betreffen und die Rolle des Betroffenen insgesamt berücksichtigen und verstärken, notwendig. Zudem ist die Untersagungsverfügung im Datenschutzrecht stets *ultima ratio*[129] und wäre eine Zurechnung, die allein diese legitimiert, daher bereits deshalb nicht ausreichend.

Ähnliches lässt sich zur Frage der Übertragung dieses Zurechnungstatbestands auf Plattformbetreiber bzgl. der Verarbeitungen durch Diensteanbieter und Drittparteien ausführen. Auch hier sind die Grundkonstellationen zunächst vergleichbar. Durch Aufnahme von Diensteanbietern auf die Plattform, auf der sich potenzielle Nutzer bewegen, sowie durch Bereitstellen der notwendigen Schnittstellen zur Erhebung von Nutzerdaten setzen Plattformanbieter eine entscheidende, die späteren Verarbeitungen ermöglichende Ursache, die ihrerseits noch nicht „gefährlich" in dem Sinne ist, als sie die späteren Datenverarbeitungen zunächst nicht näher determinieren. Aufgrund der engen Verknüpfung zwischen der eigenen Handlung und der späteren Verarbeitungshandlung könnte dem Betreiber letztere aber zugerechnet werden. Auch hier wäre es ggf. effizienter, mit dem Plattformbetreiber den einen Akteur in die Pflicht zu nehmen, dessen Handeln sich auf alle nachfolgenden, aufgrund ihrer Anzahl und Art der Aktivität nicht ohne weiteres identifizierbaren und greifbaren Akteure unmittelbar auswirkt. Doch auch hier ist die Zielrichtung einer Inpflichtnahme breiter und unter anderem auch auf Pflichten gerichtet, die das Verhalten der anderen Akteure beeinflussen und sich reflexiv auf deren eigene Pflichten auswirken.

Auch *Nichtstörer*, also Akteure, die selbst gar keinen Beitrag zur Verursachung der abzuwehrenden Gefahr geleistet haben, können unter den engen Voraussetzungen des Vorliegens eines sog. polizeilichen Notstandes in die Pflicht genommen werden.[130] Hier wird ausnahmsweise und im Interesse der Wahrung der akut bedrohten Schutzgüter auf einen Verursachungszusammenhang gänzlich verzichtet und vom unbeteiligten Einzelnen erwartet ein – zu entschädigendes – Sonderopfer zu erbringen.[131] Es genügt, dass der Nichtstörer in der Lage ist, die Gefahr wirksam abzustellen, ohne dass er einen eigenen Verursachungsbeitrag geleistet hätte. In diesen Fällen wird demnach der zu Beginn dieses Abschnitts geäußerte Grundsatz, wonach die reine Fähigkeit zur Pflichterfüllung allein nicht zur Legitimation der Inpflichtnahme genügt, ausnahmsweise durchbrochen. Überlegungen zur Übertragung dieser Ausnahme auch auf das Datenschutzrecht verbieten sich trotzdem. Wie oben aufgezeigt, erschöpft sich die polizeirechtliche Verantwortlichkeit in der Pflicht, eine einmalige, einschränkende Maßnahme von Behördenseite hinzunehmen. Lassen die Polizeigesetze es als *ultima ratio* und unter Beachtung einer Opfergrenze zu, bei gänz-

[129] Vgl. *Eichler*, in: BeckOK Datenschutzrecht, Art. 58 DSGVO Rn. 29; *Ziebarth*, in: Sydow, DSGVO, Art. 58 Rn. 54; *Nguyen*, in: Gola, DSGVO, Art. 58 Rn. 20.

[130] Siehe ausführlich zu den Voraussetzungen *Schoch*, JURA 2007, 676 (676 ff.); ebenfalls instruktiv *Kießling*, JURA 2016, 483 (484 f.).

[131] Vgl. *Kießling*, JURA 2016, 483 (484 f.).

lichem Ausschluss anderer Möglichkeiten der Gefahrenabwehr denjenigen in die Pflicht zu nehmen, der alleine wirksam diese Abwehr bewirken kann, so ist diese Inpflichtnahme von gänzlich anderer Natur als eine anhaltende Verantwortlichkeit, die zahlreiche (teils bereits proaktiv wirkende) Pflichten mit sich bringt.[132]

Die weiteren Figuren des Polizeirechts mit den ihnen zugrundeliegenden Zurechnungstatbeständen liefern daher keine tauglichen Legitimationsmuster für die Ausweitung der datenschutzrechtlichen Verantwortlichkeit auf Diensteanbieter und Plattformbetreiber. Für Diensteanbieter bleibt es insoweit bei der – unbefriedigenden – Subsumtion unter die klassische datenschutzrechtliche Zurechnung, wie sie vom EuGH implizit verwendet und im vorangegangenen Abschnitt beschrieben wurde. Für Plattformbetreiber fehlt es bis dato an einem tauglichen Zurechnungstatbestand.

c) Änderung des Bezugspunkts: Verantwortlichkeit für die eigene Schaffung eines Verarbeitungsumfelds, nicht für die Verursachung von Verarbeitungen

Abhilfe könnte hinsichtlich der Konstellation um Plattformbetreiber auf der einen und Diensteanbieter und Drittparteien auf der anderen Seite ein Verschieben des Bezugspunkts schaffen. Löst man sich von der Idee, zwingend die nachfolgenden Verarbeitungsbeiträge von Diensteanbietern und Drittparteien dem Plattformbetreiber zurechnen zu wollen, und wirft den Blick stattdessen auf die mögliche generelle Gefährlichkeit seines eigenen Handelns, für dessen Bewertung die Möglichkeit der gefahrenträchtigen Nutzung durch Dritte durchaus weiter eine Rolle spielen darf, so erlaubt dies die Legitimation einer Inpflichtnahme, die hinsichtlich ihrer Pflichten und der erhofften Wirkung breiter aufgestellt ist und nicht nur die einzelne Datenverarbeitung, sondern das gesamte Verarbeitungsumfeld, soweit es unter der Kontrolle des Plattformbetreibers ist, abdeckt. Betrachtet man die elementare Rolle einer digitalen Plattform nach Verständnis dieser Arbeit, also das Bereitstellen eines digitalen Raumes, seiner technischen Infrastruktur sowie der Ressourcen und Werkzeuge, mittels derer Akteure auf der Plattform Dienste entwickeln und anbieten können,[133] lässt sich darin leicht eine latente Gefahr bzw. zumindest ein latentes Risiko für Nutzer der Plattform erkennen. Die Verarbeitung personenbezogener Daten liegt hier im Zentrum des Geschäftsmodells vieler Dienste und Drittanbieter,

[132] Generell ablehnend bzgl. der Ausweitung von Inpflichtnahmen ohne Erfordernis eines Verantwortungszusammenhangs auch *Lennartz*, DÖV 2019, 434 (440): „Ein bloßes Praktikabilitätsargument macht ökonomisch Sinn, löst sich aber vom rechtsstaatlichen Grundsatz, am eigenen Handeln gemessen zu werden: für dieses, aber auch nur für dieses einstehen zu müssen."

[133] Siehe zu dem in dieser Arbeit verfolgten Verständnis digitaler Plattformen die Definition bei *Tiwana* u. a., Information Systems Research 2010, 675 (676) sowie die ausgiebigen Ausführungen *supra* in Kapitel 2 A. I.

für nahezu alle von ihnen spielt sie zumindest eine elementare Teilrolle.[134] Stellt man zudem auf die Plattformen generell inhärente Rolle als Intermediäre zwischen Nutzern auf der einen und Diensteanbietern und Drittparteien auf der anderen Seite ab, ist offensichtlich, dass die Wirkweise von Plattformen durch das Zusammenbringen dieser Akteure die Anzahl an Datenverarbeitungen stark begünstigt. Plattformbetreiber stellen also einen Raum zur Verfügung, der zumindest zu großen Teilen darauf ausgelegt ist, dass auf ihm personenbezogene Daten generiert, erhoben und weiterverarbeitet werden. Das reine Ausmaß der so begünstigten Datenverarbeitungen, aber auch die strukturelle Unübersichtlichkeit und Intransparenz der beteiligten Drittparteien, birgt eine grundlegende Gefahr für Betroffene. Gleichzeitig unterliegt dieser Raum regelmäßig der größtmöglichen Kontrolle des jeweiligen Plattformbetreibers, wie die Untersuchungen an früherer Stelle dieser Arbeit gezeigt haben.[135] Anstelle einer Verantwortlichkeit für die einzelnen Datenverarbeitungen bietet sich deshalb eine unmittelbare (Zustands-)Verantwortlichkeit für den Zustand – oder besser: die Ausgestaltung – dieses Raumes und der mit ihm angebotenen Infrastruktur und Ressourcen an.[136]

Eine denkbare dogmatische Rechtfertigung einer solchen Verantwortlichkeit, die ihren Ursprung ebenfalls im Gefahrenabwehrrecht im weiteren Sinne hat, ist die Begründung von *Eigensicherungspflichten*. Hierunter versteht man die Inpflichtnahme Privater zur Abwehr bestimmter von außen stammender Gefahren auf die von ihnen betriebenen und kontrollierten Einrichtungen.[137] Eine prägnante Definition stammt aus der Feder des OVG NRW:

„Unter Eigensicherungspflicht in diesem Sinne ist die einem Privaten durch Vorschriften des öffentlichen Rechts auferlegte Verpflichtung zu verstehen, von seinen privatrechtlichen Handlungsmöglichkeiten, namentlich von seinem Hausrecht, im öffentlichen Interesse – etwa zur Gefahrenvorsorge – in einer bestimmten Weise Gebrauch zu machen."[138]

Dabei betrifft die Pflicht seit ihrer Genese in den 1980er Jahren klassischerweise Fälle, in denen Betreiber kritischer Infrastrukturen, die ein besonders attrak-

---

134 Vgl. *Weichert*, ZD 2014, 605 (607).

135 Vgl. *supra* in Kapitel 1 B.

136 In diese Richtung gehend auch *Helberger* u. a., The Information Society 2018, 1 (4) für das Verhältnis zwischen sozialen Netzwerken und ihren Nutzern, das sich insofern analog zu dem Verhältnis zwischen Plattformbetreibern und Diensteanbietern bzw. Drittparteien verhält: „Thus, how platform architectures are designed, shapes how users fulfill their role responsibly." Vgl. auch *Thompson*, The American Review of Public Administration 2014, 259 (261), der von einer Verlagerung der Perspektive „from the responsibility for outcomes to the responsibility for the design of organizations" spricht.

137 Vgl. *Schoch*, in: Schoch, Besonderes Verwaltungsrecht, S. 11 (58); siehe grundlegend außerdem *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung; *Otten*, Eigensicherung.

138 OVG NRW, Urt. v. 19.06.2013, Az. 4 A 1065/12 Rn. 58.

tives Ziel für schädigende Dritte darstellen oder besonders gefährdet hinsichtlich Umweltkatastrophen sind, Sicherheitsmaßnahmen zur Abwehr solcher von außen stammender Gefahren ergreifen müssen.[139] Beispiele für Adressaten solcher einfachgesetzlich ausgestalteter Pflichten sind Betreiber von Atomkraftwerken oder Flughäfen.[140] Die Zulässigkeit solcher Pflichten wurde durch das BVerwG bestätigt,[141] ihre Voraussetzungen durch zahlreiche obergerichtliche Entscheidungen konturiert: So ist notwendig, dass entsprechende Pflichten durch das privatrechtliche Arsenal des jeweiligen Adressaten – in erster Linie also dessen Hausrecht – tatsächlich erfüllt werden können und in einem engen Zusammenhang mit den Risiken stehen, die sich aus dem Betrieb der Anlage ergeben.[142] Zudem muss die Erfüllung der Pflicht(en) „neben dem Interesse der Öffentlichkeit […] auch im eigenen Interesse des jeweiligen Unternehmens liegen."[143] Über die Jahre hat sich der Anwendungsbereich der Figur der Eigensicherungspflichten jedoch von diesen Ursprüngen emanzipiert und umfasst nun ein breiteres Feld an Konstellationen. Auch die aus § 3 NetzDG stammende Pflicht für Betreiber sozialer Netzwerke, rechtswidrige Inhalte zu entfernen, wird zuweilen als Eigensicherungspflicht klassifiziert,[144] gleiches gilt für die aus § 36 Abs. 1 S. 1 WaffG stammende Pflicht zur Sicherung der eigenen Waffe vor unbefugten Zugriffen Dritter und die auf Sicherung des eigenen Kraftfahrzeugs gerichtete Pflicht in § 14 Abs. 2 S. 2 StVO.[145]

Im Kern geht es also um Pflichten zur Ergreifung bestimmter Maßnahmen zur Gefahrenvorsorge, -abwehr und Schadensminimierung bzgl. der eigenen Anlage, aber auch bzgl. der diese nutzenden Allgemeinheit.[146] Die Pflichten können sich sowohl auf die Planung und den Bau der betreffenden Anlage als auch auf die Durchführung des alltäglichen Betriebs beziehen. So verpflichtet § 8 Abs. 1 Nr. 1 LuftSiG Flughafenbetreiber zu einer Erstellung und Gestaltung des Flughafens, die „die erforderliche bauliche und technische Sicherung" zum Schutz vor Angriffen auf die Sicherheit des Luftverkehrs bietet, während Abs. 1 Nr. 5 der Norm dazu verpflichtet, eigene Mitarbeiter sowie Mitarbeiter anderer auf dem Flughafen tätiger Unternehmen zu durchsuchen und zu kontrollieren.[147]

---

[139] Vgl. *Lennartz*, DÖV 2019, 434 (437).

[140] Siehe die Pflichten in § 7 Abs. 2 Nr. 5 AtG und § 8 LuftSiG. Für eine ausführliche Auflistung siehe *Otten*, Eigensicherung, S. 119 ff.

[141] Vgl. BVerwGE 81, 158.

[142] Vgl. OVG NRW, Urt. v. 19.06.2013, Az. 4 A 1065/12 Rn. 58 ff.; OVG Bremen, Urt. v. 31.10.2006, Az. 1 D 41/06 Rn. 31, BeckRS 2007, 23685.

[143] OVG Bremen, Urt. v. 31.10.2006, Az. 1 D 41/06 Rn. 30.

[144] Vgl. *Lennartz*, DÖV 2019, 434 (438).

[145] Vgl. *Lange*, Zweckveranlassung, S. 29.

[146] Aufgrund dieser starken Fremdschutzkomponente kritisch zum Begriff der Eigensicherungspflicht *Möstl*, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung, S. 335 ff.

[147] Ausführlich, wenn auch veraltet, zu Pflichten von Flughafenbetreibern *Czaja*, Eigensicherungspflichten von Verkehrsflughäfen.

Diese Grundsätze lassen sich gut auf Plattformbetreiber und die von ihnen betriebenen Plattformen übertragen. Bleibt man bei dem oben gezeichneten Bild in Fortführung der Dogmatik des Datenschutzrechts, ist die Gefahr, die der Plattform droht, zunächst die einzelne Datenverarbeitung selbst, nachgelagert außerdem die Möglichkeit ihrer rechtswidrigen Durchführung. Wie bereits mehrfach erwähnt und beschrieben, ist die Verarbeitung personenbezogener Daten Grundlage von sowohl Funktionsweisen als auch Geschäftsmodellen vieler digitaler Dienste und damit auch Triebfeder digitaler Plattformen, betrifft damit also unmittelbar deren Kerngebiet. Plattformen ermöglichen diese Datenverarbeitungen in mehrfacher Weise: Indem sie (End-)Nutzer, Diensteanbieter und Drittparteien zusammenbringen und die einzelnen Anbieter sichtbar machen, teilweise gar gesondert bewerben und herausstellen, ermöglichen sie den notwendigen Kontakt zwischen den Parteien; aufgrund der typischerweise hohen Anzahl an Nutzern und Anbietern, der hohen Anzahl und – insbesondere bei Smartphone-Apps – breiten Vielfalt der aus fast allen Lebensbereichen stammenden Daten sowie der vorherrschenden Intransparenz der zugrundeliegenden Akteurskonstellationen, geht mit dem Betrieb ein nicht unerhebliches Risiko einher. Die im Zusammenhang mit Eigensicherungspflichten in vielen Fällen relevanten Pflichten passen in großem Maße zu denen, die oben (in Abschnitt 1. a)) für Plattformbetreiber besprochen wurden. So wie Flughafenbetreiber zur Wahrung der Sicherheit des Flugbetriebs Pflichten zu erfüllen haben, die sich unter anderem auf die räumliche und strukturelle Gestaltung des Flughafengebäudes, aber auch auf die Kontrolle der auf dem Gelände aktiven eigenen und fremden Mitarbeiter beziehen, geht es bei Plattformbetreibern in erster Linie um Pflichten zur datenschutzfreundlichen Ausgestaltung der eigenen Infrastruktur und Interfaces sowie zur Kontrolle von Dienste- und Drittanbietern.[148] Die Gefahren drohen in beiden Fällen von Dritten – also von Akteuren, die zwar auch auf der jeweiligen Räumlichkeit agieren, aber nicht zum Lager des jeweiligen Betreibers gehören. Gleichzeitig hängen die Gefahren unmittelbar und originär mit dem Betrieb des jeweiligen Raumes zusammen. Wenngleich Plattformbetreiber davon profitieren, dass auf ihrer Plattform weitreichend und umfassend Daten verarbeitet werden, weil dies umgekehrt für eine hohe Anzahl Nutzer und eine umfassende Nutzung von Diensten steht, sind derartige Sicherungspflichten dennoch nicht nur im Interesse der Öffentlichkeit und Allgemeinheit, sondern auch der Betreiber selbst. Jedenfalls ein Erschweren datenschutzrechtswidrigen Verhaltens von Plattformteilnehmern kommt ihnen insofern zugute, als sich bekannt gewordene Fälle von Fehlverhalten und Datenlecks schnell negativ auf das Image der Plattform auswirken können, wie

[148] Hinzu tritt als datenschutzrechtliches Spezifikum die Unterstützung von Betroffenen und ggf. Aufsichtsbehörden sowie die, nicht unmittelbar die materiellen Pflichten selbst betreffende, Erwartung der weitergehenden Wirkung auch auf die Erfüllung der Pflichten durch die übrigen Akteure.

nicht zuletzt der Fall um Facebook und Cambridge Analytica gezeigt hat. Wie in Kapitel 1 aufgezeigt wurde, sind Plattformbetreiber zudem sowohl faktisch aufgrund ihrer weitreichenden Einflussmöglichkeit und Macht als auch rechtlich aufgrund ihrer vertraglichen und hausrechtlichen Rechtspositionen in der Lage, diese Pflichten wirksam zu erfüllen.

Die Voraussetzungen für eine legitime gesetzliche Inpflichtnahme von Plattformbetreibern über die Figur der Eigensicherungspflichten sind daher gegeben.

3. Annex: Zusatzbelastung für Dienste- und Drittanbieter

Eine weitere Legitimationsebene lässt sich mit Blick auf die Einschränkungen aufspannen, die sich durch Inpflichtnahme von Plattformbetreibern für Dienste- und Drittanbieter ergibt. Einerseits lässt sich hier anführen, dass Plattformbetreiber bereits jetzt ihre Macht ausüben, indem sie vertragliche Bedingungen für die Aufnahme auf ihre Plattformen stellen und deren Einhaltung kontrollieren sowie bei Fehlverhalten Akteure sanktionieren oder gänzlich von der Plattform ausschließen. Auch Entscheidungen für eine restriktivere Ausgestaltung der Zugriffskanäle auf personenbezogene Daten sind bereits jetzt Teil des Plattformalltags[149] und wirken sich beschränkend auf die Handlungsfreiheit von Diensteanbietern und Drittparteien aus. Eine nunmehr explizit gesetzlich verankerte *Pflicht* zur strukturierten und bewusst datenschutzfreundlichen Durchführung dieser Maßnahmen würde daran also vermeintlich nichts ändern. Ein derartiges Verständnis würde aber übersehen, dass jedenfalls im Verhältnis zwischen dem Verordnungsgeber und den betroffenen Parteien eine solche gesetzliche Inpflichtnahme eines Akteurs zu Maßnahmen zulasten anderer Akteure eine rechtfertigungsbedürftige Grundrechtsbeschränkung der zuletzt Genannten darstellt.[150] Für den in seinem Handeln stets an die Grundrechte gebundenen Staat ebenso wie für die gem. Art. 51 Abs. 1 GRCh grundrechtsgebundenen Unionsorgane macht es daher einen entscheidenden Unterschied, ob Plattformbetreiber aus eigener Motivation heraus ihre Macht zulasten der Akteure auf ihren Plattformen ausüben oder ob sie gesetzlich zur Ausübung dieser Macht verpflichtet werden.[151]

Einer tiefergehenden Erörterung der Frage der Rechtfertigung dieser Belastung bedarf es hier trotzdem nicht. Versteht man eine Ausweitung der Verantwortlichkeit auch auf Plattformbetreiber nämlich, wie in dieser Arbeit vor-

---

[149] Stellvertretend sei hier auf die jeweiligen Ausgestaltungsänderungen bei Facebook und Apple hingewiesen, die nach dem Cambridge Analytica- respektive AccuWeather-Skandal implementiert wurden. Vgl. die Aufbereitung dieser Fälle *supra* bei Kapitel 1 A.

[150] Vgl. *Lennartz*, DÖV 2019, 434 (436).

[151] Wenngleich auch bei Nichtexistenz einer solchen Verpflichtung die Ausübung der Macht eine grundrechtsrelevante Schwelle überschreiten und im Rahmen der mittelbaren Drittwirkung der Grundrechte gerichtlich überprüft werden kann.

geschlagen, unter anderem als Inpflichtnahme zum Zwecke der Kompensation von Defiziten, die das bisherige Verantwortlichkeitskonzept und damit die Inpflichtnahme der bisherigen Verantwortlichen ereilt, so wird schnell offenbar, dass Maßnahmen der Plattformbetreiber die Diensteanbieter und Drittparteien im Kern nicht stärker belasten als die sie sowieso schon treffenden Pflichten der DSGVO. Mit anderen Worten: Die von Plattformbetreibern im Rahmen ihrer Pflichten geforderten Maßnahmen zulasten von Akteuren auf Plattformen haben letztlich nur eine instrumentelle Wirkung hinsichtlich der Durchsetzung der klassischen Verantwortlichenpflichten, die Diensteanbieter und Drittparteien treffen. Die Zusatzbelastung für Letztgenannte erschöpft sich somit darin, in größerem Maße zur Befolgung der sie bereits vorher treffenden Pflichten gezwungen zu sein. An ein solches bloßes Mehr an Durchsetzung bestehender Pflichten muss dann auch bloß derselbe Maßstab zur Rechtfertigung angelegt werden, der auch an die ursprünglichen Pflichten angelegt wurde. Die Strukturermächtigung aus Art. 8 Abs. 1 GRCh[152] sowie die unter Umständen aktivierte Schutzpflicht aus Art. 8 GrCh i. V. m. anderen Grundrechte wie Ar. 7 GRCh rechtfertigt daher auch die hier infragestehende Zusatzbelastung.

III. Zwischenergebnis

Es wurde aufgezeigt, dass die Ausweitung der datenschutzrechtlichen Verantwortlichkeit auch auf Diensteanbieter und Plattformbetreiber mit Blick auf die durch komplexe Akteurskonstellationen einhergehenden Defizite für das klassische Verantwortlichkeitskonzept notwendig ist (I.). Legitim ist die mit einer solchen neuartigen Inpflichtnahme einhergehende Zusatzbelastung für die betroffenen Akteure zum einen deshalb, weil beide in der Lage sind, sowohl die typisierten Arten von materiellen Pflichten, die eine Inpflichtnahme mit sich bringen würde, als auch die instrumentell mit der Inpflichtnahme verbundenen Erwartungen hinsichtlich der Auswirkungen auf die übrigen Verantwortlichen und ihre Fähigkeit zur Pflichtenerfüllung zu erfüllen (II. 1.). Zum anderen liegt in den Fällen beider Akteursgruppen jeweils eine hinreichende Nähe des eigenen Handelns zu den konkreten Datenverarbeitungen anderer Akteure bzw. zu der Schaffung von essenziellen Verarbeitungsgrundlagen vor, um auch in dieser Hinsicht eine Verantwortlichkeit zu rechtfertigen (II. 2.). Wo es um die Inpflichtnahme von Plattformbetreibern geht, erlaubt der Betrieb einer typischerweise in großem Maße datengetriebenen und damit im weitesten Sinne gefahrgeneigten Plattform die Belegung mit Eigensicherungspflichten, da die Vielzahl vorgenommener Datenverarbeitungen in Verbindung mit der Vielzahl, Komplexität und Intransparenz der beteiligten Akteure sichernde Maßnahmen erforderlich macht. Wo die Inpflichtnahme von Diensteanbietern im Raum

[152] Siehe hierzu ausführlich *supra* in Kapitel 2 A. I. 1. a) bb).

steht, ist mit der aktuellen Rechtsprechungslinie des EuGH unmittelbar auf die durch Einbezug von Drittparteien ermöglichten Datenverarbeitungen abzustellen, die sich bei hinreichender Zweckkongruenz jedenfalls *auch* als die Ihre darstellen, sodass eine Zurechnung mit dem althergebrachten Instrumentarium des Datenschutzrechts ausreicht. Die dabei bestehenbleibenden Unklarheiten bei der Grenzziehung dieser Zurechnung sind dennoch unbefriedigend: Welches Ausmaß an Ermöglichung und Zweckkongruenz genügt, auf welche Fälle die Ausweitung anwendbar ist und in welchen Fällen ggf. Ausnahmen greifen, bleibt offen. Für die isolierte Frage der Legitimierung der Zusatzbelastung sollen diese offenen Punkte aber außenvorbleiben und erst als Feinjustierung der konkreten Ausgestaltung im nächsten Abschnitt unter dem Gesichtspunkt der Möglichkeit einer praxistauglichen Weiterentwicklung und zielgerechten Konturierung der gemeinsamen Verantwortlichkeit diskutiert werden.

C. Ansatz 1: Die Weiterentwicklung der gemeinsamen Verantwortlichkeit

Ein erster Ansatz zur zielgerichteten Weiterentwicklung der datenschutzrechtlichen Verantwortlichkeit vor dem Eindruck der modernen Verarbeitungsrealität ist die Weiterentwicklung der bereits angestoßenen Entwicklung hin zu einem extensiveren Einsatz der existierenden Figur der gemeinsamen Verantwortlichkeit. Wie oben bereits festgestellt, bietet sich dieser bei Betrachtung der hier in den Blick genommenen Akteursrollen primär für Diensteanbieter im Verhältnis zu den von ihnen einbezogenen Drittparteien an; hier weisen die strukturellen Eigenschaften der jeweiligen Fallszenarien (insbesondere bei Betrachtung der Fashion ID-Entscheidung) große Parallelen auf und liegt ein unmittelbares Vorliegen der vom EuGH etablierten Voraussetzungen daher nahe. Vorteil einer gemeinsamen Verantwortlichkeit ist, dass ihr die bereits angesprochene reflexive Verknüpfung und gegenseitige Bezugnahme der beteiligten Akteure schon zugrunde liegt, die für die Kompensierung der aufgezeigten konzeptionellen Defizite essenziell ist. Eine solch enge Verknüpfung der jeweiligen Inpflichtnahmen ist mit Blick auf die Art des Zusammenwirkens zwischen Diensteanbieter und Drittpartei gerechtfertigt. „Der Beitrag des einen wäre ohne den Beitrag des anderen nicht denkbar."[153]

Im Folgenden soll daher zunächst in einem ersten Schritt zurück auf die in Kapitel 3 gemachten Erkenntnisse geblickt und kurz rekapituliert werden, welche elementaren Bestandteile die gemeinsame Verantwortlichkeit hinsichtlich ihrer Voraussetzungen, ihrer Reichweite und ihrer einzelnen Pflichten ausmacht und zusammengefasst werden, wo ihre zentralen Defizite – insbesondere

[153] *Weichert*, ZD 2014, 605 (608).

bei der Übertragung auf weitere, über die den EuGH-Entscheidungen zugrundeliegenden Fälle hinausgehende, Anwendungsfälle – liegen (I.). Sodann wird untersucht, inwieweit den Defiziten schon bei zielgerechter Anwendung des jetzigen Rechts unter Ausnutzung der Skalierbarkeit des Pflichtenkatalogs entgegengewirkt werden kann (II.), um dann Vorschläge für mögliche Weiterentwicklungen *de lege ferenda* zu machen (III.). Ein Zwischenfazit fasst die erworbenen Erkenntnisse zusammen und resümiert, ob und wenn ja für welche Akteursgruppen die Fortsetzung des durch den EuGH eingeschlagenen Weges ein tauglicher Ansatz zur Stabilisierung des Gesamtkonzepts ist (IV.)

I. Auswirkungen und Grenzen der gemeinsamen Verantwortlichkeit

Die gemeinsame Verantwortlichkeit zielt auf die Einhaltung der Datenschutzbestimmungen und die Schaffung von Transparenz zugunsten des Betroffenen auch in Fällen großer Komplexität infolge *bewusster* Zusammenarbeit mehrerer Akteure ab, indem diese nicht zuletzt zur Bewusstmachung ihrer eigenen Rolle und zur Klärung und Verteilung der jeweiligen Aufgaben und (internen) Verantwortlichkeiten gezwungen werden. Wie aber die obigen Untersuchungen gezeigt haben, führt die vom EuGH schrittweise vorgenommene Ausweitung der gemeinsamen Verantwortlichkeit *en passant* auch zu Unklarheiten und Unsicherheit auf mehreren Ebenen.[154]

Zum einen fehlt es zum jetzigen Zeitpunkt an einer klaren Abgrenzung, wer nun tatsächlich in welchen Konstellationen Verantwortlicher ist und wer nicht. Die vom EuGH angeführten und unter die etablierte Definition von der „Festlegung von Zwecken und Mitteln der Verarbeitung" gem. Art. 4. Nr. 7 DSGVO subsumierten Kriterien lassen vieles offen und legen insgesamt eher eine extensive denn eine restriktive Anwendung nahe.[155] Dadurch aber führen sie letztlich zu derselben Ausgangsproblematik zurück, die das Rechtsinstitut der gemeinsamen Verantwortlichkeit überhaupt erst beheben sollte: Unklarheiten bei der Verteilung und Zuordnung von Verantwortlichkeiten, sowohl im Interesse der jeweiligen Verantwortlichen, die ihr Handeln erkennbar und frühzeitig danach ausrichten sollen,[156] als auch der Betroffenen und Aufsichtsbehörden, die zur Ausübung ihrer Betroffenenrechte und Kontrollbefugnisse Klarheit benötigen.[157] Geht man also zunächst im Interesse einer möglichst einfachen und klaren Zuordnung davon aus, dass jede bewusste Nutzung einer fremden daten-

[154] Siehe die Ausführungen in Kapitel 2 C. II. c).

[155] So auch schon vor Erlass der EuGH-Urteile zu den entsprechenden Fällen *Weichert*, ZD 2014, 605 (610): „Die Nutzung fremder datenverarbeitender Infrastrukturen und Dienste im Internet beschränkt sich nicht auf Fanpages und Facebook."

[156] Vgl. *Sydow/Kring*, ZD 2014, 271 (272): „Verhinderungspotential hat nicht erst das rechtliche Verbot, sondern die juristische Unsicherheit, das Haftungsrisiko."

[157] Diese Erwartungen und Gefahren bereits betonend *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftrags-

verarbeitenden Infrastruktur und jeder Einbezug eines fremden datenverarbeitenden Dienstes bei gleichzeitigem Angebot eigener Inhalte oder Dienste zu einer gemeinsamen Verantwortlichkeit mit dem Anbieter der genutzten Infrastruktur bzw. des genutzten Dienstes im Hinblick auf die Daten der Nutzer der eigenen Inhalte bzw. des eigenen Dienstes führt,[158] wird dieses Problem (zumindest auf den ersten Blick) gelöst, dafür aber ein anderes verstärkt. Klare Grenzen lassen sich weder den Urteilen noch der bereits weit früher verfassten Typologie der *Art. 29-Datenschutzgruppe*[159] entnehmen.[160]

Hinzu kommt eine ebenso starke Ungewissheit über die konkreten Konsequenzen für den bzw. die Verantwortlichen im Einzelfall, auf zwei separaten Ebenen.

Zum einen: Wen treffen welche Pflichten, wer muss also welche proaktiven Maßnahmen ergreifen und wer darf, ggf. in welcher Reihenfolge, von Betroffenen bei Geltendmachung ihrer Rechte und Ansprüche und von Aufsichtsbehörden bei Ausübung ihrer Befugnisse in Anspruch genommen werden? Wie verteilt sich also die Pflichtenverteilung im Einzelnen auf die gemeinsamen Verantwortlichen? Die mit der Fashion ID-Entscheidung aufgegriffene[161] und bereits weit vorher durch die *Art. 29-Datenschutzgruppe* initial etablierte[162] Betrachtung einzelner Verarbeitungs*phasen* zur Begrenzung der jeweiligen Verantwortlichkeit in Verbindung mit der Prämisse, dass zwei oder mehrere gemeinsame Verantwortliche nicht zwingend den *gleichen Grad* an Verantwortlichkeit haben müssen,[163] können als Ansatz zur Abschichtung und Abgrenzung verstanden werden – freilich auch hier, ohne eindeutige Grenzen und Wirkungen zu definieren.[164] Wenngleich die phasenbezogene Betrachtungs-

verarbeiter", S. 29; Siehe auch *Mahieu* u. a., jipitec 2019, 85 (95): „[…] while it indeed helps to defend the relevant rights, it also leads to legal uncertainty."

158 So auch *Mahieu* u. a., jipitec 2019, 85 (99): „Integrating a service which involves processing data, and having the ability to influence the processing, also leads to the qualification of controller."

159 Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 18 ff.

160 Zu diesem Urteil kommen auch *Mahieu* u. a., jipitec 2019, 85 (90). Ähnlich auch *Bygrave/Tosoni,* in: Kuner u. a., GDPR, S. 153: „In a situation where controller responsiblity is shared amongst increasingly large numbers of entities, the risk arises that responsibility becomes diluted if not pulverised."

161 Treiber dieses Aufgreifens war hier Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 97ff, dessen Ausführungen sich der EuGH in Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 1 anschloss.

162 Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 25 ff.

163 Siehe *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 39 sowie Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 75, der eine genauere Diskussion der praktischen Auswirkungen einer ungleichen Verantwortlichkeitsverteilung aber ebenfalls schuldig bleibt.

164 Auch hier noch zur Stellungnahme der *Art. 29-Datenschutzgruppe Mahieu* u. a., jipitec

weise vermuten lässt, dass die tatsächlichen Möglichkeiten der Einflussnahme berücksichtigt werden, bleiben auch im Rahmen derjenigen Phasen, für die ein Akteur ohne weiteres verantwortlich ist, genügend Möglichkeiten für Pflichten, die ohne Mitwirkung des oder der anderen gemeinsamen Verantwortlichen nicht erfüllt werden können. Bestes Beispiel dafür ist der Fanpage- bzw. Websitebetreiber, der seine Informationspflicht auch bei Begrenzung auf die initiale Übermittlung an Facebook nicht umfassend erfüllen kann, solange Facebook ihm nicht offenlegt, was genau zu welchen Zwecken mit diesen Daten gemacht wird.

Zum anderen, und aufbauend auf diese Erkenntnis: Wer darf bei Pflichtverletzungen inwieweit, und ggf. in welcher Reihenfolge, sanktioniert oder auf Schadensersatz und ähnliche Rechtsfolgen hin in Anspruch genommen werden? Wie verteilt sich also die Haftung im Einzelnen zwischen den gemeinsamen Verantwortlichen? Und inwieweit spielt die eben angesprochene Problematik einer Pflichtverletzung, die – etwa in Form einer nicht erfüllten Informationspflicht – aus der Sphäre des anderen gemeinsamen Verantwortlichen stammt, hier eine Rolle? Art. 82 Abs. 2 S. 1 DSGVO stellt jedenfalls für die schadensersatzrechtliche Haftung klar, dass *jeder* an einer Verarbeitung beteiligte Verantwortliche grundsätzlich zu haften hat. Abs. 4 der Norm konkretisiert, dass mehrere gemeinsame Verantwortliche zum Zwecke der Sicherstellung eines wirksamen Schadensersatzes im vollen Umfang gemeinsam, also *gesamtschuldnerisch* haften,[165] wird aber gleichzeitig von Abs. 3 dahingehend eingeschränkt, dass eine Exkulpationsmöglichkeit besteht für Verantwortliche, die nachweisen können „in keinerlei Hinsicht" für die Umstände, durch die Schäden eingetreten sind, verantwortlich zu sein. Für die Sanktionierung durch Aufsichtsbehörden gibt es hingegen mangels Verschuldenserfordernis keine Exkulpationsmöglichkeit und kann der vorgelagerte unter den gemeinsamen Verantwortlichen, wie im Falle Wirtschaftsakademie letztlich durch das BVerwG bestätigt,[166] gemäß dem Grundsatz der möglichst effizienten Gefahrenabwehr ohne weiteres primär in Anspruch genommen und im schlimmsten Fall zur Untersagung seiner Tätigkeit verpflichtet werden.[167]

Damit ist zu konstatieren, dass die DSGVO in einem begrenzten Rahmen selbst klare Limitierungen setzt und Vorgaben macht. Über diesen Rahmen hinaus verbleibt jedoch ein großes Maß an Unklarheit, das bei der Bestimmung

---

2019, 85 (91): „The Working Party introduces the principle that parties can have partial responsibility, but it does not develop a consistent framework to determine the exact scope and limit of this partial responsibility."

165 Vgl. *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 82 DSGVO Rn. 57.

166 Vgl. BVerwG, Urt. v. 11.09.2019, Az. 6 C 15.18 (Wirtschaftsakademie Schleswig-Holstein) Rn. 37.

167 Siehe zur Konkurrenz zwischen Unionsverwaltungsrecht und mitgliedstaatlichem Verwaltungsrecht sowie zu den Ermessensspielräumen von Aufsichtsbehörden bei der Durchsetzung der DSGVO *Schreiber*, ZD 2019, 55 (59 f.).

der Verantwortlichkeit selbst beginnt und bei ihrem konkreten Ausmaß sowie der Verteilung sowohl der einzelnen Pflichten als auch der Haftung im Einzelfall endet. Dies ist einerseits problematisch für die betroffenen Verantwortlichen, denen es so akut an Planungssicherheit und klaren Vorgaben mangelt. Gleichzeitig verhindert diese Unsicherheit der relevanten Akteure von vornherein die mit der Ausweitung der Verantwortlichkeit erwartete Wirkung. Wo die in die Pflicht genommenen Akteure nicht eindeutig und frühzeitig wissen können, dass sie in die Pflicht genommen werden, was genau von ihnen erwartet wird und in welchen Fällen sie mit Sanktionen rechnen müssen, geht das Verantwortlichkeitskonzept nicht auf.[168] Folgt man daher der eingangs gemachten Lösung einer möglichst weitreichenden Verantwortlichkeit aller Stellen, die durch Ermöglichung von Verarbeitungen bei gleichzeitigem Wissen um die damit verfolgten Zwecke einen irgendwie gearteten Vorteil erlangen, und erleichtert so die Zuordnung, verbleiben die nachgelagerten Ungewissheiten auf Ebene der Pflichten- und Haftungsverteilung.

II. Zielgerechte Skalierbarkeit der Verantwortlichenpflichten

Fraglich ist nach dieser ersten Erkenntnis daher, inwieweit der Pflichtenkatalog der DSGVO flexibel und skalierbar genug ist, um durch das extensive Verständnis nunmehr als vorgelagerte gemeinsame Verantwortliche in die Pflicht genommene Diensteanbieter mit solchen Pflichten zu belegen, die mit Blick auf die Zielsetzung des (erweiterten) Verantwortlichkeitskonzepts[169] einerseits und die tatsächlichen Fähigkeiten der Akteursgruppe andererseits sinnvoll erscheinen, also tatsächlich und mit der erwarteten Wirkung erfüllt werden können. Zwar liegen die Erwartungen ausweislich der Argumentation des EuGH und des Verständnisses vieler Rezipienten in der Literatur zu großen Teilen nicht in der eigenen Handlungsfähigkeit der neu hinzugekommenen Verantwortlichen, sondern in dem Druck, den diese durch ihre eigenen Haftungsrisiken mittelbar auf die chronisch datenschutzwidrig handelnden Infrastruktur- und Diensteanbieter ausüben.[170] Eine Inpflichtnahme, die nur eine solch mittelbare und damit den Pflichtigen als Mittel zum Zweck objektifizierende Wirkung zeitigt und gar nicht erwartet, dass dieser die ihn treffenden materiellen Pflichten tatsächlich erfüllen kann, wäre aber verfehlt. Einen Akteur in die Pflicht zu nehmen, um damit Druck auf einen anderen, ebenfalls pflichtigen, Akteur auszuüben, ist zwar nicht *per se* illegitim, darf aber jedenfalls nicht der einzige Grund der Inpflichtnahme sein.[171] Ist der Pflichtenkatalog *de lege lata* also nicht hinreichend

---

[168] Siehe dazu schon ausführlich die dritte Prämisse *supra* bei Kapitel 2 B. II. 3.

[169] Siehe hierzu in diesem Kapitel bei B. I. und II.

[170] Stellvertretend hierfür *Globocnik*, IIC 2019, 1033 (1042), der von „enforcement against Big Tech by the back door" spricht.

[171] Vgl. *Lennartz*, DÖV 2019, 434 (440).

flexibel und skalierbar, wäre das möglicherweise ein Indiz für die Notwendigkeit einer verordnungsgeberischen Nachbesserung.

Eine zielgerechte Skalierbarkeit der Pflichtenzuordnung und -reichweite würde daher bedeuten, Diensteanbietern und ggf. Plattformbetreibern diejenigen Pflichten zuzuschreiben, die von ihnen bei realweltlicher Betrachtung wirksam erfüllt werden können. Nur dann läge auch ein Einklang mit den Grundprämissen der Verantwortlichkeit, insbesondere der Prämisse des zentralen, wissenden und handlungsfähigen Verantwortlichen vor.[172] Dabei müsste ebenfalls ein Ausgleich hinsichtlich der Frage gefunden werden, welche Handlungen und ggf. Erfolge ausreichen, um die Pflicht als erfüllt anzusehen – eine Haftung um der schieren Haftung willen ist bei Betrachtung auf der Makroebene kein tauglicher Bestandteil eines Regulierungskonzepts, dessen Ziel die tatsächliche Verbesserung des Schutzes für Betroffene ist.

Wie bereits in Kapitel 2 erörtert,[173] kennt die DSGVO aber eine nur teilweise Inpflichtnahme von Verantwortlichen weder dem Wortlaut noch der Systematik nach: „The obligations incumbent on a controller in principle befall the controller ‚as a complete set'."[174] Ein gegenteiliges Verständnis verfolgte zumindest zeitweise die *Art. 29-Datenschutzgruppe*, die mit Blick auf Anbieter von Online-Inhalten bereits 2010 zum identischen Verantwortlichkeitsbegriff der DSRL eine „bestimmte Verantwortung" für die Übermittlungen von Nutzer-IP-Adressen an in das Angebot einbezogene Anbieter von Werbenetzwerken sah, die „der eines für die Datenverarbeitung Verantwortlichen verwandt" sein sollte.[175] Nach dieser Lesart – die wahlweise eine gänzlich neue, verantwortlichenähnliche, Inpflichtnahme oder eine echte Verantwortlichenstellung mit abgespecktem Pflichtenkatalog bedeuten könnte – böte die DSGVO eine größere Flexibilität als gedacht. Im Endeffekt spricht für ein solches Verständnis aber wenig. Weder wurde es im Nachgang von Aufsichtsbehörden umgesetzt noch bei der Konzeption der DSGVO berücksichtigt. Auch lässt Art. 26 Abs. 3 DSGVO, den es in dieser Form in der zum Zeitpunkt der Stellungnahme der Datenschutzgruppe aktuellen DSRL nicht gab, keine Zweifel daran, dass jedenfalls diejenigen Pflichten, denen einforderbare Betroffenenrechte gegenüberstehen, zwingend für jeden gemeinsamen Verantwortlichen gelten.[176] Spätestens mit der EuGH-Rechtsprechung seit Wirtschaftsakademie, die nach hiesigem Verständnis auch auf die von der Datenschutzgruppe behandelten Konstellationen zwischen Inhalte-Anbieter und Werbenetzwerkbetreiber anzuwenden ist,

---

172 Hierzu ausführlich *supra* Kapitel 2 B. II.

173 Siehe *supra* Kapitel 2 C. II. 4. d) cc) (3).

174 *Van Alsenoy*, CLSR 2012, 25 (39).

175 *Art. 29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, S. 28.

176 Anders aber *Kollmar*, NVwZ 2019, 1740 (1742), die in der Norm eine Pflicht auch der im Innenverhältnis nicht zuständigen Verantwortlichen allein zur Wahrnehmung, nicht aber zur Erfüllung der Betroffenenrechte sieht.

ist zudem geklärt, dass auch für die bloße Übermittlung von IP-Adressen eine vollständige gemeinsame Verantwortlichkeit besteht. Es bleibt daher bei der bereits in Kapitel 3 gemachten Feststellung, wonach einzig die *phasenweise* Begrenzung der Verantwortlichkeit ein gewisses Maß an Flexibilität bietet. Ist die Verantwortlichkeit also auf diejenigen Verarbeitungsphasen begrenzt, für die ein Akteur den ausreichenden Mittel- und Zweckeinfluss besitzt, treffen ihn in diesem Rahmen zwar alle Pflichten ausnahmslos, doch wird zumindest der Lebenssachverhalt eingegrenzt, innerhalb dessen sie erfüllt werden müssen. Dennoch verbleibt fraglich, ob diese Einschränkung bei gleichbleibendem Pflichtenkatalog mit Blick auf die Wirksamkeit der Inpflichtnahme genügt. Beispiele für Pflichten, die einen vorgelagerten gemeinsamen Verantwortlichen in „seiner" Verarbeitungsphase treffen, ohne dass er sie selbständig und ohne Abhängigkeit von dem bzw. den weiteren Verantwortlichen erfüllen kann, verbleiben schließlich weiterhin. Die Informationspflichten, deren Nichterfüllung das BVerwG im Falle Wirtschaftsakademie angeprangert hatte, sollen hier ebenso wie die aus Art. 26 Abs. 1 S. 2 DSGVO stammende Pflicht zum Abschluss einer die jeweilige Pflichtenerfüllung abgrenzenden Vereinbarung, die ohne Kooperation des Gegenüber nicht möglich ist und deren Nichterfüllung bereits zur Rechtswidrigkeit der Datenverarbeitung führt,[177] stellvertretend genannt werden.

Im Endeffekt würde eine nicht modifizierte Anwendung der gemeinsamen Verantwortlichkeit daher trotz einiger möglicherweise erfüllbarer Pflichten im Kern doch wieder auf die folgende an den vorgelagerten Verantwortlichen (bspw. einen Diensteanbieter) gerichtete Prämisse zurückführen: „Such dir einen Infrastruktur- oder Drittanbieter, der gänzlich datenschutzkonform agiert oder bereit ist, dir soweit entgegenzukommen, wie es dir zur Erfüllung deiner Pflichten nötig ist; gelingt dir dies nicht, bist du für die Datenschutzverstöße des von dir ausgewählten Akteurs mit verantwortlich." Eine solche, letztlich auf die Auswahl des Vertragspartners und Ausgestaltung der Kooperation gerichtete Pflicht kann aber ihre Wirkung jedenfalls dann nicht entfalten, wenn die Macht- und Informationsasymmetrie so groß ist, dass es weder verfügbare Alternativen zur Auswahl gibt (wie es bei der Nutzung von Facebook der Fall ist) noch Verhandlungsposition und technische Gegebenheiten für einen hinreichenden Einblick und die hinreichende Kontrolle hinsichtlich des nötigen Entgegenkommens (wie es im Verhältnis zwischen Diensteanbietern und per bspw. SDK einbezogenen Drittparteien der Fall ist)

[177] Grund dafür ist nicht zuletzt die Tatsache, dass die Transparentmachung der Zusammenarbeit sowie der Pflichtenaufteilung dem Betroffenen zur Verfügung gestellt werden soll und eine hinreichende Aufklärung dessen im Sinne der Art. 13, 14 DSGVO in entsprechenden Konstellationen nur mit der damit einhergehenden Kenntnis möglich ist. Vgl. *Datenschutzkonferenz*, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, S. 3 f.; *Schreiber*, ZD 2019, 55 (56).

gibt. Auch für die Verhältnismäßigkeit des damit verbundenen Eingriffs in die (Charta-)Grundrechte der in die Pflicht genommenen Akteure hätte dies Implikationen; hier träten zumindest Zweifel an der Geeignetheit des Eingriffs zutage. Diese Tatsache wird zusätzlich erschwert durch die, wie oben konstatiert, sehr geringen Hürden zur Qualifikation als gemeinsamer Verantwortlicher. Es zeigt sich somit, dass die gemeinsame Verantwortlichkeit – mag sie auch in ihren Grundgedanken auf die den EuGH-Urteilen zugrundeliegenden sowie den hier betrachteten Fällen übertragbar sein – bei näherer Betrachtung an vielen Ecken und Enden nicht richtig passt. Insbesondere Art. 26 Abs. 1 S. 2 DSGVO mit seiner Pflicht zum Abschluss einer Vereinbarung zur Koordination und Aufteilung der relevanten Pflicht geht implizit von einem Verhältnis zwischen den beteiligten Akteuren aus, das wenn nicht vollkommen gleichwertig, dann jedenfalls so gestaltet ist, dass ein Aushandlungsprozess stattfinden kann, zu dem beide Beteiligten beitragen. Zwar ist nicht von der Hand zu weisen, dass auch im Falle der so typischen *take it or leave it*-Situation noch eine eigenverantwortliche Entscheidung und Handlung *pro* Nutzung der jeweiligen Infrastruktur oder des jeweiligen Drittanbieters vorliegt, sodass der handelnde Akteur nicht völlig verantwortungslos bleiben darf. Das heißt aber nicht, dass der Realität einer im Detail nun einmal vorliegenden Unmöglichkeit der Einflussnahme auf die einzelnen Umstände nicht durch die Ausgestaltung der Verantwortlichkeit Rechnung getragen werden sollte – nicht nur aus Gründen der Legitimität und der Achtung der Rechte der in die Pflicht genommenen Akteure, sondern insbesondere aus Gründen der Wirksamkeit dieser Inpflichtnahme.

III. Möglichkeiten der Umgestaltung

Die konsequente und auch zielführende Entscheidung wäre es also, den vonseiten des EuGH und in begrenztem Rahmen vorher bereits der *Art. 29-Datenschutzgruppe* eingeschlagenen Weg zu Ende zu führen und die bis dato nur begrenzt ausgereifte Weiterentwicklung der gemeinsamen Verantwortlichkeit gesetzlich so zu unterfüttern und konturieren, dass Unsicherheiten auf ein Minimum reduziert werden und die *Ausgestaltung* der Verantwortlichkeit in Form der konkret auf die vorgelagerten gemeinsamen Verantwortlichen anzuwendenden Pflichten besser mit den Verursachungsbeiträgen und Handlungsfähigkeiten der betroffenen Akteure sowie mit den an sie gerichteten Wirkungserwartungen korrespondieren. Speziell hinsichtlich der gemeinsamen Verantwortlichkeit ergeben sich aus der unterkomplexen Anwendung Probleme, die damit zusammenhängen, dass der bestehende Pflichtenkatalog ohne Modifikation angewandt wird und der Verantwortliche darunter leiden muss, dass er bestimmte Pflichten, die schon konzeptionell nicht zu seinen Einflussmöglichkeiten und Fähigkeiten passen, nicht erfüllen kann. Dabei ist es grundsätzlich gerade die

Aufgabe des Gesetz- bzw. Verordnungsgebers, sich über solche wirkungsbezogenen Elemente der Verantwortlichkeitszuschreibung Gedanken zu machen, während Exekutive und Judikative – unterhalb der Schwelle des EuGH – hinreichend klare Kriterien zur Anwendung benötigen.[178]

1. De lege lata

Fraglich erscheint aber zunächst, ob die hinreichend klaren Kriterien sowie die ebenso erforderliche Konturierung und Weiterentwicklung der bis dato nur in Bruchstücken vorliegenden Konzeption der gemeinsamen Verantwortlichkeit nicht auch *de lege lata* bei entsprechender Auslegung und Rechtsfortbildung durch den EuGH und, nachgelagert, die Aufsichtsbehörden bzw. Institutionen wie den EDSA erreichbar wären. Für eine solche Konkretisierung, Konturierung und Weiterentwicklung spräche die vermeintlich schnellere und leichtere Erreichbarkeit eines solchen Ergebnisses gegenüber eines erneuten Gesetzgebungsverfahrens zur Modifikation der DSGVO. Wie langwierig und zäh die Verhandlung für solche Verfahren sich gestalten können, zeigt nicht nur die Entwicklungsgeschichte der DSGVO selbst, sondern auch die noch andauernde Entwicklung der ePrivacy-VO.[179] Demgegenüber steht aber die Tatsache, dass auch die fortgeführte Konturierung durch den EuGH bei realistischer Betrachtung langwierig verlaufen würde und auf die entsprechenden Vorlagen durch nationalstaatliche Gerichte angewiesen wäre. Gegen die Hoffnung einer homogenisierten und zielgerichteten Klärung durch die Aufsichtsbehörden spricht zudem die Uneinheitlichkeit der Herangehensweisen der einzelnen mitgliedstaatlichen Behörden, sodass auch in dieser Hinsicht eine homogene Konkretisierungsrichtung nicht ohne weiteres zu erwarten wäre.

Eine derartig weitreichende richterliche Rechtsfortbildung, wie sie der EuGH im Zusammenhang mit der gemeinsamen Verantwortlichkeit getätigt hat, bedarf im Falle einer solch komplexen Verantwortlichenstellung bei gleichzeitiger Unklarheit über entscheidende Aspekte (wer ist unter welchen Umständen Verantwortlicher? Wie weit reicht die Verantwortlichkeit?) zudem grundsätzlich zumindest im Anschluss daran einer Nachbetrachtung und Kodifizierung durch den Verordnungsgeber.[180] Das gilt erst recht für die hier vorgeschlagene, darauf

---

[178] Siehe *van Alsenoy*, CLSR 2012, 25 (39): „External considerations should in principle not enter the analysis at this point. They can and should, however, be taken into account when assessing whether or not the current framework is still tailored to deal with today's processing realities."

[179] Diese gilt derzeit nach mehreren Entwürfen sowie langen und letztlich erfolglosen Verhandlungen als gescheitert und wartet auf eine Neufassung durch die Kommission. Vgl. *Martini* in: Paal/Pauly, DSGVO/BDSG, Art. 32 Rn. 17g. *Hemmert-Halswick*, MMR-Aktuell 2019, 422777.

[180] Vgl. *Reinhardt*, AöR 2017, 528 (564), der empfiehlt, dass „eventuelle Schutzlücken durch die Gerichte nicht selber geschlossen, sondern als offene Gestaltungsaufträge an den Gesetzgeber zurückgegeben werden". Siehe zudem die Kritik von *Bassini*, Bocconi Legal Papers

aufbauende und noch mehr Akteure in die Pflicht nehmende Konkretisierung und Weiterentwicklung dieser Figur, durch die sich die ohnehin bereits weit vom Normtext entfernte Auslegung noch stärker von diesem entkoppeln und für weitere Unbestimmtheit der betroffenen Normen sorgen würde. Auch hier ließe sich insofern der oberflächliche Vergleich zum Polizeirecht bemühen, in dessen Rahmen neuartige bzw. atypische, aber eingriffsschwere[181] polizeiliche Maßnahmen als Reaktion auf neuartige bzw. atypische Situationen für einen gewissen Zeitraum auf die polizeirechtliche Generalklausel gestützt werden dürfen; sobald die Situation bekannt und die für sie verwendete Maßnahme etablierter ist und der Gesetzgeber Gelegenheit gehabt hätte, eine entsprechende Standardmaßnahme als Ermächtigungsgrundlage zu erlassen, trägt die Generalklausel diese dann hingegen nicht mehr.[182]

Wenngleich also die Konkretisierung in Form von Auslegung und richterlicher Rechtsfortbildung sowie behördlicher Anwendung der Tatbestandsmerkmale der gemeinsamen Verantwortlichkeit sowie einiger der Verantwortlichenpflichten der niedrigschwellige und daher grundsätzlich vorzugswürdige Weg wäre, um die hier vorgeschlagene Weiterentwicklung der gemeinsamen Verantwortlichkeit umzusetzen, ist die Weiterentwicklung *de lege ferenda* aus den aufgeführten Gründen und aufgrund der – im Folgenden noch darzulegenden – Menge der unterbreiteten Weiterentwicklungsvorschläge als vorzugswürdig anzusehen.

2. De lege ferenda

Diese Vorzugswürdigkeit bestätigt sich auch durch die zusätzlichen Möglichkeiten der Weiterentwicklung, die sich nicht zwingend an die jetzige Form der gemeinsamen Verantwortlichkeit halten muss. Die Nichtexistenz einer dritten Form der Verantwortlichkeit wurde in der Literatur zuweilen bereits bemängelt.[183] Ob es eine solche *zusätzliche* Verantwortlichkeit für die besprochenen Fälle zwingend bräuchte oder eine weitergehende Ausgestaltung der gemeinsamen Verantwortlichkeit mit abgespecktem oder jedenfalls flexibler anzuwendendem Pflichtenkatalog ausreicht, soll zunächst dahinstehen. Entscheidend ist in jedem Fall, dass der von *Art. 29-Datenschutzgruppe* und EuGH unisono angepriesene, aber bisher inhaltsleer belassene „unterschiedliche Grad an Verant-

2019, 103 (127) an der entsprechenden EuGH-Rechtsprechung: „Instead, the Court of Justice in certain cases seems to have drawn conclusions going beyond its mandate, with important consequences for the actors involved."

[181] Dort für den in Anspruch genommenen Störer, hier für den zusätzlich in die Pflicht genommenen neuen Verantwortlichen.

[182] Vgl. *Kingreen/Poscher*, Polizei- und Ordnungsrecht, S. 86 ff. m. w. N.

[183] Vgl. etwa *Marosi/Matthé*, ZD 2018, 357 (362): „Die Verrenkungen des EuGH, um hier zu einem bestimmten Urteil zu kommen, offenbaren allerdings auch die Schwächen des Systems der Verantwortlichkeit."

wortung"[184] operationalisierbar gemacht und einem entsprechend korrespondierenden unterschiedlichen Grad an Pflichtigkeit gegenübergestellt wird.

a) Modifikation der Verantwortlichkeitszuschreibung

Ein sinnvoller Ansatz in diese Richtung könnte es sein, unterschiedliche Konstellationen gemeinsamer Verantwortlicher zu fixieren. Die Möglichkeit mehrerer gleichberechtigter gemeinsamer Verantwortlicher existiert, wie auch einige der von der *Art. 29-Datenschutzgruppe* aufgeführten Beispielsfälle zeigen.[185] Nichtsdestotrotz sollte die DSGVO explizit widerspiegeln, dass der Normalfall – jedenfalls in den hier primär in den Blick genommenen Akteurskonstellationen – derjenige ist, in dem es einen *primären* und einen oder mehrere *sekundäre* Verantwortliche gibt. Indizien dafür, welcher Akteur die primäre Verantwortlichenstellung innehat, gibt es dabei zahlreiche: die Nähe zu den verarbeiteten Daten, die Verhandlungsposition gegenüber den anderen Akteuren, die faktische wie auch technisch vermittelte Macht, verarbeitungsrelevante Handlungen ggf. ohne Wissen und Verhinderungsmöglichkeit der anderen Akteure durchzuführen. Wenngleich die hiesigen Konstellationen um Diensteanbieter und Drittparteien in vielen Fällen keine derart großen Machtasymmetrien aufweisen, wie sie gegenüber den wenigen besonders mächtigen Plattformen wie Facebook und Google vorliegen, bedingt die mit der technischen Basis der Nutzung von Infrastrukturen und Plugins einhergehende inhärente Intransparenz dennoch eine grundlegende Informations- und teilweise auch eine gewisse Machtasymmetrie zulasten der nutzenden Diensteanbieter.[186] Auch die Tatsache, dass sie die Daten ihrer Nutzer nicht selbst aktiv an den Drittanbieter übermitteln, sondern dieser die Daten unmittelbar eigenständig abruft, ist ein zentraler Punkt. Übermittelt ein Diensteanbieter die Daten seiner Nutzer aktiv an Dritte, liegt bereits unproblematisch ein Fall zweier getrennter Verantwortlicher oder aber ein klassischer Fall gemeinsamer Verantwortlichkeit vor; einer Modifikation bedarf es dann gar nicht. Es kann daher davon ausgegangen werden, dass Diensteanbieter in den hier relevanten Fällen die Rolle des sekundären Verantwortlichen einnehmen.

Eine gesetzliche Verankerung dieser bereits auf Ebene der *Zuschreibung* der Verantwortlichkeit ansetzenden klaren Distinktion zwischen den Graden der Verantwortlichkeit würde sich gesetzessystematisch zunächst gut als Zusatz zur Definition des Verantwortlichen in Art. 4 Nr. 7 DSGVO einfügen. Da diese De-

[184] *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 39 sowie EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 43, Rs.C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 70 sowie Rs. C-25/17 (Jehovan todistajat), EU:C:2018:551 Rn. 66.

[185] Siehe *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 24 ff.

[186] Siehe dazu ausführlich *supra* in Kapitel 1 B. I.

finition jedoch noch möglichst abstrakt gehalten ist und die Möglichkeit der gemeinsamen Verantwortlichkeit bereits jetzt einzig durch die Inklusion des Wortes „gemeinsam" erkennen lässt, wäre ein solcher Zusatz hier nicht optimal, zumal die grundlegenden Voraussetzungen der Verantwortlichkeit ja gerade unangetastet bleiben sollen. Naheliegender erscheint daher ein Zusatz zu den in Art. 26 Abs. 1 DSGVO niedergelegten Grundlagen der gemeinsamen Verantwortlichkeit. Hier heißt es bisher in Satz 1:

„Legen zwei oder mehr Verantwortliche die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche."

In Betracht käme daher das Hinzufügen eines neuen, an die nachfolgenden Sätze zur Vereinbarungspflicht anschließenden, Satz 4 nach folgendem Muster:

„In Abhängigkeit des jeweiligen Einflusses auf die Festlegung ist neben der gleichwertigen Verantwortlichkeit aller Verantwortlichen auch eine Einstufung als primärer oder sekundärer Verantwortlicher möglich; die Einordnung obliegt den Verantwortlichen und erfolgt anhand einer funktionalen Betrachtungsweise unter Berücksichtigung aller Kriterien des Einzelfalls."

In Betracht käme es zudem, die Einstufung der einzelnen Verantwortlichen auch in der von ihnen anzufertigenden Vereinbarung zu fixieren und den Betroffenen gem. Abs. 2 S. 2 der Norm zur Verfügung zu stellen. Gleichzeitig sollte Art. 26 Abs. 3 DSGVO, nach dem Betroffene ihre Rechte gegenüber jedem einzelnen der Verantwortlichen geltend gemacht werden können, beibehalten werden. Auch dann, wenn – wie im folgenden Abschnitt besprochen werden soll – der unterschiedliche Grad an Verantwortlichkeit für eine unterschiedliche Pflichtenlast sorgt, muss gewährleistet bleiben, dass die Mehrzahl an Verantwortlichen und die damit einhergehende Ungewissheit, wer der korrekte Ansprechpartner ist, nicht zu ihren Lasten geht. Um aber zu verhindern, dass sekundäre Verantwortliche für die Nichterfüllung von Pflichten des primären Verantwortlichen haften müssen, die sie selbst rein faktisch gar nicht erfüllen konnten,[187] obwohl sie das Begehren des Betroffenen an diesen weitergegeben hatten, sollte ein weiterer Satz nach folgendem Muster zu Abs. 3 hinzugefügt werden:

„Die Pflicht des sekundären Verantwortlichen beschränkt sich auf die Entgegennahme und Weitergabe der von Betroffenen geltend gemachten Ansprüche und Rechte an den gemäß Vereinbarung zuständigen primären Verantwortlichen."

Dies entspricht dem Verständnis, das in der Literatur vereinzelt bereits *de lege lata* vertreten wird[188] und bietet einen überzeugenden Ausgleich zwischen Betroffenenschutz und Verantwortlichkeitslimitierung.

[187] Man denke hier etwa an die Rechte auf Auskunft und auf Löschung der Daten gem. Art. 15 und 17 DSGVO, wenn der sekundäre Verantwortliche keinen eigenen Zugriff auf die betreffenden Daten hat.

[188] Vgl. *Kollmar*, NVwZ 2019, 1740 (1742).

b) Modifikation der Verantwortlichkeitsausgestaltung

Ist nun also die Möglichkeit unterschiedlicher Grade an Verantwortlichkeit bereits auf Normebene verankert, stellt sich die Frage, wie genau eine sachgerechte und zielführende Ausgestaltung dieses Prinzips, also eine eingeschränkte Pflichtenzuteilung für sekundäre Verantwortliche, im Detail aussehen könnte. Eine solche Pflichtenzuteilung muss zwei miteinander konfligierende Zielsetzungen vereinen können: einerseits den Einzelfall hinreichend berücksichtigen, um nach Maßgabe des funktionalen Verständnisses der Verantwortlichkeit die faktischen Fähigkeiten des infragestehenden Verantwortlichen mit einfließen zu lassen, andererseits aber auch hinreichend bestimmt sein, um ausreichend Rechtssicherheit für alle beteiligten Verantwortlichen bieten zu können.

Hier bietet sich ein zweigeteilter Ansatz an. Einerseits können bestehende Verantwortlichenpflichten übernommen und angewendet werden, die in jedem Fall und unabhängig von der konkreten Einflusslage und Fähigkeit des sekundären Verantwortlichen erfüllt werden können bzw. sollten (aa)). Andererseits bietet sich die Erschaffung einer oder mehrerer neuer Pflicht(en) an, die – getreu dem generellen Konzept der DSGVO – abstrakt gehalten sind und je nach Risiko und Umständen des Einzelfalls eine unterschiedliche Reichweite haben, gleichzeitig aber eine klare Wirkrichtung aufweisen (bb)). Ein solches Pflichtenkonzept verhindert die Unsicherheit, die damit einherginge, in jedem Einzelfall jede einzelne Verantwortlichenpflicht auf ihre Anwendung auf den jeweiligen sekundären Verantwortlichen hin abzuklopfen. Gleichzeitig erlaubt die Schaffung reichweitenflexibler neuer Pflichten die nötige Offenheit, um die Ausprägung der Inpflichtnahme in Abhängigkeit der Einzelfallkriterien sachgemäß zu skalieren.

aa) Einzelfallunabhängige Anwendung existierender Pflichten

Für sekundäre gemeinsame Verantwortliche müsste also feststehen, welche der Verantwortlichenpflichten sie in jedem Fall treffen. Hierfür käme entweder ein zusätzlicher Absatz in Art. 26 DSGVO in Betracht, der diese Pflichten an zentraler Stelle abschließend aufzählt. Eine andere Möglichkeit bestünde darin, an die Vorgehensweise für den Auftragsverarbeiter anzuknüpfen und unmittelbar im Text der entsprechenden Pflichten einen Zusatz einzufügen, der klarstellt, dass die jeweilige Pflicht auf sekundäre Verantwortliche anwendbar ist (etwa in Art. 32 Abs. 1 DSGVO: „[…] treffen primäre und sekundäre Verantwortliche und der Auftragsverarbeiter […]“). Sinnvoll erscheint eine Kombination aus beiden Vorgehensweisen, die in Art. 26 DSGVO die im nächsten Abschnitt zu behandelnden eigenständigen neuen Pflichten definiert, während die jeweils anwendbaren existierenden Pflichten in ihrem jeweils eigenen Normtext auf die Anwendbarkeit auf den sekundären gemeinsamen Verantwortlichen hinweisen.

Bei der Frage, welche Pflichten anwendbar sein sollten und welche nicht, wird im Folgenden kursorisch vorgegangen, um die wichtigsten Pflichten auf ihre Tauglichkeit hin zu überprüfen, da eine vollständige Prüfung aller Pflichten den Rahmen dieser Arbeit sprengen würde.

(1) Anwendbare Pflichten

Inhaltlich bietet sich zuvorderst die Anwendbarkeit der Informationspflicht gem. Art. 13 DSGVO[189] an. Nicht umsonst stand diese in den beiden bedeutsamen EuGH-Entscheidungen im Mittelpunkt. Sekundäre Verantwortliche in Form von vorgelagerten Akteuren, die fremde Infrastrukturen oder Dienste in ihre Dienste einbinden, sind typischerweise der unmittelbare Bezugsakteur zum Betroffenen. Es muss daher in jedem Fall ihnen obliegen, bspw. darüber zu informieren, von wem im Zuge der Nutzung der Infrastruktur bzw. des Dienstes personenbezogene Daten zu welchen Zwecken und in welchem Umfang abgerufen oder weitergegeben werden. Ob diese Informierung originär durch den sekundären Verantwortlichen erfolgt oder dieser nur dafür sorgt, dass der primäre Verantwortliche seinerseits die nötigen Informationen direkt einbindet und dem Betroffenen zugänglich macht, ist letztlich irrelevant.[190] Teil der Informationen müssten, wie bereits im letzten Abschnitt geschildert, auch die wichtigsten Inhalte der Vereinbarung zwischen den gemeinsamen Verantwortlichen gem. Abs. 26 Abs. 2 S. 2 DSGVO sein. Entscheidend ist nun nachfolgend, wie eine solche Pflicht mit der Tatsache umgehen würde, dass der primäre Verantwortliche schlicht keine oder keine hinreichenden Informationen über seine Verarbeitungsvorgänge mitteilt. Nach jetzigem Verständnis von EuGH und BVerwG führt jedenfalls die Nichterteilung der Information, wie sie in den beiden Fällen Wirtschaftsakademie und Fashion ID zur Geltung kam, zu einer Rechtswidrigkeit der Datenverarbeitung und zu einer jedenfalls in bestimmten Fällen zulässigen Sanktionierung des gemeinsamen Verantwortlichen durch die Aufsichtsbehörde. Im Ergebnis bedeutet dies wohl, dass auch die gar nicht oder nur lückenhaft erfolgte Übermittlung der relevanten Informationen durch einen (primären) gemeinsamen Verantwortlichen (wie in den EuGH-Fällen Facebook) dazu führen kann, dass der sekundäre Verantwortliche trotz bestem eigenem Bemühen datenschutzwidrig handelt und haften muss, weil der von ihm gewählte Kooperationspartner seinen Teil nicht beiträgt bzw. beitra-

[189] Art. 14 DSGVO, der die Informationspflicht bei Erhebung der Daten *nicht* unmittelbar beim Betroffenen betrifft, spielt hier keine Rolle, da die betrachtete Akteursgruppe des Diensteanbieters definitionsgemäß dem Betroffenen unmittelbar gegenübersteht und Daten bei ihm erhebt.

[190] Diese Tatsache verkennt der EuGH in Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 102 f., wenn er ausführt, dass die Informationspflicht durch den Websitebetreiber zu erfüllen ist, weil nur dieser im infragestehenden Zeitpunkt unmittelbar mit dem Seitenbesucher interagiert.

gen will. Zwar ließe sich argumentieren, dies liege eben im Risiko des sekundären Verantwortlichen und dieser habe sich schließlich durchsetzen oder, bei fehlender Durchsetzung, idealerweise einen anderen, zuverlässigeren Kooperationspartner suchen müssen. Eine solch strikte, letztlich auf das Verbot der Nutzung einer Vielzahl von Anbietern gerichtete Lesart der Pflicht ist aber, wie bereits mehrfach angeklungen, kaum zielführend. Zum einen ignoriert sie die faktischen Machtverhältnisse zwischen den betreffenden Akteursgruppen im digitalen Raum, die in den allermeisten Fällen eine große Asymmetrie aufweisen und einzelnen Diensteanbietern keine Verhandlungsbasis geben – es herrscht typischerweise ein Klima des *take it or leave it*.[191] Auch stehen, wie die beiden EuGH-Urteile zeigen, häufig keine ernsthaften Anbieteralternativen zur Auswahl, wenn besonders marktmächtige und in ihrem spezifischen Angebot quasi konkurrenzlose Akteure involviert sind.[192] Zielführender wäre daher ein flexibleres Verständnis der Informationspflicht, das in der Anwendung darauf hinausläuft, den sekundären Verantwortlichen zur Übermittlung derjenigen Informationen zu verpflichten, die ihm zur Verfügung stehen. Verbunden werden sollte diese Pflicht mit einer Sekundärpflicht dazu, jegliche im Rahmen des Möglichen und Zumutbaren stehenden Bemühungen anzustrengen, die nötigen Informationen vom primären Verantwortlichen zu bekommen. Hat der sekundäre Verantwortliche dies getan und die ihm nach Abschluss dieser Bemühungen zur Verfügung stehenden Informationen übermittelt, hat er seiner Pflicht Genüge geleistet und liegt das datenschutzwidrige Verhalten allein beim primären Verantwortlichen, der dafür naturgemäß unmittelbar haftbar gemacht werden kann. Eine Anpassung des Normtextes von Art. 13 DSGVO wäre dafür zwar nicht zwingend, aber jedenfalls im Interesse der Normenklarheit angebracht.

Neben dieser noch unmittelbar an die verarbeiteten Daten und die mit ihnen verfolgten Zwecke anknüpfenden Pflicht bieten sich für sekundäre Verantwortliche, die nach Maßgabe der hier betrachteten Fallszenarien typischerweise weder direkten Zugriff auf die verarbeiteten Daten noch unmittelbaren Einfluss auf den Akt der Datenerhebung durch den primären Verantwortlichen haben, vor allen Dingen diejenigen Pflichten an, die die Verarbeitungsumgebung betreffen und auf Systemgestaltung und Einrichtung technisch-organisatorischer

---

[191] Besonders symptomatisch zeigt sich dieses Phänomen im Verhältnis zwischen Google und Presseverlegern in Bezug auf die Nutzungsbedingungen von Google Ads. Eine Gruppe von Verlegern machte im Zuge des Wirksamwerdens der DSGVO in einem offenen Brief auf die einseitig und zu ihren Lasten angewandten Bedingungen aufmerksam und kritisierte den Mangel an Transparenz und Verhandlungsmöglichkeiten: „You refuse to provide publishers with any specific information about how you will collect, share and use the data", siehe *Natasha Lomas*, Google accused of using GDPR to impose unfair terms on publishers, Techcrunch.com vom 01.05.2018 (https://techcrunch.com/2018/05/01/google-accused-of-using-gdpr-to-impose-unfair-terms-on-publishers/). Zuletzt abgerufen am 14.01.2022.

[192] Zur Vornahme der Marktabgrenzung für Internetplattformen am Beispiel sozialer Netzwerke siehe *Podszun*, GRUR 2020, 1268 (1269).

Maßnahmen gerichtet sind. Von besonderer Relevanz dürfte hier die Scharnierpflicht[193] des Art. 24 DSGVO in Verbindung mit den Pflichten zu *privacy by design* und *by default* gem. Art. 25 DSGVO sowie der Pflicht zu Datensicherheit nach Art. 32 DSGVO sein. Führt man sich erneut vor Augen, dass der dem sekundären Verantwortlichen „vorwerfbare"[194] Akt der Einflussnahme auf die Datenverarbeitung einerseits die Ermöglichung der Verarbeitung durch den primären Verantwortlichen, andererseits die gemeinsame Zweckfestlegung in Form des Wissens um die ermöglichte Verarbeitung und eines irgendwie gearteten gemeinsamen Vorteils (wohl wirtschaftlicher Natur) in deren Folge ist, liegt es nahe, die an diesen Akt der Ermöglichung und deren Art und Weise anknüpfenden Pflichten in den Mittelpunkt der Pflichtigkeit zu stellen. Sekundäre Verantwortliche sollten daher stets dazu verpflichtet sein, im Rahmen des Möglichen und Zumutbaren bereits proaktiv Maßnahmen zu ergreifen, die das mit Nutzung oder Einbezug des primären Verantwortlichen einhergehende Risiko schmälern. Der risikobasierte Ansatz[195] der Norm in Verbindung mit den (technischen wie auch finanziellen) Möglichkeits- und Zumutbarkeitserwägungen der speziellen Pflichten in Art. 25 und 32 DSGVO[196] erlaubt hier ein gutes Maß an Flexibilität. *In concreto* könnten diese Pflichten dann beispielsweise darauf gerichtet sein, den mit der Nutzung bestimmter Technologien und Einbezugsmodalitäten wie etwa SDKs und anderer Plugins einhergehenden Risiken bewusst entgegenzuwirken und ggf. existierende Alternativmethoden zu verwenden, wo sie verfügbar sind, aber auch die technische Entwicklung im Blick zu behalten, um später aufkommende, risikoärmere Alternativen ggf. wahrnehmen zu können. Ein Beispiel für solche Maßnahmen bei der Ausgestaltung der Nutzungsbedingungen ist etwa die Möglichkeit, Google Fonts zur Nutzung auf der eigenen Website nicht als Fremdcode von Googles Servern zu laden, sondern auf dem eigenen Server zu hosten, um so die Übermittlung von Besucherdaten an Google gänzlich zu verhindern.[197] Auch die Abwahl bestimmter Möglichkeiten, um so die Übermittlung von Daten zu verringern, kann eine geeignete Maßnahme sein. Hier muss freilich stets beachtet werden, inwieweit die Alternativnutzung auch zu einem geringeren Nutzen der Kooperation für den sekundären Verantwortlichen führt. Nicht jede Maßnahme kann von ihm verlangt werden, wenn ihre Einführung bedeutet, dass die

---

[193] *Petri*, in: Simitis u. a., DSGVO/BDSG, Art. 24 DSGVO Rn. 1 spricht hier von einer „Verknüpfung von Verarbeitungsgrundsätzen und relativ konkreten technisch-organisationsrechtlichen Vorgaben".

[194] Im Sinne von: die Schwelle des verantwortlichkeitsrelevanten Verursachungszusammenhangs überschreitend.

[195] Siehe *Schröder*, ZD 2019, 503 (503 ff.) für die Grundlagen dieses Ansatzes.

[196] Diese berücksichtigen etwa den aktuellen Stand der Technik und Implementierungskosten der infrage kommenden Maßnahmen.

[197] Siehe hierzu die entsprechende Anleitung unter https://wiki.selfhtml.org/wiki/HTML/Tutorials/Google-Fonts_selbst_hosten. Zuletzt abgerufen am 14.01.2022.

Kooperation faktisch komplett ihren Nutzen verliert. Eine risikoärmere Variante kann auch eine sein, die von sich aus nicht datensparsamer oder sicherer ist, dem Diensteanbieter aber ein Mehr an Kontrolle und/oder Transparenz erlaubt.

Eng verknüpft mit den vermittels Art. 24 DSGVO anwendbaren risikosensiblen technisch-organisatorischen Pflichten ist die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung gem. Art. 35 DSGVO.[198] Diese sollte in den Fällen des Einbezugs fremder und eigenständig datenverarbeitender Infrastrukturen und Dienste regelmäßig Pflicht sein, eine entsprechende Aufnahme in die Liste in Abs. 3 der Norm wäre daher geboten. Vorgelagert zur Durchführung der eben geschilderten technisch-organisatorischen Maßnahmen sollten sekundäre Verantwortliche somit verpflichtet sein, die mit dem Einbezug eines Akteurs auf eine spezifische Art und Weise (wie etwa per SDK) einhergehenden Risiken bereits proaktiv zu ermitteln und die Notwendigkeit von Abhilfemaßnahmen abzuschätzen sowie konkrete Maßnahmen heranzuziehen und auf ihre Wirksamkeit hin zu begutachten.

Fraglich ist zuletzt, ob sekundäre Verantwortliche eine eigene Rechtsgrundlage für die Verarbeitung vorweisen müssen sollten. Gesicherter *status quo* ist derzeit seit der Fashion ID-Entscheidung des EuGH, dass jeder gemeinsame Verantwortliche eine eigene tragfähige Rechtsgrundlage haben muss.[199] Überzeugend erscheint dies in jedem Fall dort, wo, wie etwa im Falle Wirtschaftsakademie, der sekundäre Verantwortliche (s)einen Vorteil aus der Kooperation (unter anderem) dadurch gewinnt, dass die als Endprodukt der von ihm ermöglichten Datenverarbeitung entstandenen Informationen von ihm genutzt werden können. Lässt also ein Fanpage-Betreiber Statistiken über die Besucher seiner Seite oder ein App-Anbieter Statistiken über die Benutzer seiner App erstellen, so braucht er dafür in gleichem Maße eine Rechtsgrundlage, wie wenn er die Verarbeitung selbst durchführen würde. Hier trägt die Kooperation mit der Drittpartei starke Züge von der mit einem Auftragsverarbeiter; auch in einer solchen Konstellation wäre der Auftraggeber ohne weiteres Verantwortlicher und benötigte eine eigene und tragfähige Rechtsgrundlage. Dass gleichzeitig auch die Verarbeitungen, die die Drittpartei zu ihren eigenen Zwecken (die freilich mit denen des sekundären Verantwortlichen *kongruent* sind)[200] und Vorteilen durchführt, ermöglicht werden, negiert diese Komponente und damit das Bedürfnis nach einer eigenen Rechtsgrundlage nicht.

---

[198] Zur Bedeutung dieser Pflicht im Kontext der Instrumente des Gesamtkonzepts der Verantwortlichkeit siehe *supra* bei Kapitel 2 B. I. 1. d) und e).

[199] Vgl. EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 97, nach dem insbesondere jeder Verantwortliche eigene berechtigte Interessen benötigt, die gem. Art. 6 Abs. 1 lit. f. stärker als die des Betroffenen wiegen müssen.

[200] Siehe die Ausführungen zu den Voraussetzungen der gemeinsamen Verantwortlichkeit bei Kapitel 2 C. II. 4.

Fraglich ist weiterhin, ob dies auch in den vielen Fällen gelten sollte, in denen der eigene Nutzen der Kooperation in keiner so offensichtlichen und engen Verbindung zu den verarbeiteten Daten oder daraus gewonnenen Informationen steht. Wenn etwa schlicht die Möglichkeit des Datenabrufs monetarisiert wird, ohne dass der Diensteanbieter im Nachgang einen konkreten Nutzen aus den aus den Daten gewonnenen Informationen gewinnt, liegt zwar im Sinne der gemeinsamen Verantwortlichkeit immer noch eine Verarbeitung vor, die sich *auch* als diejenige des sekundären Verantwortlichen darstellt, dennoch aber ist die innere Verbindung zu seinen Beiträgen und seinem verfolgten Zweck und gezogenen Nutzen schlicht nicht eng genug. Einer eigenen Rechtsgrundlage darf es hier also nicht bedürfen. Die Konsequenz daraus aber darf deshalb nicht sein, dass die Verantwortlichkeit des sekundären Verantwortlichen vollkommen unabhängig davon ist, ob der primäre Verantwortliche eine taugliche Rechtsgrundlage als grundlegendste Voraussetzung für die Rechtmäßigkeit der betreffenden Verarbeitungen hat und vorweisen kann. Eine taugliche Neuschöpfung einer entsprechenden Pflicht, die anstelle der Pflicht zu einer eigenen Rechtsgrundlage anwendbar sein sollte, soll deswegen in (bb)) vorgestellt werden.

Insgesamt bleibt naturgemäß bei all den genannten Pflichten weiterhin eine nicht unerhebliche Restunsicherheit. Diese geht aber oftmals – so etwa bei den sehr abstrakten technisch-organisatorischen Pflichten – schon von der generellen Fokussierung der DSGVO auf abstrakte und risikosensible Pflichten aus und wird durch die gemeinsame Verantwortlichkeit nicht noch zusätzlich verschärft. Hier ist daher auf dieselben, zumindest auf dem Papier in der DSGVO angelegten, Mechanismen zur Beseitigung von Rechtsunsicherheit abzustellen: die Interaktion mit Aufsichtsbehörden und Interessenverbänden, aber auch die Nutzung der eigenen Handlungsoptionen in Form von genehmigten Verhaltensregeln und Zertifizierungen gem. Art. 40 und 42 DSGVO.

(2) Nicht anwendbare Pflichten

Als Annex zu den in jedem Fall anwendbaren Pflichten soll nun kurz auf diejenigen Pflichten eingegangen werden, die auf sekundäre Verantwortliche mit Blick auf die diesen Konstellationen typischerweise zugrundeliegenden Beziehungsgeflechte prinzipiell nicht anwendbar sein sollten. Die Szenarien, in denen der sekundäre Verantwortliche keiner eigenen Rechtsgrundlage bedarf, wurden im vorangegangenen Abschnitt bereits beschrieben.

Des Weiteren können zuvorderst alle weiteren, über Art. 13 DSGVO hinausgehenden,[201] Betroffenenrechte genannt werden. Vergegenwärtigt man sich, dass ein typisches Charakteristikum sekundärer Verantwortlicher darin besteht,

[201] Sofern man diesen, der zwar eine unmittelbare Pflicht und kein Recht beinhaltet, nichtsdestoweniger aber im „Rechte der betroffenen Personen" betitelten Kapitel 3 der Verordnung beheimatet ist, als Betroffenenrecht klassifizieren will.

dass der Einbezug des primären Verantwortlichen so erfolgt, dass dieser ohne weiteres Zutun und ohne Transparenz eigenständig Daten abrufen kann, so liegt nahe, dass die unmittelbar auf Bestand, Nutzung und Attribute (wie etwa Richtigkeit) der Daten gerichteten Pflichten kaum je von einem sekundären Verantwortlichen erfüllt werden können. Wie bereits bei der oben angesprochenen Pflicht nach Art. 13 DSGVO ist hier daher stattdessen ein Verständnis zu wählen, nach dem die Betroffenen ihre Rechte gegenüber dem sekundären Verantwortlichen geltend machen können, dieser aber nur zur Weitergabe dieses Verlangens an sowie zur Einwirkung auf den primären Verantwortlichen bzgl. Erfüllung verpflichtet ist.

bb) Flexible Anwendung einer Auswahl- und Überwachungspflicht

Nach diesem Abgleich mit den bestehenden Verantwortlichenpflichten der DSGVO, die nur teilweise Anwendung auf den sekundären Verantwortlichen finden sollen, bedarf es einer übergeordneten Pflicht, die im Kern dasjenige Handlungsvermögen in den Blick nimmt, das mit den Beiträgen und Einflüssen korrespondiert, die bei genauer Betrachtung in erster Linie dafür gesorgt haben, dass er die Schwelle zur Verantwortlichkeit überschritten hat. Im Kern ist dies, bei einer streng beitragsfokussierten Betrachtung, die die Zweckkongruenz als quasi-subjektives Element außen vor lässt, die Verursachung der stattfindenden Verarbeitung(en) durch entweder die Nutzung einer fremden Infrastruktur als Basis oder den Einbezug eines fremden Akteurs in das eigene Angebot. Wenngleich am Ende eine Verantwortlichkeit *für* eine Datenverarbeitung oder Verarbeitungsreihe besteht, die sich eben im Rahmen der von ihm beeinflussten Verarbeitungsphasen *auch* als diejenige des sekundären Verantwortlichen darstellt, darf dies nicht darüber hinwegtäuschen, dass hinter dieser Formulierung eine datenschutzspezifische Umschreibung eines ganz spezifischen Lebenssachverhalts steht. Noch stärker als bei der klassischen Verarbeitung des einzelnen Verantwortlichen, bei der der Begriff eine Vielzahl unterschiedlichster Handlungsszenarien und -konstellationen abdeckt, ist der Lebenssachverhalt hier von vornherein eng begrenzt. Es erscheint daher nur sachgemäß, dass eine zentrale Pflicht für die Rechtmäßigkeit dieses Handelns auch an das infragestehende Handeln selbst anknüpft.

Als eine potenziell geeignete Möglichkeit bietet sich hier daher eine generelle Sorgfaltspflicht für sekundäre Verantwortliche hinsichtlich der Auswahl und anhaltenden Überwachung ihrer Kooperationspartner sowie der Ausgestaltung der Kooperationsbedingungen an. Sekundäre Verantwortliche müssen im Rahmen einer solchen Pflicht stets das in ihrer Macht stehende tun, um bei der Auswahl ihrer Kooperationspartner im Rahmen der gegebenen Möglichkeiten nur datenschutzkonform handelnde Partner zu wählen. Zudem sind sie verpflichtet, im Rahmen ihrer Möglichkeiten Einfluss auf die vertragliche, technische

und sonstige Ausgestaltung des Kooperationsverhältnisses zu nehmen. Verorten ließe sie sich idealerweise abermals in Art. 26 DSGVO, im Zusammenhang mit der oben bereits geschilderten Aufnahme eines separaten Absatzes für die Figur des sekundären Verantwortlichen.

Punktuell wurde eine solche Pflicht, teils im Rahmen einer gänzlich eigenständigen Auswahl- und Überwachungsverantwortung, bereits in Literatur wie auch Rechtsprechung diskutiert.[202] Ausgangspunkt waren auch hier die den zentralen EuGH-Entscheidungen zugrundeliegenden Fälle, in deren Zusammenhang insbesondere vor Urteilsspruch des EuGH händeringend nach Möglichkeiten gesucht wurde, trotz der damals noch vermuteten Nicht-Verantwortlichkeit etwa eines Fanpage-Betreibers nach klassischen Maßstäben der datenschutzrechtlichen Verantwortlichkeit diesen und andere Akteure in ähnlichen Konstellationen noch für sein bzw. ihr Handeln verantwortlich zu machen. Auch das BVerwG beschäftigte die Frage: In seiner zweiten Vorlagefrage an den EuGH in der Sache Wirtschaftsakademie ersuchte es von diesem die Antwort auf die Frage, ob die aus Art. 17 Abs. 2 DSRL stammende Pflicht, nur Auftragsverarbeiter zu wählen, die eine hinreichende Gewähr für ausreichende technisch-organisatorische Maßnahmen bieten können, auch in anderen Konstellationen bestehen oder nach nationalem Recht begründet werden könnte.[203] Der EuGH selbst sah in seinem Urteil bereits eine klassische datenschutzrechtliche Verantwortlichkeit des Fanpage-Betreibers als gegeben an, sodass er von einer Beantwortung dieser, letztlich hilfsweisen, Frage gänzlich absah.[204] Auch in der Sache Fashion ID kam mit der Vorlagefrage der hilfsweisen Anwendbarkeit des nationalstaatlichen Instituts der Störerhaftung eine Überlegung auf, die in eine ähnliche Richtung wies, nämlich eine Verpflichtung einer Person, „alles in ihrer Macht Stehende und ihr Zumutbare zu tun, um den Eintritt dieser Rechtsverletzung zu verhindern".[205] Auch hier wurde dieser Frage im endgültigen Urteil kein weitergehender Platz eingeräumt, weil es auf ihre Beantwortung nicht mehr ankam. Dennoch zeigen die beiden Vorlagefragen, dass hinter den Überlegungen der Einstufung der betreffenden Akteure als gemeinsame Verantwortliche stets die konkrete Stoßrichtung stand, „von den Unternehmen zu erwarten, dass sie bei der Auswahl ihres Dienstleisters sorgfältig sind".[206]

---

[202] Siehe etwa *Martini/Fritzsche*, NVwZ-Extra 2015, 1 (9 ff.).

[203] EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 24.

[204] Vgl. EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388 Rn. 44: „Nach alledem ist auf die erste und die zweite Frage zu antworten, dass […] der Begriff des ‚für die Verarbeitung Verantwortlichen' im Sinne dieser Bestimmung den Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage umfasst."

[205] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 109.

[206] Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 64, der hier die in die gleiche Richtung gehende, im Rahmen des Verfahrens geäußerte Erklärung der belgischen Regierung unterstützt.

Die in den letzten Abschnitten mehrfach erwähnten Macht- und Informationsasymmetrien, die Diensteanbietern in den allermeisten Fällen nahezu keine Verhandlungsmacht und häufig auch wenig Ausweichmöglichkeiten lassen, stehen nur scheinbar in Widerspruch zu einer solchen Pflicht. Denn wie schon bei den im vorangegangenen Abschnitt behandelten risikosensiblen Pflichten bietet sich hier eine Flexibilität in der Reichweite und Prüfstrenge der Pflicht an, die entsprechend der jeweiligen Akteurskonstellation im Einzelfall zu unterschiedlichen Ergebnissen führen kann. Diese Flexibilität einer solchen Sorgfaltspflicht in Verbindung mit den im vorangegangen Abschnitt beschriebenen Pflichten ist gerade ihr Vorteil gegenüber einem zu strikten Pflichtenkatalog, der letztlich auf ein bloßes Verbot zur Nutzung jedweder Plugins und Infrastrukturen hinausliefe. Generalanwalt *Bobek* ist zuzustimmen ist, wenn er sagt:

„Schließlich gilt, dass keine gute (Auslegung einer) Regel dazu führen sollte, dass die darin vorgesehenen Verpflichtungen von den jeweiligen Adressaten tatsächlich nicht erfüllt werden können. Soll also die […] Verantwortlichkeit nicht in eine an alle Akteure gerichtete und gerichtlich gestützte Anordnung mutieren, offline zu gehen und soziale Netzwerke, Plugins sowie gegebenenfalls sonstige Drittinhalte nicht mehr zu nutzen, muss bei der Bestimmung der Verpflichtungen und Verantwortlichkeiten die Lebenswirklichkeit eine Rolle spielen […].“[207]

Eine Pflicht zur sorgfältigen Auswahl, Überwachung und Ausgestaltung von Kooperationspartnern und Kooperationsbedingungen kann dieser Anforderung hinsichtlich der Berücksichtigung der Lebenswirklichkeit dann Genüge leisten, wenn sie ein ausreichend großes Spektrum an Erwartungen und möglichen Konsequenzen abdeckt und alle wichtigen Kriterien zur Bestimmung im Einzelfall berücksichtigt. Zu diesen Kriterien sollten die ebenfalls von Generalanwalt *Bobek* genannten Aspekte wie Kenntnis, originäre Verhandlungsmacht und Möglichkeiten der Einflussnahme,[208] darüber hinaus aber auch beispielsweise die Möglichkeit des Ausweichens auf alternative Angebote zählen.

Im ersten Schritt würde eine solche Sorgfaltspflicht also bedeuten, im Vorfeld sicherzustellen, dass der angestrebte Kooperationspartner die mit der Kooperation bezweckten und ermöglichten Datenverarbeitungen datenschutzkonform durchführt. Dazu kann es gehören, alle notwendigen Informationen über die zu verarbeitenden Daten, Verarbeitungszwecke sowie die gewählte Rechtsgrundlage einschließlich näherer Details[209] vom primären Verantwortlichen einzufordern. Daneben lassen sich hier erneut die bereits aus dem Um-

---

[207] Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 93.

[208] Vgl. Generalanwalt *Michal Bobek*, Schlussanträge zu EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2018:1039 Rn. 93.

[209] So etwa die genauen Umstände bei der Einholung einer Einwilligung gem. Art. 6 Abs. 1 lit. a oder der Weg zur Abwägungsentscheidung, wenn der primäre Verantwortliche sich auf die Verarbeitung zu Wahrung berechtigter Interessen gem. Art. 6 Abs. 1 lit. f DSGVO beruft.

feld der Auftragsdatenverarbeitung bekannten Pflichten aufführen, nach denen der Pflichtige sich hinreichende Garantien präsentieren lassen muss, die aufzeigen, dass und inwiefern ausreichende technische und organisatorische Maßnahmen getroffen wurden.[210] Wo Kooperationspartner dies nicht von sich aus anbieten, muss versucht werden, entsprechende Kooperationsbedingungen auszuhandeln. Kurz gesagt: Sekundäre Verantwortliche dürfen sich primäre Verantwortliche als Kooperationspartner nur dann aussuchen, wenn sie im Rahmen ihrer Möglichkeiten sichergehen können, dass diese stets datenschutzkonform handeln oder diesbezüglich jedenfalls die ihrerseits größtmöglichen Bemühungen an den Tag legen. Ist ein solcher Kooperationspartner gefunden, setzt sich die Pflicht auch im Fortgang der Kooperation fort und hält den sekundären Verantwortlichen dazu an, veränderte Praktiken im Blick zu behalten und insbesondere dann die Kooperation einzustellen, wenn trotz erteilter Garantien datenschutzwidriges Verhalten bekannt wird. Hier zeigt sich zudem ein Ansatzpunkt, an dem die im nachfolgenden Abschnitt zu behandelnden Pflichten im Rahmen der Verantwortlichkeit für Plattformbetreiber die Fähigkeiten von Diensteanbietern unterstützen können.[211]

Doch was ist nun die Rechtsfolge, wenn die Auswahl des Kooperationspartners diesen Anforderungen an eine sorgsame Auswahl nicht genügt, weil der gewählte Partner nicht transparent genug ist, nicht genügend Garantien vorzeigen kann und insgesamt erhebliche Zweifel an der Datenschutzkonformität seines Handelns lässt? Hier könnten die offenen Begriffe des „Zumutbaren“ und „Möglichen“ als Stellschrauben und Einfalltüren für den Einbezug der berücksichtigungswürdigen Lebenssachverhalte dienen. Besteht in der Realität daher etwa eine besonders ausgeprägte Machasymmetrie wie gegenüber Facebook, Google oder Amazon, so müssen sich die Anforderungen an die Bemühungen des sekundären Verantwortlichen bzgl. der Ausgestaltung der Kooperationsbedingungen entsprechend verringern – wo ein *take it or leave it*-Modell vorherrscht, das keine individuellen Verhandlungen zulässt, hilft auch eine Pflicht zum Verhandeln nicht weiter. Gleiches gilt für Fälle, in denen schlicht keine Ausweichmöglichkeiten auf andere, datenschutzkonformere Kooperationspartner möglich sind. Würde man es hier ahnden, dass der sekundäre Verantwortliche sich nicht sorgfältiger nach einem (nicht existierenden) anderen Partner umgesehen hat, würde man letztlich doch wieder pauschal die Nutzung bestimmter Dienste und Branchen verbieten.

Die Reichweite der Auswahl- und Überwachungspflicht sollte daher je nach Lebenswirklichkeit einen Punkt auf dem Spektrum zwischen bloßer sorgfältiger Best Practice-Auswahl bis hin zum Verbot der Nutzung bestimmter einzelner

[210] Vgl. hierzu Art. 28 Abs. 1 DSGVO, dessen Vorgängernorm, Art. 17 Abs. 2 DSRL, wie erwähnt bereits im Zusammenhang mit der Wirtschaftsakademie-Entscheidung des EuGH erwähnt wurde.

[211] Siehe *infra* bei D.

Anbieter darstellen. Zu letzterem darf sich die Pflicht dabei nur dann als *ultima ratio* verdichten und konkretisieren, wenn es ernsthafte Ausweichmöglichkeiten zum infragestehenden Kooperationspartner gibt. Hier, ebenso wie in Fällen des Aufrechterhaltens der Kooperationsbeziehung trotz Bekanntwerden datenschutzwidriger Praktiken, verdichtet sich die Pflicht also zu einer, die das *Ergebnis* der Auswahl überprüft. In den übrigen Fällen, in denen die Machtasymmetrien so groß sind, dass weder Verhandlungs- noch Ausweichmöglichkeiten bestehen, nimmt die Dichte hingegen ab und „nur" der *Prozess* und die Bemühungen der Auswahl werden überprüft.

Auch diese Pflicht brächte naturgemäß ein großes Maß an Abstraktheit und damit auch Unsicherheit mit sich. Wie bei allen abstrakten und ausfüllungsbedürftigen Pflichten der DSGVO müsste sie durch Anwendung und Konkretisierung durch sekundäre Verantwortliche sukzessive mit Leben gefüllt werden. Insbesondere die Frage, wann eine zumutbare Ausweichmöglichkeit bei der Wahl eines Kooperationspartners gegeben ist, dürfte oftmals nur mit großen Schwierigkeiten zu beantworten sein. In vielen anderen Fällen ist eine Ausweichmöglichkeit offensichtlich nicht gegeben, sei es, weil der vom Kooperationspartner angebotene Mehrwert nahezu einzigartig ist (siehe etwa die Reichweite einer Facebook-Fanpage) oder weil die existierenden Alternativpartner offensichtlich die gleichen Datenschutzmaßstäbe an den Tag legen wie der in den Blick genommene Akteur (siehe etwa die Auswahl zwischen Facebook oder Google hinsichtlich *social login*-Angeboten)[212]. Hier erweckt eine bloß auf das Mögliche und Zumutbare begrenzte Pflicht zunächst den Anschein, zu kurz zu greifen und die Pflichtigen zu leicht aus der Verantwortlichkeit zu entlassen. Man sollte sich jedoch stets die begrenzten Einflussmöglichkeiten sekundärer Verantwortlicher vor Augen führen und damit die Lebenswirklichkeit der Regelungsmaterie im Blick behalten. Zudem sollte nicht vergessen werden, dass die hier verfolgte konzeptionelle Weiterentwicklung der gemeinsamen Verantwortlichkeit neben dem sekundären Verantwortlichen weiterhin eine volle primäre Verantwortlichkeit der in diesen Fällen datenschutzwidrig handelnden Akteure bestehen lässt. Das systematisch datenschutzwidrige Handeln gesamter Branchen oder einzelner, singulär mächtiger Akteure auf dem Rücken vorgelagerter Akteure mit bloß geringen Einflussmöglichkeiten zu bekämpfen, indem man diese zu teils völliger Abstinenz verpflichtet, ist daher weder verhältnismäßig noch rechtspolitisch zielführend. Ziel des Datenschutzes muss es sein, „kran-

[212] Erst kürzlich führte Apple ein eigenes *single sign-on*-Feature ein, das explizit auf die eigene Nutzung von Daten verzichtet und darüber hinaus den Schutz von Nutzerdaten vor der Weitergabe an die jeweiligen Diensteanbieter und Drittparteien verspricht. Hier zeigt sich also ein gutes Beispiel für die Entwicklung möglicher Alternativanbieter. Siehe *Lily Hay Newman*, ‚Sign In With Apple' Protects You in Ways Google and Facebook Don't, Wired vom 06.04.2019 (https://www.wired.com/story/sign-in-with-apple-sso-google-facebook/). Zuletzt abgerufen am 14.01.2022.

ke“ Geschäftsmodelle und Akteure effektiv und unmittelbar zu regulieren und nicht durch Bestrafung der sie nutzenden Akteure als letztes Glied der Kette schlicht den Weg des geringsten Widerstandes zu gehen. Der mit einer derart weitreichenden Verpflichtung bezweckte Druck auf systematisch datenschutzwidrig handelnde Akteure,[213] der mittelbar zu einer solchen Regulierung beiträgt, wird zudem durch die hier vorgeschlagene Pflicht in begrenztem Maße ebenfalls ausgeübt. Die Wirkung der Auswahl- und Überwachungspflicht sollte zudem zwingend im Zusammenspiel mit den im nächsten Abschnitt noch zu behandelten Pflichten für Plattformbetreiber betrachtet werden, welche – die Einbettung des betreffenden Diensteanbieters in eine Plattform vorausgesetzt – darauf gerichtet sind, die Macht- und Transparenzasymmetrien sekundärer Verantwortlicher abzumildern und so zu einer besseren Befähigung zur Pflichtenerfüllung hinzuwirken.[214]

IV. Zwischenergebnis – Bestandsaufnahme des Ansatzes

Was lässt sich also abschließend zur gemeinsamen Verantwortlichkeit als Ansatz zur Lösung der drohenden Dysfunktionalität des Gesamtkonzepts der datenschutzrechtlichen Verantwortlichkeit sagen? In ihrem derzeitigen, durch den EuGH geschaffenen und durch erste Versuche nationaler Aufsichtsbehörden und Gerichte wie auch EDSA[215] leidlich mit Leben gefüllten Zustand kann sie als nicht mehr als ein erster Schritt in Richtung eines aufgefüllten Verantwortungsvakuums angesehen werden. Gleichzeitig öffnet sie durch ihre (zu diesem Zeitpunkt) große Unbestimmtheit und Weite mehrere neue Problemstellen, die sich mit dem bestehenden gesetzlichen Instrumentarium nicht in Gänze lösen lassen. Der auf den vorangehenden Seiten unterbreitete Ansatz einer Umgestaltung und Weiterentwicklung der gemeinsamen Verantwortlichkeit bietet daher einen Ansatz für eine tragfähigere Lösung eines Teils der Probleme.

Dabei trägt er einerseits der vermeintlich widersprüchlichen Tatsache Rechnung, dass Diensteanbieter bei der Nutzung fremder datenverarbeitender Infrastrukturen bzw. dem Einbezug dritter datenverarbeitender Parteien zwar einen entscheidenden Beitrag zur Ermöglichung der nachfolgenden Datenverarbeitungen leisten, zugleich aber nur sehr begrenzte unmittelbare Einflussmöglichkeiten besitzen und meist Opfer immenser Kontroll-, Transparenz- und Machtasymmetrien sind. Der dieser Realität folgende Ansatz der Auftrennung in

[213] Vgl. *Globocnik*, IIC 2019, 1033 (1042). So auch bereits explizit Generalanwalt *Yves Bot*, Schlussanträge zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2017:796 Rn. 74: „Außerdem ist eine aktive Einbeziehung […] durch ihre Bestimmung zu für die Verarbeitung Verantwortliche geeignet, durch eine Reflexwirkung einen Anreiz für das soziale Netzwerk selbst zu schaffen, diese Vorschriften einzuhalten.“

[214] Vgl. hierzu erneut die Ausführungen *supra* bei B. I. und II.

[215] Siehe *European Data Protection Board*, Guidelines 8/2020 on the targeting of social media users.

sekundäre und *primäre* Verantwortliche im Rahmen der gemeinsamen Verantwortlichkeit versucht, diese Widersprüchlichkeit aufzufangen.

Auf der Ebene der konkreten Pflichten, die mit der sekundären Verantwortlichkeit einhergehen sollten, trägt der Ansatz zudem der Tatsache Rechnung, dass im Mittelpunkt des die Verantwortlichkeit begründenden Verursachungsbeitrags die Auswahl und der Einbezug des primären Verantwortlichen steht. Dieser Erkenntnis folgend fokussiert der Ansatz bei der Frage der Anwendung bestehender DSGVO-Pflichten ebenso wie bei der Auslotung der Konzeption einer neuen Sorgfaltspflicht die Einflussmöglichkeiten, die im Rahmen dieses Beitrags bestehen.

Das Ergebnis ist ein Pflichtenkatalog, der sekundäre Verantwortliche in erster Linie zu sorgfältigen Bemühungen bei der Auswahl ihrer Kooperationspartner ebenso wie bei der Ausgestaltung und Verhandlung der Kooperationsgrundlagen anhält. Anstelle einer pauschalen Anwendung der gemeinsamen Verantwortlichkeit mitsamt ihrer nur bedingt flexiblen Skalierung wird so ein weniger weit reichender, dafür aber flexiblerer Rahmen gewählt, der die begrenzten Möglichkeiten der betroffenen Akteure nicht einfach ignoriert. Ordnet man die nun gefundenen Akteursgruppen des sekundären und primären Verantwortlichen in den in Kapitel 2 gefundenen größeren Rahmen ein, bedarf es sodann noch einer Betrachtung der Gruppe der Plattformbetreiber und ihrer möglichen Verantwortlichkeit. Dieser Betrachtung und der Frage, ob und wie eine Inpflichtnahme von Plattformbetreibern die verbleibenden Defizite kompensieren kann, widmet sich der folgende Abschnitt.

D. Ansatz 2: Die Schaffung einer neuen Verantwortlichkeitsfigur für Plattformen

Im vorangegangenen Abschnitt wurde aufgezeigt, dass die gemeinsame Verantwortlichkeit in Form ihres jüngsten, durch mehrere EuGH-Urteile geschärften, Begriffsverständnisses einen grundsätzlich tauglichen Ansatz dafür darstellt, durch ein Mehr an mehrere Akteure miteinander verknüpfender Verantwortlichkeit den Gefahren entgegenzuwirken, die der Wirksamkeit des datenschutzrechtlichen Verantwortlichkeitskonzepts insgesamt drohen. Um die derzeit jedoch noch verbleibenden Ungewissheiten, die mit einer sehr breiten Anwendung der gemeinsamen Verantwortlichkeit einhergehen, auszugleichen und das von EuGH und anderen Akteuren propagierte Verständnis eines „unterschiedlichen Grad(es) an Verantwortlichkeit“ zwischen den Akteuren auch anhand des konkreten Pflichtenkatalogs operationalisierbar und so zu mehr als einer bloßen Behauptung zu machen, wurde ein Vorschlag für eine Weiterentwicklung ge-

macht, der sich auf die tatsächlichen Einflussmöglichkeiten von Diensteanbietern gegenüber Drittparteien konzentriert.

Auch eine derartig fortentwickelte gemeinsame Verantwortlichkeit ist jedoch nicht in der Lage, all die oben bei A. identifizierten Defizite des Verantwortlichkeitskonzepts im Lichte der modernen Verarbeitungsrealität zu kompensieren. Ein Blick zurück auf die in Kapitel 1 aufgezeigten zentralen Akteursgruppen und ihre Einflusssphären und Kontrollmöglichkeiten lässt einen Grund dafür erahnen: Neben Diensteanbietern und Drittparteien stellen oftmals Plattformbetreiber eine dritte Gruppe, die innerhalb der Gemengelage an Akteuren eine herausgehobene Stellung innehat und mit ihren Entscheidungen und ihrem Verhalten die anderen beiden Gruppen sowohl befähigen als auch limitieren kann. Hinzu kommt, dass auch bei einer nach den oben geschilderten Maßstäben fortentwickelten und stärker gesetzlich ausgeformten gemeinsamen Verantwortlichkeit ein grundlegendes Problem bestehen bleibt: Sie ist mit der Breite der in sie gesetzten Erwartungen und damit auch mit der Breite der von ihr potenziell abgedeckten Fälle und Konstellationen überfordert. Dem sehr weiten Anwendungsbereich wurde durch den Vorschlag eines abgemilderten Pflichtenkatalogs bereits in Teilen entgegengewirkt. Idealerweise könnte eine Verantwortlichkeit für Plattformbetreiber, die nach bisherigem Verständnis grundsätzlich ebenfalls als gemeinsame Verantwortliche in Betracht kämen, zusätzlich dazu beitragen, das überfrachtete Institut der gemeinsamen Verantwortlichkeit punktuell zu entlasten.

Dass die Inpflichtnahme von Plattformbetreibern legitim – das heißt: sowohl zielführend als auch auf einen hinreichenden Ursächlichkeitszusammenhang zwischen infragestehendem Plattformbetreiberverhalten und der dadurch entstehenden abstrakten Gefährlichkeit nachfolgender Verarbeitungen durch die anderen beiden Akteure aufbauend – ist, wurde oben bei II. bereits erörtert. Hier soll es nun darum gehen, wie eine solche Verantwortlichkeit für das Verarbeitungsumfeld, das eine digitale Plattform darstellt, im Detail aussehen könnte. Dafür soll zunächst vorgelagert begründet werden, weshalb Plattformbetreiber eine eigene Verantwortlichkeitsfigur benötigen und nicht ebenfalls als gemeinsame Verantwortliche eingestuft werden sollten (I.). Sodann soll sich hinsichtlich der Konzeption einer solchen neuen Figur insbesondere über zwei Aspekte Gedanken gemacht werden: die Formulierung der Zurechnungskriterien bzw. Tatbestandsvoraussetzungen für die Einordnung als „Verantwortlicher“ (II.) sowie die Schaffung von sinnvollen (im Sinne von: die Fähigkeiten der Akteure ideal ausnutzenden) und erfüllbaren Pflichten (III.). Abschließend soll ein ehrlicher Blick auf die Limitierungen und möglichen Probleme einer solchen Verantwortlichkeit geworfen (IV.) und ein Zwischenfazit gezogen werden (V.).

I. Notwendigkeit einer neuen Figur

Um zu eruieren, weshalb eine neue Verantwortlichkeitsfigur vonnöten ist, bedarf es zunächst einer Abgrenzung zur gemeinsamen Verantwortlichkeit. Auf den ersten Blick könnte es einleuchten, auch Plattformbetreiber schlicht unter den bestehenden, bereits weitestgehend geöffneten Anwendungsbereich der gemeinsamen Verantwortlichkeit zu subsumieren. Plattformbetreiber bringen durch den Betrieb ihrer Plattformen Diensteanbieter und Drittparteien als Datenverarbeiter und Nutzer als Betroffene zusammen und ermöglichen insofern die Verarbeitungen. Indem sie zudem die den Verarbeitungen zugrundeliegende Infrastruktur schaffen und Vorgaben dafür machen, wie Dienste auf der Plattform ausgestaltet zu sein haben, nehmen sie zudem unmittelbar Einfluss auf das „Wie" der folgenden Verarbeitungen, also auf die Mittel, die Diensteanbietern und Drittparteien für Datenverarbeitungen zur Verfügung stehen. Da die Verarbeitung von Nutzerdaten heutzutage essenzieller Teil des Angebots digitaler Dienste ist – sei es aufgrund einer datenzentrierten Funktionsweise, sei es getrieben durch den Wunsch nach Funktionsanalyse, Fehlerfindung und -behebung oder schlicht nach Monetarisierung –, ist Plattformbetreibern die Tatsache dieser Ermöglichung auch ohne weiteres bewusst. Gleiches gilt, wenn auch nicht im Detail und bzgl. jedes Einzelnen, für von Diensteanbietern einbezogene Drittparteien. Sie profitieren in mehrfacher Hinsicht von der Nutzung dieser Dienste und letzten Endes auch von den Datenverarbeitungen, die von Diensten und Drittparteien vorgenommen werden: Die Attraktivität einer Plattform hängt in besonderem Maße von der Vielfalt und Attraktivität der dort auffindbaren Dienste ab, sodass erfolgreiche Dienste einen zentralen Faktor für erfolgreiche Plattformen darstellen.[216] Auf vielen Plattformen, die einen eigenen Distributionskanal anbieten, partizipieren Plattformbetreiber zudem unmittelbar an den Einnahmen, die kostenpflichtige Dienste einspielen. Ob dieser Zusammenhang zwischen erfolgreichen Diensten, die auf möglichst weitreichende Möglichkeiten zur eigenen oder für Dritte ermöglichten Datenverarbeitung angewiesen sind, und erfolgreichen Plattformen ausreicht für das, was seit Fashion ID als Erfordernis kongruenter Zwecke verlangt wird,[217] erscheint zweifelhaft, mit Blick auf die derzeitige Uneindeutigkeit der Voraussetzungen aber auch nicht ausgeschlossen. Es sprechen jedoch unabhängig von der Frage der theoretischen *Möglichkeit* der Anwendbarkeit gewichtige Gründe gegen den *Sinn* einer solchen.

---

[216] So wird etwa die Erfolglosigkeit des inzwischen eingestellten mobilen Windows-Betriebssystems für Smartphones gemeinhin mit der bis zum Schluss geringen Anzahl an Apps im Vergleich zu Konkurrenten wie *iOS* und *Android* in Zusammenhang gebracht. Vgl. etwa *Vlad Savov*, Windows Phone was a glorious failure, The Verge vom 10.10.2017 (https://www.theverge.com/2017/10/10/16452162/windows-phone-history-glorious-failure). Zuletzt abgerufen am 14.01.2022.

[217] Siehe EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629 Rn. 80.

Wie bereits oben unter B. II. in diesem Kapitel dargelegt wurde, ist der Anknüpfungspunkt für die Inpflichtnahme von Plattformbetreibern insgesamt nicht die Verantwortlichkeit für die einzelne Datenverarbeitung eines Diensteanbieters oder gar einer Drittpartei. Im Mittelpunkt steht stattdessen die unmittelbare Verantwortung für die Gefährdung, die mit der Schaffung eines großflächigen und bedeutsamen Verarbeitungsumfelds einhergeht. Die klassisch datenschutzrechtliche Verantwortlichkeit, die sich auch in der gemeinsamen Verantwortlichkeit wiederfindet, ist aber gerade die des „*für die Verarbeitung* Verantwortlichen“[218]. Die einzelne Verarbeitung bzw. die Verarbeitungsreihe ist und bleibt ihr Fixpunkt, auf sie bezieht sich ein Großteil der Pflichten. Wenngleich auch die oben vorgeschlagene Weiterentwicklung des sekundären gemeinsamen Verantwortlichen mit ihrer neu geschaffenen Auswahl- und Überwachungspflicht in Teilen eine Emanzipation von diesem Grundsatz darstellt, besteht dort jedenfalls noch eine hinreichende Nähe zu konkreten einzelnen Datenverarbeitungen, wie auch die Nähe zu den Pflichten gegenüber Auftragsverarbeitern zeigt. Im Falle von Plattformbetreibern fehlt es an dieser Nähe. Durch den vorgelagerten Zeitpunkt der Formulierung von Nutzungsbedingungen, der Aufnahme eines Dienstes auf die Plattform oder der Ausgestaltung der zugrundeliegenden Infrastruktur findet eine detaillierte Vorprägung der später stattfindenden konkreten Datenverarbeitungen nur in sehr begrenztem Maße statt. Ein Anknüpfen an eben diese einzelnen Datenverarbeitungen, wie es das Modell der datenschutzrechtlichen Verantwortlichkeit klassischerweise vorsieht, wäre deshalb nicht zielführend. Diese Überlegung sollte nicht in einem die immense Bedeutung – die das Handeln von Plattformbetreibern, insbesondere in Form ihrer *boundary resources*, für die Möglichkeitsräume von Diensteanbietern und Drittparteien unbestritten hat – schmälernden Sinne verstanden werden. Sie zeigt aber, dass eine dergestalt auf das Verarbeitungsumfeld und die Verarbeitungsumstände bezogene Plattformverantwortlichkeit effektiver ist, wenn sie auch mit eigenen, originär vor diesem Hintergrund entwickelten Pflichten einhergeht. Entsprechend der Natur und Wirkweise von *boundary resources* als plattformweit die Grundbedingungen aller verarbeitungsrelevanten Handlungen auf der Plattform limitierende Ausgestaltungsentscheidungen, bedarf es auch solcher Pflichten, die an diese Wirkrichtung anknüpfen.

Mit anderen Worten: Der Adressatenwechsel weg vom unmittelbar datenverarbeitenden Akteur hin zum die zentralen Umstände bestimmenden Akteur muss auch mit einem entsprechenden Instrumentenwechsel korrespondieren. Ein weiterer Vorteil einer neuen Verantwortlichkeitsfigur kann zudem darin gesehen werden, dass so der notorisch weite bis ausufernde Anwendungsbereich der gemeinsamen Verantwortlichkeit insofern entschlackt und entlastet wird, als eine große Gruppe einheitlicher Sachverhalte nun separat reguliert wird.

[218] So die Überschrift von Art. 24 DSGVO (Hervorhebung durch den Autor).

Dies bedeutet auch eine jedenfalls teilweise Homogenisierung des Anwendungsbereichs, der ggf. zu einer leichteren Konkretisierung und Anwendung beitragen kann. Der Möglichkeit, ggf. einzelne bestehende Verantwortlichenpflichten auch in den Pflichtenkatalog der Plattformverantwortlichkeit zu inkorporieren, soll das eben Gesagte gleichwohl nicht entgegenstehen. Auf diese Möglichkeit soll später bei der Frage der Ausgestaltung der einzelnen Pflichten noch zurückzukommen sein.[219]

II. Die Voraussetzungen für die Pflichtigkeit

Ist nun also geklärt, dass eine eigene Verantwortlichkeit für Plattformbetreiber viele Vorteile gegenüber einer pauschalen Subsumierung als gemeinsame Verantwortliche mit sich bringt, stellt sich die nachfolgende Frage, wie eine solche Verantwortlichkeit konkret aussehen könnte. Der erste Schritt hierfür ist die Bestimmung des Adressatenkreises, also die Ausgestaltung der Voraussetzungen für die Einordnung als Verantwortlicher.

Da die Verantwortlichkeit letztlich im Sinne einer funktionellen Betrachtungsweise den tatsächlichen Einfluss- und Kontrollmöglichkeiten folgen soll, kann hier in erster Linie die bei der Betrachtung in Kapitel 1 verwendete und dem Verständnis dieser Arbeit zugrundeliegende Definition einer digitalen Plattform herangezogen werden: Eine Verantwortlichkeit besteht demnach für Akteure, die digitale Räume und die zugrundeliegende technische Infrastruktur sowie die Ressourcen bereitstellen und kontrollieren, auf der und auf deren Basis sie selbst, aber auch und vor allem dritte unabhängige Akteure Dienste entwickeln und anbieten. Konstitutives Element ist daher in jedem Fall eine „*extensible codebase*“[220]*,* das heißt: das Anbieten von Werkzeugen und die Integration in die eigene Infrastruktur, durch die der von Dritten entwickelte Dienst sich im weitesten Sinne als Erweiterung der Plattform selbst darstellt. Mit diesem Element hängt die Fähigkeit zusammen, *boundary resources*[221] zu entwickeln und einzusetzen, also Handlungsspielräume bei Entwicklung und Nutzung der Dienste auf der Plattform festzulegen.

Eine solche Verantwortlichkeit besteht daher immer nur in Relation zu solchen Akteuren, deren Dienste in einem entsprechenden Verhältnis zur Plattform stehen. Ein Plattformbetreiber kann diese Rolle deshalb gegenüber manchen Akteuren einnehmen, während andere Akteure die Plattform nutzen, ohne Gebrauch von der betreffenden Funktionalität zu machen. Ein Beispiel hier-

---

[219] Siehe *infra* bei III. 2.

[220] Vgl. die Definition bei *de Reuver* u. a., Journal of Information Technology 2018, 124 (127): „Platforms that merely mediate between different user groups but offer no extensible codebase should not be considered digital platforms […].“

[221] Vgl. *Ghazawneh/Henfridsson*, Information Systems Journal 2013, 173 (173 ff.) sowie die ausführliche Behandlung *supra* bei Kapitel 1 B. II.

für wäre die die Art und Weise, wie Facebook gegenüber den Entwicklern von Apps wie Your Digital Life eine Rolle als digitale Plattform im hier verstandenen Sinne einnimmt und somit hinsichtlich der von solchen Apps vorgenommenen Verarbeitungen unter die Plattformverantwortlichkeit fällt. Nicht ausreichend ist hingegen die reine Nutzung der Intermediärsfunktion einer Plattform, sodass Facebook in Relation zu privaten Nutzern oder Fanpage-Betreibern, die im Rahmen ihrer Seite personenbezogene Daten in Form von Beiträgen oder Fotos verarbeiten, nicht als Plattformverantwortlicher in Betracht kommt.[222]

Ähnlich wie bei der gemeinsamen Verantwortlichkeit stellt sich allerdings die grundsätzliche Frage hinsichtlich eines Bedürfnisses nach einer irgendwie gearteten Bagatellschwelle. Die hier herangezogene Definition einer digitalen Plattform ist zunächst griffig und einfach zu handhaben, doch lässt sich nicht leugnen, dass auch sie bei genauer Betrachtung eine Vielzahl unterschiedlicher und hinsichtlich ihrer Ausgestaltung, Größe und Einflussmöglichkeiten sehr heterogener Plattformen umfasst. Nicht jede Plattform ist im gleichen Ausmaß groß, marktmächtig und einflussreich. Es gilt daher zu klären, ob neben den unmittelbar mit dem Gedanken einer außerordentlich einflussreichen Plattform verknüpften Beispiele um Apple, Facebook, Amazon, oder Google bspw. auch weniger offensichtliche Fälle, etwa Internetbrowser wie Firefox, Mailprogramme wie Thunderbird oder Mediaplayer wie Kodi hinsichtlich der für sie entwickelten Erweiterungen,[223] oder klassische Betriebssysteme wie Windows oder Linux hinsichtlich der für sie entwickelten Programme in den Anwendungsbereich der Plattformverantwortlichkeit fallen sollten. Letztlich steht hinter dieser Frage die Überlegung, welche Elemente einer Plattform entscheidend für ihre Einflussfähigkeit auf das Datenverarbeitungsverhalten von Diensteanbietern und Drittparteien und für die Annahme der abstrakten Gefährlichkeit ihres Betriebs, insgesamt also für das Bedürfnis ihrer Inpflichtnahme, sind. Hier lassen sich verschiedene denkbare Ansätze beschreiten, die jeweils typisiert einen für die Gefahrgeneigtheit und bzw. oder Kontrollfähigkeit der Plattform möglicherweise besonders bedeutsamen Aspekt in den Mittelpunkt stellen, dessen geringere Ausgeprägtheit als Anknüpfungspunkt für den Ausschluss bestimmter Akteure im Sinne einer Bagatellgrenze dienen könnte. Eine solche Eingrenzung des Kreises der Verantwortlichen geschähe dann wieder vor dem Hintergrund einer streng verhältnismäßigen Belastung der mit einer Plattformverantwortlichkeit belegten Akteure.

---

[222] Hier wären allerdings, je nach Natur der von Nutzern oder Fanpage-Betreibern erstellten Inhalte, ggf. andere Rechtsinstitute wie das NetzDG oder das Urheberrecht einschlägig.

[223] Letztgenannter Mediaplayer war bereits Teil eines EuGH-Urteils, in dem der Verkauf von sog. Streaming-Boxen, die Kodi mitsamt urheberrechtsverletzenden Add-Ons bereits vorinstalliert hatten, verboten wurden. Siehe EuGH, Rs. C-527/15, ECLI:EU:C:2017:300.

1. Zur möglichen Notwendigkeit einer Mindestgröße

Eine denkbare Herangehensweise wäre es, auf die Größe der Plattform im Sinne der Anzahl ihrer Nutzer abzustellen. Hinter einer solchen Einschränkung stünde der Gedanke, dass mit zunehmender Anzahl von Nutzern eine größere Anzahl Betroffener, aber auch Diensteanbieter und Drittparteien korrespondiert und somit rein quantitativ mehr Daten verarbeitet werden, ergo schon grundsätzlich ein höheres Risiko im Sinne des Gedankens der reinen Datenverarbeitung als risikosensible Handlung besteht. Gleichzeitig erhöht sich durch das Plus auf Ebene der ermöglichten Datenverarbeitungen auch das Risiko datenschutzwidriger Verarbeitungen durch Diensteanbieter und Drittparteien. Neben dieser rein quantitativen Betrachtung lässt sich außerdem anführen, dass die Größe einer Plattform aufgrund parallel steigender Netzwerkeffekte Auswirkungen darauf hat bzw. Rückschlüsse darauf geben kann, inwieweit Nutzer noch die Möglichkeit haben, der Plattform den Rücken zu kehren oder nicht (sog. Lock in-Effekt).[224] Umgekehrt spricht das geringere Ausmaß an Netzwerkeffekten bei geringerer Plattformgröße dafür, dass kleine Plattformen ihre Entscheidungs- und Kontrollfähigkeit nicht im gleichen Maße ausüben können wie große Plattformen, ohne dass Diensteanbieter sich bei ihnen unlieben Entscheidungen schlicht von der Plattform verabschieden. Auch kleine Plattformen entwickeln *boundary resources* und setzen sie ein, stellen also die Infrastruktur und Werkzeuge für Diensteanbieter bereit und bestimmen die Bedingungen für den Zutritt zu und das Handeln auf der Plattform, sodass sie auf dem Papier dieselben Kontrollfähigkeiten wie große Plattformen haben; sie sind aber in größerem Maße als letztere darauf angewiesen, mit ihren Entscheidungen alle anderen Marktseiten (sprich: Diensteanbieter und Nutzer) zufriedenzustellen, um die betreffenden Akteure nicht abzuschrecken. Die zunehmende Größe einer Plattform bedeutet daher auch eine größere Alternativlosigkeit hinsichtlich ihrer Nutzung, sodass die Erfüllung von Pflichten, deren Wirkung sich restriktiv auf das Verhalten von Diensteanbietern auswirkt, kleine Plattformen stärker belastet. Gleiches gilt für den generellen Ressourcen- und Kostenaufwand, der mit der Erfüllung insbesondere präventiver und technisch-organisatorischer Pflichten einhergeht.

---

[224] Solche Effekte liegen vor, wenn die einmal getroffene Entscheidung von Nutzern für eine Plattform sich dergestalt verfestigt, dass hohe Wechselkosten und andere Gründe den Wechsel zu einer anderen Plattform erheblich erschweren oder nahezu unmöglich machen, vgl. *Conrad/Licht*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 39 Rn. 475. Innerhalb der DSGVO stellt das Recht auf Datenportabilität ein eher dem Wettbewerbsrecht zugehöriges Instrument dar, das dem Entstehen solcher Effekte entgegenwirken soll. Siehe dazu *Jülicher* u. a., ZD 2016, 358 (360 ff.); dabei stehen insbesondere soziale Netzwerke im Fokus, sodass *Conrad*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, § 34 Rn. 635 gar von einer „*Lex* Facebook" spricht.

Stellt man sich daher auf den Standpunkt, gerade die Größe einer Plattform stelle ein taugliches Kriterium zur Einschränkung des Adressatenkreises dar, indem es einerseits die Gefahrgeneigtheit der Plattform, andererseits die Kontrollfähigkeit ihres Betreibers berücksichtige, wäre die Festlegung einer festen Mindestgrenze an Nutzern ein denkbares Kriterium zur Einschränkung des Kreises der Verantwortlichen. Bekannt ist ein solcher Anknüpfungspunkt für eine Bagatellgrenze dem deutschen Recht etwa aus dem NetzDG, das in seinem § 1 Abs. 2 solche sozialen Netzwerk vom Anwendungsbereich des Gesetzes ausnimmt, die im Inland weniger als zwei Millionen registrierte Nutzer haben. Auch hier ist der Grund dafür der, dass die aufwendigen Prüfpflichten des NetzDG „nur von sozialen Netzwerken mit entsprechenden Ressourcen und Kapazitäten bewältigt werden" können.[225] Unumstritten ist diese Bagatellgrenze wohlgemerkt nicht – weder hinsichtlich ihres Anknüpfens an die Anzahl registrierter Nutzer für die Beurteilung des potenziellen Schadens,[226] noch hinsichtlich der Grundprämisse, ein größeres Netzwerk sei zwingend mit mehr wirtschaftlichen Ressourcen ausgestattet[227].

Nicht alle der in der dortigen Diskussion vorgebrachten Einwände lassen sich jedoch unmittelbar auf die hier diskutierte Plattformverantwortlichkeit übertragen. Während etwa die Schlussfolgerung, mehr Nutzer eines sozialen Netzwerks würden zwangsläufig eine größere Perpetuierungswirkung der einzelnen geteilten rechtswidrigen Inhalte mit sich bringen, mit Blick auf die regelmäßige bloße Verbreitung in abgegrenzten Rezipientenkreisen und nicht dem gesamten Netzwerk schnell als unterkomplex entlarvt ist, lässt sich im hiesigen Szenario nicht leugnen, dass mehr Nutzer und Diensteanbieter zwingend auch mehr Datenverarbeitungen bedeuten. Das Anknüpfen an die Anzahl Betroffener bzw. das quantitative Ausmaß an Verarbeitungen ist dem Datenschutzrecht zudem alles andere als fremd. So ordnet etwa § 38 Abs. S. 1 BDSG in Ergänzung zu Art. 37 DSGVO die Pflicht zur Bestellung eines Datenschutzbeauftragten auch dann an, wenn beim Verantwortlichen „in der Regel mindestens 20 Personen ständig" mit der Verarbeitung personenbezogener Daten beschäftigt sind und dementsprechend mit vielen Verarbeitungen zu rechnen ist. Erwg. 75 der Verordnung führt es als einen Beispielsfall für ein Risiko für die Rechte und Freiheiten natürlicher Personen an, wenn „die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Per-

[225] BT-Drucks. 18/12356, S. 19.

[226] *Liesching*, in: Spindler u. a., TMG/NetzDG, § 1 NetzDG Rn. 67 führt zutreffend aus, dass „die Zahl der registrierten Nutzer weder Indikator noch Indiz für die Wahrnehmungsreichweite" ist.

[227] Vgl. *Liesching*, in: Spindler u. a., TMG/NetzDG, § 1 NetzDG Rn. 66, der hierin eine „gesetzgeberische Fehlannahme" sieht, da ein Plus an registrierten Nutzern mangels Entgeltpflicht sich finanziell nicht auswirke. Dieser Gedanke führt allerdings insofern zu kurz, als für das auf Werbe(vermittlungs)einnahmen basierende Geschäftsmodell sozialer Netzwerke letztlich doch jeder zusätzliche Nutzer auch zusätzliche Einnahmen bedeutet.

sonen betrifft." Auch der hinsichtlich seiner Ambitionen oft mit der DSGVO verglichene – allerdings inhaltlich sehr stark von dieser abweichende – California Consumer Privacy Act (CCPA) knüpft als eins von mehreren möglichen Tatbeständen zur Qualifikation der pflichtigen Akteure in seinem § 1798.40 (c) daran an, ob diese personenbezogene Daten von mindestens 50.000 (in Kalifornien wohnhaften) Personen verarbeiten.[228] Einen etwas anderen Anknüpfungspunkt wählt das – der DSGVO jedenfalls mit Blick auf das Marktortprinzip und die Berechnung von Bußgeldern als teilweises Vorbild dienende[229] – europäische Kartellrecht, wenn es als ungeschriebene Bagatellklausel des in Art. 101 AEUV verankerten Verbots wettbewerbsbeschränkender und handelsbeeinträchtigender Koordinierungsmaßnahmen von Unternehmen die Spürbarkeit der Konsequenzen der infragestehenden Maßnahmen verlangt und Maßnahmen mit nicht spürbaren, bloß geringfügigen Auswirkungen von dem Verbot ausnimmt.[230] Kriterium zur Ermittlung der Spürbarkeit ist dabei nicht die einzelne Maßnahme, sondern die Marktstellung der beteiligten Unternehmen, für deren Beurteilung in erster Linie auf die jeweiligen Marktanteile zurückgegriffen wird, wobei ein (mindestens gemeinsamer) Marktanteil von 5 % die Spürbarkeit regelmäßig indizieren soll.[231]

Aus systematischer Hinsicht lässt sich gegen das Anknüpfen an die Größe der Plattform daher zunächst nichts einwenden. Der verfolgte Zweck, weniger gefahrgeneigte Plattformen und zur Pflichtenerfüllung befähigte Plattformen auszuschließen, lässt sich so zumindest in einigen Aspekten grundsätzlich erreichen. Möglich wäre neben der Nutzerzahl als zentralem Kriterium auch ein Anknüpfen an die Marktstellung der jeweiligen Plattform in Anlehnung an Art. 101 AEUV. Beide Vorgehensweisen bringen ihre jeweils eigenen Probleme mit sich. Während bzgl. der Nutzerzahl die aus der Debatte um das NetzDG stammende Kritik an der geringen Aussagekraft von Nutzerzahlen, die keinen Aufschluss über die Aktivität oder Passivität der einzelnen Nutzer geben, sowie an der Frage der Notwendigkeit einer Beschränkung auf registrierte Nutzer, auch hier ihre Berechtigung hat, krankt die Bestimmung von Marktstellung im digitalen Bereich bekanntermaßen an der Schwierigkeit, tragfähige Marktabgrenzungen überhaupt vorzunehmen und marktbeherrschende Stellungen zu bestimmen.[232] Zudem muss konstatiert werden, dass nach der hier verfolgten

---

[228] Siehe hierzu ausführlich *Botta*, PinG 2019, 261 (263 f.).

[229] Vgl. *Schröder*, in: Krönke, Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, S. 13 (18, 24).

[230] Siehe *Stockenhuber*, in: Grabitz u. a., Das Recht der Europäischen Union, Art. 101 AEUV Rn. 217 ff. m. w. N.

[231] Siehe ausführlich hierzu und zur unterschiedlichen Prüfungspraxis von Kommission und EuGH *Stockenhuber*, in: Grabitz u. a., Das Recht der Europäischen Union, Art. 101 AEUV Rn. 219–223.

[232] Vgl. *Paal/Hennemann*, NJW 2017, 1697 (1698 ff.); siehe außerdem *Bundeskartellamt*, Arbeitspapier – Marktmacht von Plattformen und Netzwerken, S. 7 ff.

Definition und den oben gemachten Erkenntnissen[233] eine jede Plattform, völlig unabhängig von ihrer Größe, *boundary resources* entwickelt und einsetzt und damit plattformweit (nicht nur, aber insbesondere) datenverarbeitungsrelevante Handlungsräume ermöglicht und begrenzt. Die damit einhergehende Gefahrgeneigtheit (im Sinne der Ermöglichung von Datenverarbeitungen) und Kontrollfähigkeit (im Sinne der Gestaltung und Durchsetzung von Limitierungen) mag zwar mit zunehmender Größe weiter zunehmen, ist aber in allen Fällen bereits dem Grunde nach enthalten.

2. Zur möglichen Notwendigkeit eines Mindestumsatzes

Ebenfalls denkbar wäre die Formulierung eines Mindestumsatzes, der von einer Plattform jährlich erreicht werden muss, um die Schwelle zur Verantwortlichkeit zu überschreiten. Der bereits erwähnte kalifornische CCPA kann hier ebenfalls als Vorbild dienen, dient ein jährlicher Bruttoumsatz von 25 Millionen US-Dollar doch auch hier in § 1798.40 (c) als möglicher Tatbestand für eine Verantwortlichkeit von Unternehmen.[234]

Auch dieses Kriterium baut auf dem Gedanken auf, finanzschwache Plattformen von den Pflichten der Plattformverantwortlichkeit zu dispensieren, da die mit der Erfüllung der Pflichten verbundenen Aufwände und Ressourcen sie über Gebühr belasten könnten. Letztlich ersetzt das Kriterium des Umsatzes also schlicht das der Größe. Hinsichtlich der Aussagekraft über die finanziellen und sonstigen Ressourcen und Kapazitäten ist dieser Austausch unbestritten von Vorteil. Gleichzeit kann jedoch, anders als bei der Größe, die ein unmittelbares Maß für die Anzahl auf der Plattform erfolgender Datenverarbeitungen ist, nicht ohne weiteres davon ausgegangen werden, dass eine umsatzstärkere Plattform zwingend eine größere Gefahrgeneigtheit mit sich bringt als eine umsatzschwächere Plattform. Es besteht daher die Gefahr, durch die typisierte Betrachtung der Finanzstärke auch solche Plattformen aus der Verantwortung zu entlassen, die trotz geringen Umsatzes eine Vielzahl von Nutzern haben und so einen digitalen Raum bieten, an dem sich überdurchschnittlich viele Verarbeitungen abspielen. Ein Heranziehen dieses Kriteriums ist daher im Ergebnis nicht empfehlenswert.

3. Zur möglichen Notwendigkeit eines Mindestgrads an Geschlossenheit der Plattform

Eine weitere denkbare Einschränkung könnte darin bestehen, ein Mindestmaß an Geschlossenheit der jeweiligen Plattform zu verlangen. Entscheidend wäre dann, dass der infragestehende Plattformbetreiber nach einer funktionalen Be-

[233] Siehe die grundlegenden Ausführungen in Kapitel 1 A. und B. sowie die Analyse in diesem Kapitel bei A.

[234] Vgl. auch hier vertiefend *Botta*, PinG 2019, 261 (263 f.).

trachtung die ihm zur Verfügung stehende Macht auch in hinreichendem Maße nutzt, auf seiner Plattform also bereits bestimmte Restriktionen gegenüber den Möglichkeitsräumen von Diensteanbietern und Drittparteien setzt. Der Gedanke hinter einem solchen Erfordernis wäre es, dass Betreiber von Plattformen, die ihrer Grundkonzeption nach eher offen gestaltet sind, von einer auf restriktive Gestaltung gerichteten Inpflichtnahme unverhältnismäßig stärker belastet wären als Betreiber von Plattformen, die von vornherein geschlossener konzipiert sind. Dieser Gedanke liegt im ersten Moment nahe: Ein Plattformbetreiber, der die Dienste auf seiner Plattform kaum oder gar nicht selektiert und ihnen keine Vorgaben zur Ausgestaltung ihrer Dienste macht, hätte stärker damit zu kämpfen, bspw. jeden neuen Dienst vor der Aufnahme auf seine datenschutzrelevanten Vorhaben und Absichten sowie Garantien für Datenschutzmaßnahmen hin zu untersuchen als ein Betreiber, der solche Screenings sowieso schon durchführt. Über diesen, den Ressourcenaufwand betreffenden – und damit Vergleiche zu der unter 1. diskutierten Bagatellschwelle im NetzDG aufweisenden –, Aspekt hinaus trifft eine Inpflichtnahme die Betreiber offener Plattformen auch insofern stärker, als diese je nach Ausgestaltung und Reichweite der Pflichten ggf. gezwungen wären, die grundlegende Ausrichtung ihrer Plattform aufzugeben.

Auf der anderen Seite lassen sich in erster Linie zwei Argumente gegen ein Erfordernis der hinreichenden Geschlossenheit einer Plattform vorbringen. Zum einen erfüllt das Kriterium der Geschlossenheit nur eines der beiden oben bereits etablierten Ideale einer Bagatellgrenze: Sie dispensiert zwar solche Betreiber, die durch eine Inpflichtnahme stärker betroffen und schlechter in der Lage wären, die an sich gerichteten Pflichten zu erfüllen, ohne dass aber die von ihnen betriebenen Plattformen auch gleichzeitig weniger gefahrenträchtig wären. Offene Plattformen sind vielmehr, zumindest potenziell, gerade diejenigen, die bei entsprechender Größe und Popularität ein gleiches Ausmaß an Datenverarbeitungen ermöglichen und den verarbeitenden Akteuren dabei ein zusätzliches Maß an Freiheit bei der datenverarbeitungserheblichen Gestaltung ihrer Dienste lassen.

Zum anderen gilt es zu berücksichtigen, dass die Offenheit einer Plattform im Sinne von (fehlenden) Einschränkungen des Nutzerkreises sowie der Dichte der daraufhin erfolgenden Überprüfungen nur einen Teil der Einfluss- und Kontrollmacht eines Plattformbetreibers ausmacht. Mit der hier zugrunde gelegten Definition einer digitalen Plattform, die grundlegend auf die Bereitstellung einer Infrastruktur und der zur Gestaltung von Drittdiensten notwendigen Werkzeuge abstellt, ist auch die Ausgestaltung der Infrastruktur selbst bereits unmittelbar Ausübung von Entscheidungsmacht und verarbeitungsrelevanter Kontrolle. Jede Gestaltungsentscheidung hier hat bereits Auswirkungen auf die Möglichkeitsräume von Diensteanbietern und damit auf die von ihnen durchgeführten Datenverarbeitungen. Selbst eine, nach obigen Kriterien, als *offen* zu kategori-

sierende Plattform ist daher noch in den relevanten Bereichen als besonders entscheidungsmächtig und kontrollfähig anzusehen, übt sie doch allein durch diese Gestaltungsentscheidungen erheblichen Einfluss aus. Sie dann jedoch aus der Verantwortung zu entlassen, wäre nach allen mit der Einführung einer Bagatellgrenze verbundenen Zwecken und Idealen unsinnig. Den Unterschieden zwischen eher offenen und eher geschlossenen Plattformen sollte stattdessen besser auf Ebene der Pflichtenverteilung sowie des Ausmaßes der einzelnen Pflichten Rechnung getragen werden. Legt man dieser Ebene das Ideal einer ausreichenden Flexibilität zugrunde, könnten in den hier besprochenen Fällen etwa die auf die Ausgestaltung der Infrastruktur gerichteten Pflichten stärker in den Vordergrund rücken, während die auf die Ausgestaltung und Kontrolle der Aufnahme- und Nutzungsbedingungen gerichteten Pflichten nicht oder jedenfalls nicht in vollem Umfang angewendet werden könnten. Eine solche Lösung wäre einer pauschalen Ausnahme jeglicher offenen Plattformen auch insofern überlegen, als die grundlegende Schwierigkeit hinsichtlich der insgesamten Operationalisierung des Kriteriums „Offenheit" und Festlegung eines wie auch immer gearteten Grenzwerts durch die Einzelfallbetrachtung im Rahmen der jeweiligen Pflicht und ihrer Anwendbarkeit bzw. Reichweite aufgelöst wird.

4. Zwischenergebnis

Von den hier diskutierten Ansätzen zur Bestimmung einer Bagatellgrenze für die Verantwortlichkeit von digitalen Plattformbetreibern im Rahmen der auf ihren Plattformen stattfindenden Datenverarbeitungen vermag einzig die Einführung einer Mindestgröße im Grundsatz zu überzeugen. Wenngleich dieser Ansatz seine eigenen Schwierigkeiten, insbesondere bei der Bestimmung eines konkreten Grenzwerts, mit sich bringt, ist der Zusammenhang zwischen der Größe einer Plattform und der Anzahl der dort stattfindenden Datenverarbeitungen unstrittig eng genug, um hier eine Differenzierung jedenfalls für möglich zu halten.

Gleichzeitig verbleibt die Tatsache, dass auch kleine – ebenso wie offene und umsatzschwache – Plattformen nach der hier verwendeten Definition eine erweiterbare Codebasis für Diensteanbieter bereitstellen und mittels Entwicklung und Einsatz von *boundary resources* die grundlegenden Handlungsräume definieren, innerhalb derer diese Diensteanbieter Daten verarbeiten können. Da Akteure, auf die dies nicht zutrifft, somit bereits über die hier verwendete Plattformdefinition ausgeschlossen werden, würde eine wie auch immer gearteten Bagatellgrenze zwingend diesen Kreis an Akteuren weiter ausdünnen. Überzeugender, weil feingliedriger, erscheint es daher, den unterschiedlichen Graden an Gefahrgeneigtheit und Kontrollmöglichkeit *innerhalb* dieses Kreises an Akteuren nicht durch eine harte Bagatellgrenze, sondern durch eine Berücksichtigung auf Ebene der flexiblen Verteilung und Anwendung der einzel-

nen Verantwortlichenpflichten Rechnung zu tragen. So lässt sich, wie noch zu zeigen sein wird, zielgerechter eine verhältnismäßigkeitsgetriebene Schonung einzelner Akteure herbeiführen, ohne diese dabei vollkommen aus der Verantwortung zu entlassen.

Die Qualifikation als digitale Plattform im Sinne der hier verwendeten Definition[235] ist damit im Ergebnis ausreichend, um als Plattformverantwortlicher eingestuft zu werden. Einer darüber hinausgehenden Bagatellgrenze bedarf es nicht. Dem Pflichtenkatalog, dessen Flexibilität und Skalierbarkeit anstelle einer Bagatellgrenze die verhältnismäßige Berücksichtigung unterschiedlicher Arten von Plattformbetreibern sicherstellen soll, widmet sich der nächste Abschnitt.

III. Die konkreten Pflichten der Plattformverantwortlichkeit

Wie könnte also eine Plattformverantwortlichkeit hinsichtlich ihres Pflichtenkonzepts aussehen? Klar erscheint hier zunächst nur, dass es sich organisch in das existierende Verantwortlichkeitskonzept der DSGVO einfügen können müsste. Wie oben bei A. bereits erläutert, wäre mit der Ausweitung der Verantwortlichkeit auf Plattformen zudem die Erwartung einer reflexiven Bezugnahme auf die weiteren datenschutzrechtlichen Verantwortlichen verbunden. Die Pflichten müssten daher idealerweise so ausgestaltet sein, dass sie die bestehenden Defizite des momentanen Verantwortlichkeitskonzepts nicht nur objektiv und isoliert abmildern, sondern auch die weiteren Verantwortlichen besser befähigen, aber auch stärker verpflichten, ihre eigenen Pflichten wirksam zu erfüllen. Im Rahmen der nun folgenden Überlegungen sollen dafür verschiedene Ansätze aufgezeigt werden, die sich an den bestehenden Pflichten der DSGVO, den aufgezeigten konzeptionellen Defiziten sowie den konkreten Einflussmöglichkeiten digitaler Plattformen, aber auch an existierenden Rechtsregimen und Diskussionen um die Verantwortlichkeit von Plattformen im Generellen orientieren. Möglich erscheinen hier folgende Herangehensweisen: einerseits eine reine Intermediärshaftung, wie sie aus dem Urheber- und Markenrecht bekannt ist und vor Einführung des NetzDG auch den Schutz von Persönlichkeitsrechten prägte (1.), andererseits ein vollständiges Verantwortlichkeitskonzept, das neben einer Haftungszuordnung auch konkrete Pflichten formuliert (2.).

1. Reine Intermediärshaftung

Denkbar wäre es etwa, mit Blick auf die Vermittlerfunktion von digitalen Plattformen, die Verantwortlichkeit insgesamt nur rudimentär auszugestalten in Form einer bloßen Intermediärshaftung, die bei Verletzung nicht näher definier-

[235] Siehe *Tiwana* u. a., Information Systems Research 2010, 675 (676) sowie die Ausführungen *supra* in Kapitel 1 A. I.

ter und eher abstrakt gehaltener Pflichten dann zu einer Sanktionierung von Plattformbetreibern führen würde, wenn diese im konkreten Fall durch ihr Handeln oder die Ausgestaltung ihrer Plattform besonders gefahrenträchtige Verarbeitungsumstände geschaffen haben.

Ein solcher Ansatz wäre im Bereich des Datenschutzrechts insofern nicht gänzlich neu, als etwa im Zusammenhang mit der Fashion ID-Entscheidung des EuGH bereits darüber nachgedacht wurde, das deutsche Haftungsregime der Störerhaftung auf Akteure anzuwenden, bei denen eine Qualifizierung als klassisch datenschutzrechtlicher Verantwortlicher nicht in Betracht kommt.[236] Um die Möglichkeit eines solchen Rückgriffs, die vom EuGH zwar nicht explizit und abschließend beantwortet, aber nach überzeugender Lesart wohl jedenfalls implizit für möglich erachtet wurde,[237] soll es hier nicht gehen. Auch ähnelt der Websitebetreiber, der im zugrundeliegenden Fall ein *social plugin* von Facebook eingebunden hatte, nach hiesigem Verständnis eher der Rolle des Diensteanbieters, weshalb die Überlegungen nicht ohne weiteres auf Plattformbetreiber übertragbar sind. Sie zeigen jedoch, dass derartige Überlegungen als Ansätze zur Auflösung der mit der heute vorherrschenden Akteurskomplexität einhergehenden Gefahren der datenschutzrechtlichen Debatte nicht fremd sind. In der deutschen Dogmatik wird unter der Störerhaftung die (zivilrechtliche) Haftung eines Akteurs verstanden, der selbst täterschaftlich keine verletzende Handlung vornimmt, aber durch Verletzung einer ihm eigenen Prüfungsflicht mittelbar zu der verletzenden Handlung eines anderen Akteurs beiträgt und dabei gleichzeitig derjenige ist, der die verletzende Handlung des Dritten sehr einfach abstellen kann.[238] Noch kürzer formuliert: Wer willentlich und adäquat kausal zur Verletzung eines Rechtsguts beiträgt, ohne Täter oder Teilnehmer zu sein, kann als Störer in Anspruch genommen werden.[239] Die Rechtsfolge einer solchen Haftung ist entsprechend begrenzt auf die Beseitigung und Unterlassung der Verletzungshandlung des Dritten bzw. des eigenen Verhaltens oder Zustands, das diese Handlung begünstigt.[240] Voraussetzung für eine sol-

---

[236] Siehe etwa die Ausführungen bei *Piltz*, K&R 2014, 80.

[237] So etwa *Kremer*, CR 2019, 676 (678); skeptischer hingegen *Golland*, K&R 2019, 533 (536).

[238] Vgl. *Wagner*, in: MüKo BGB Band VII, § 823 BGB Rn. 852 ff. grundlegend zudem *Wollin*, Störerhaftung im Immaterialgüter- und Persönlichkeitsrecht; *Picker*, Privatrechtssystem und negatorischer Rechtsschutz, S. 1 ff.

[239] Dieses Institut wurde im Ausgangspunkt vom BGH, insbesondere im Bereich des Immaterialgüterrechts, entwickelt. Siehe BGH, Urt. v. 11.03.2004, Az. I ZR 304/01 (Internet-Versteigerung) Rn. 55 ff.; Urt. v. 12.07.2012, Az. I ZR 18/11 (Alone in the Dark) Rn. 34ff; Urt. v. 05.05.2015, Az. I ZR 240/12 (Kinderhochstühle im Internet III) Rn. 77 ff. Ausführlich zu der Rechtsprechung über die Jahre *Wollin*, Störerhaftung im Immaterialgüter- und Persönlichkeitsrecht, S. 69 ff.

[240] Das ergibt sich bereits daraus, dass die Störerhaftung zivilrechtsdogmatisch an § 1004 BGB anknüpft, dessen Ansprüche auf Beseitigung und Unterlassung störender Handlungen gerichtet sind.

che Haftung ist die Verletzung von Verhaltenspflichten, deren Kontur über die Jahre in der Rechtsprechung nach und nach herausgearbeitet wurde.[241]

Auch auf unionsrechtlicher Ebene hat die Haftung von Intermediären, über das Datenschutzrecht hinaus, einige Tradition. So ordnen Art. 8 Abs. 3 InfoSoc-RL und Art. 11 S. 3 Durchsetzungs-RL im Bereich des Urheberrechts und geistigen Eigentums an, dass Mitgliedstaaten im Interesse einer wirksamen Rechtsdurchsetzung Möglichkeiten zum Erlass gerichtlicher Anordnungen auch gegen Vermittler vorsehen sollen, deren Dienste von Dritten zur Verletzung von entsprechenden Schutzrechten genutzt werden.[242] Im Bereich des Lauterkeitsrechts ist eine Intermediärshaftung bisher zwar nicht explizit verankert, wird aber zumindest (gestützt auf Art. 5 Abs. 1, 2 UGP-RL) vereinzelt bereits gefordert.[243] Auch hier findet sich eine Konturierung und Einschränkung dieser Haftung im Wege des sog. Haftungsprivilegs für Intermediäre, das vermittels Art. 12 bis 15 eCommerce-RL klarstellt, dass keine generelle Haftung für fremde Inhalte besteht, solange der Vermittler keine positive Kenntnis von der Rechtswidrigkeit der Inhalte hat und bei Kenntniserlangung unverzüglich die Löschung veranlasst. Letztlich bedeutet dies eine *notice and takedown*-Pflicht, die gleichzeitig dadurch klar begrenzt wird, dass Art. 15 Abs. 1 eCommerce-RL allgemeine Überwachungspflichten verbietet. Die Herangehensweise der EU (wie auch in Teilen diejenige des deutschen Rechts) kann also als Kompromiss verstanden werden: Plattformen und andere Intermediäre sind einerseits in einer zu herausgehobenen und befähigten Position zur Beseitigung von Rechtsverstößen, um nicht in Anspruch genommen zu werden.[244] Andererseits ist ihre Bedeutung für die ökonomischen und gesellschaftlichen Entwicklungen heutzutage so groß, dass eine überbordende Haftung und das damit drohende Abwürgen der Entwicklung und ihrer Vorteile verhindert werden soll, sodass nur eine privilegierte Haftung in Betracht kommt.[245]

Angewendet auf Betreiber digitaler Plattformen bzgl. Datenverarbeitungen, die durch Dritte – genauer: Diensteanbieter oder einbezogene Drittparteien – vorgenommen werden, käme eine ähnliche Art der Intermediärshaftung grundsätzlich ebenfalls infrage. Auch Plattformbetreiber nach hiesigem Verständnis sind bei erlangter Kenntnis um datenschutzwidrige Praktiken der auf ihren Plattformen tätigen Akteure grundsätzlich in der Lage, das datenschutzwidrige Verhalten bspw. durch Entzug der entsprechenden Zugriffsberechtigungen

---

[241] Siehe auch hier die umfassende Analyse bei *Wollin*, Störerhaftung im Immaterialgüter- und Persönlichkeitsrecht, S. 106 ff.

[242] Einen guten Überblick hierüber verschafft *Ohly*, ZUM 2015, 308 (309 ff.).

[243] Vgl. *Ohly*, GRUR 2017, 441 (443 ff.).

[244] Vgl. Erwg. 59 der InfoSoc-Richtlinie: „Oftmals sind diese Vermittler selbst am besten in der Lage, diesen Verstößen ein Ende zu setzen."

[245] Siehe hierzu etwa *Nolte/Wimmers*, GRUR 2014, 16 (17): „Der Schutz durch diese Privilegierungen ist essenziell für die Erbringung der Vermittlungsleistungen, unabhängig davon, wie groß ein Unternehmen ist."

oder kompletten Ausschluss von der Plattform abzustellen. Dennoch spricht einiges gegen eine solch „abgespeckte" Form der Haftung, der zwar denknotwendig die Verletzung von Pflichten vorausgeht, bei der aber dennoch in erster Linie das *nachträgliche* Abhelfen im Mittelpunkt steht. Wie bereits mehrfach aufgezeigt, ist die Haftung aber im Datenschutzrecht hinsichtlich ihrer Funktion als Regelungsinstrument nur eines von vielen und dient eher als Druckmittel für die Einhaltung der zahlreichen, auf unterschiedlichste Handlungen gerichteten Pflichten, von denen viele gerade *proaktiv* ausgerichtet sind und die Verantwortlichen schon im Vorfeld der Verarbeitung zu datenschutzsensiblen Vorkehrungen veranlassen sollen. Der Fokus beim datenschutzrechtlichen Verantwortlichkeits- und damit auch Regelungskonzept liegt daher weitaus stärker auf der Beeinflussung *positiven* Verhaltens als auf der reinen Pönalisierung *negativen* Verhaltens. Diese Überlegungen werden mit Blick auf Plattformbetreiber noch verstärkt, wenn man sich vergegenwärtigt, dass ihre Macht- und Einflussposition gerade nicht nur aus ihrer Vermittlerrolle besteht, sondern auch und gerade von der technischen Ebene des Bereitstellens einer *extensible codebase* lebt, mittels derer Dritte ihre Dienste gestalten können. Plattformbetreiber bieten daher nicht nur den Raum an, der Anbieter und Nutzer zusammenbringt, sondern gestalten noch weitaus grundlegender die Möglichkeitsräume dafür, was Diensteanbieter anbieten können und auf welche Daten sie dafür unter welchen Bedingungen zugreifen können. Damit sich dies auch in den sie treffenden Pflichten widerspiegelt, braucht es aber zwangsläufig ein komplexeres und feingliedrigeres Verantwortlichkeitskonzept, das von den Pflichten und ihrer Steuerungswirkung her gedacht wird und nicht von der Haftung her, die im Nachgang durch die Einführung von Sorgfalts- und Verhaltenspflichten begrenzt werden soll. Ein solches Mehr an Komplexität in der Verantwortlichkeitsausgestaltung muss zudem nicht zwingend eine größere Belastung darstellen als die, insofern vergleichsweise unterkomplexe, reine Haftung. Auch in Bereichen, die klassischerweise dem herkömmlichen Konzept der Intermediärshaftung unterfielen, ist eine Entwicklung hin zu einer Art komplexeren Intermediärsverantwortung festzustellen,[246] wie unter anderem die DSM-RL im Bereich des Urheberrechts[247] oder das in der Weiterentwicklung befindliche NetzDG im Bereich der

[246] Vgl. *Frosio*, Int J Law Info Tech 2018, 1 (7): „Legal theory is increasingly shifting the discourse from liability to enhanced ‚responsibilities' for intermediaries under the assumption that OSPs' role is unprecedented for their capacity to influence the informational environment and users' interaction within it." Vgl. auch *Helberger* u. a., The Information Society 2018, 1 (3 ff.); *Kuczerawy*, in: KU Leuven Centre for IT & IP Law, Rethinking IT and IP law: celebrating 30 years CiTiP, S. 141 (141 ff.): „Current policy discourse on intermediary liability in the European Union is steadily shifting from liability to responsibility."

[247] Siehe ausführlich zur dortigen Plattformverantwortlichkeit *Hofmann*, ZUM 2019, 617 (620 ff.); *Wagner*, GRUR 2020, 447 (451 ff.); *Hofmann*, GRUR 2019, 1219 (1219 ff.); für einen internationalen Vergleich von Regimen der Intermediärshaftung im Urheberrecht siehe *Jones*, Die urheberrechtliche Haftung von Intermediären im Rechtsvergleich.

Persönlichkeitsrechte[248] zeigen.[249] In anderen Bereichen werden bisher nicht in die Pflicht genommene Intermediäre erstmals in komplexere Verantwortungsregime einbezogen.[250]

Es spricht daher alles für die Konzeption eines vollständigen Verantwortlichkeitskonzepts anstelle einer simplifizierten Intermediärshaftung. Dabei können die Erkenntnisse und Zielrichtungen der bestehenden Regime von Intermediärshaftung im Rahmen der einzelnen Pflichten dennoch berücksichtigt werden und als Inspiration einfließen.

2. Vollständiges Verantwortlichkeitskonzept

Ein Verantwortlichkeitskonzept für Plattformbetreiber müsste daher eine ausgewogene Mischung aus Pflichten beinhalten, die mehrere Zwecke erfüllen: sich an den konkreten Einfluss- und Kontrollmöglichkeiten typischer Plattformbetreiber orientieren, diese also möglichst effektiv nutzbar machen und dabei die typische Entstehungs- und Entwicklungsdynamik von Einflussnahmeentscheidungen berücksichtigen[251]; eine hinreichende Flexibilität in Anwendung und Auswirkung aufweisen, um den unterschiedlichen Ausprägungen an Marktmacht und Offenheit unter den Plattformen Rechnung zu tragen[252]; sich organisch in die Gesamtsystematik der DSGVO einfügen; die weiteren beteiligten Akteure und Verantwortlichen bei der Befähigung zur Erfüllung ihrer Pflichten und Aufgaben unterstützen und so zu einer Verringerung der konzeptionellen Defizite des Verantwortlichkeitskonzepts beitragen[253].

Im Folgenden soll daher ein Ausblick darauf gegeben werden, aus welchen Pflichten sich eine solche Verantwortlichkeit speisen könnte. Dieser folgt einer Einteilung in proaktive Pflichten (a)), reaktive Pflichten (b)) und Rechtsfolgen und Haftungstatbestände (c)).[254] Dabei soll stets auch darauf eingegangen werden, inwieweit die oben genannten Zwecke von den einzelnen Pflichten erfüllt werden.

---

[248] Vgl. hierzu *Kalbhenn/Hemmert-Halswick*, MMR 2020, 518 (518 ff.), die eine Entwicklung „vom Compliance-Ansatz zu Designvorgaben" feststellen. *Lang*, AöR 2018, 220 (222 ff.); weitergehende und gesetzesübergreifende Entwicklungsvorschläge machen *Sahl/Bielzer*, ZRP 2020, 02 (3 ff.).

[249] Ein erster Ansatz dafür, klassische Intermediärshaftung und das datenschutzrechtliche Verantwortlichkeitskonzept für Intermediäre zusammenbringen, findet sich bei *Erdos*, Int J Law Info Tech 2018, 189 (210 ff.).

[250] So etwa – nicht unumstritten – Medienintermediäre im Bereich des neuen Medienstaatsvertrags. Siehe hierzu unter anderem *Liesem*, ZUM 2020, 377 (377 ff.); *Paal/Heidtke*, ZUM 2020, 230 (230 ff.).

[251] Siehe hierzu die in Kapitel 1 B. II. gewonnenen Erkenntnisse.

[252] Siehe das Zwischenergebnis im vorangegangenen Abschnitt (II. 4.).

[253] Siehe die Ausführungen zu Notwendigkeit und Legitimation der Zusatzbelastung weiterer Verantwortlicher unter B. in diesem Kapitel.

[254] In grober Anlehnung an *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 6: „Die Mittel zur Anregung eines verantwortungsvollen Verhaltens können proaktiv oder reaktiv sein."

a) Proaktive Pflichten

Ein zentraler Bestandteil des datenschutzrechtlichen Verantwortlichkeitskonzepts, der auch bei der neuartigen Verantwortlichkeit von Plattformen zum Tragen kommen muss, sind proaktive Pflichten, die – dem Zweck des Datenschutzes, die Verarbeitungsfolgen in geordnete, „verbindlich vorgezeichnete" Bahnen zu lenken,[255] folgend – den Verantwortlichen zwingen, bereits im Vorfeld einer konkreten Verarbeitung oder Verarbeitungsreihe sein Umfeld unter Berücksichtigung der Risiken für Betroffene datenschutzkonform auszugestalten und die entsprechenden Maßnahmen zu ergreifen, um absehbare Gefahren zu erkennen und abzumildern. Ein hierauf gerichteter Fokus entspricht zudem dem oben[256] festgestellten Zurechnungstatbestand der Verantwortlichkeit für die Plattform als selbstgeschaffenes Verarbeitungsumfeld und nicht für individuelle Datenverarbeitungen.[257]

Für Plattformbetreiber, die nicht unmittelbar an den Verarbeitungen von Diensteanbietern und Drittparteien beteiligt sind und deren die Verantwortlichkeit auslösende Handlung gerade der Betrieb und die Ausgestaltung ihrer Plattform ist, ist diese Art von Pflichten besonders relevant. Die größten Auswirkungen auf das Verarbeitungsverhalten von Diensteanbietern und Drittparteien, aber auch auf die Stellung und Ermächtigung von Nutzern im Rahmen ihrer Rolle als datenschutzrechtliche Betroffene, haben die Entscheidungen hinsichtlich der Ausgestaltung der eigenen Plattform, ihrer Infrastruktur und ihrer Nutzungsregeln. Wie in Kapitel 1 ausführlich dargelegt wurde, machen Plattformbetreiber bereits jetzt, also ohne rechtliche Verpflichtung, breitflächig und bewusst Gebrauch von dieser Gestaltungsmacht, um die Nutzung und Entwicklung der Plattform so lenken, wie es ihren Werten und Vorstellungen entspricht.[258] Gleichzeitig müssen sie auf die Befindlichkeiten von Diensteanbietern (und in begrenztem Ausmaß auch Nutzern) Rücksicht nehmen, um das fragile Gleichgewicht zwischen Kontrolle und kreativitätsfördernder Freiheit, das der Wertschöpfung auf Plattformen zugrunde liegt und von dem Plattformbetreiber profitieren, nicht zu stören. Die letztendlich implementierten Entscheidungen sind daher sehr volatil und Ergebnis eines stetigen Aushandlungsprozesses zwischen Plattformbetreiber und Diensteanbieter und eines stetigen Balanceakts zwischen Kontrolle und Freiheit. Dieser Tatsache müssen proaktiv

---

255 *Hornung/Spiecker gen. Döhmann*, in: Simitis u. a., DSGVO/BDSG, Einleitung Rn. 18.

256 Abschnitt B. II. 2. c) in diesem Kapitel.

257 Eine entsprechende Verlagerung „from the responsibility for outcomes to the responsibility for the design of organizations" wurde von *Thompson*, The American Review of Public Administration 2014, 259 (261) bereits für Szenarien mit vielen beteiligten Akteuren, wenn auch im Bereich staatlicher Institutionen, aufgezeigt; eine erste Übertragung dieses Gedankens auf das Design von Plattformen findet sich bei *Helberger* u. a., The Information Society 2018, 1 (4).

258 Vgl. auch *Greene/Shilton*, New Media & Society 2018, 1640 (1640 ff.).

ausgerichtete Gestaltungspflichten Rechnung tragen, was freilich aber nicht bedeuten soll, eine geringere Wirkung oder Reichweite dieser Pflichten im Interesse zufriedener Diensteanbieter in Kauf zu nehmen. Es muss aber bedeuten, Plattformbetreibern hinreichend viel Spielraum bei der Art und Weise ihrer Erfüllung zu lassen, indem man mit Blick auf diesen Aushandlungsprozess darauf vertraut, dass ihre Erfahrung und Expertise im Umgang mit derartigen Entscheidungen ebenso wie der regelmäßige Austausch mit Diensteanbietern zur Findung von Lösungswegen beiträgt, die der Verordnungsgeber nie selbst hätte vorgeben können.[259] Wie die Betrachtung der einzelnen Instrumente der DSGVO in Kapitel 2 B. 1. aufgedeckt hat, sind derartige Pflichten, etwa im Bereich der regulierten Selbstregulierung, schon Bestandteil des bisherigen Konzepts und könnten daher im Grundsatz sachgerecht adaptiert werden.

aa) Privacy by design

Eine erste auf die Stellung und spezifische Machtposition von Plattformbetreibern passende Pflicht ist die zur datenschutzfreundlichen Technikgestaltung in Art. 25 Abs. 1 DSGVO. Ziel dieser Pflicht ist es bereits klassischerweise, *id est* bei ihrer Anwendung auf bisherige Verantwortliche, durch frühzeitige Gestaltung der gesamten Verarbeitung und ihrer Umstände dafür zu sorgen, dass die Datenschutzgrundsätze des Art. 5 DSGVO und die Anforderungen der Verordnung insgesamt erfüllt werden.[260] Werden damit bereits im Stadium der Entwicklung eines Verarbeitungssystems datenschutzrechtliche Grundsätze in das Design des Systems „eingegossen", so der Gedanke, unterstützt dies später einerseits den wohlwollenden Verantwortlichen bei seinen Bemühungen um datenschutzkonforme Ausführung der Verarbeitung(en) und erschwert gleichzeitig ungewollte wie auch beabsichtigte Verstöße.[261] Dass Plattformbetreiber diese Funktion – auch ohne rechtliche Verpflichtung – durch ihre Designentscheidungen bereits ausüben, wurde zuweilen bereits beobachtet. So konstatierten *Greene & Shilton* etwa mit Verweis auf die entsprechende Wirkung von Ausgestaltungsentscheidungen: „‚Privacy by design' is thus perhaps better termed, at least in the mobile development space, ‚privacy permitted by design' or ‚privacy by platform'."[262]

Bisher waren im Rahmen von Art. 25 Abs. 1 DSGVO zwei größere Wirksamkeitsbarrieren auszumachen: zum einen der begrenzte Adressatenkreis auf die *Nutzer* datenverarbeitender Systeme und Dienste, die auf die konkrete Gestaltung in den allermeisten Fällen kaum Einfluss hatten, während die *Herstel-*

[259] Hier zeigen sich klare Parallelen zu den bereits vom Datenschutzrecht genutzten Instrumenten der regulierten Selbstregulierung. Vgl. dazu die Ausführungen in Kapitel 2 B. I. 1. c) und d) sowie 2. a) bb).

[260] *Hansen*, in: Simitis u. a., DSGVO/BDSG, Art. 25 DSGVO Rn. 17.

[261] Vgl. *Hansen*, in: Simitis u. a., DSGVO/BDSG, Art. 25 DSGVO Rn. 17.

[262] *Greene/Shilton*, New Media & Society 2018, 1640 (1657).

ler als entscheidungsrelevante Akteure der Pflicht gerade nicht unterfielen;[263] zum anderen die Befürchtung einer praktischen Irrelevanz der Norm, bedingt durch die Tatsache, dass bei einer möglichen Verletzung der Pflicht stets auch eine Verletzung einer konkreten materiellen Pflicht sehr wahrscheinlich und vorrangig relevant wäre.[264]

Beiden Bedenken würde eine Anwendung auf Plattformhersteller grundlegend entgegenwirken. Im Verhältnis zu Diensteanbietern nehmen sie eine den Herstellern von Software und Systemen nicht unähnliche Rolle ein. Diensteanbieter entwickeln zwar in (je nach Offenheit der Plattform graduell unterschiedlicher) Freiheit und nach eigener Kreativität ihre Dienste, greifen dabei aber auf die vom jeweiligen Plattformbetreiber zur Verfügung gestellten Werkzeuge zurück und sind hinsichtlich der Möglichkeitsräume bei der Nutzung des Dienstes auf das begrenzt, was auf Ebene der Infrastruktur, auf die der Dienst aufsetzt, erlaubt und möglich ist. Auch hier wäre es daher angebracht, bereits den Plattformbetreiber zu einer datenschutzfreundlichen Gestaltung zu verpflichten, zumal neben Diensteanbietern eben auch Drittparteien „Nutznießer" dieser vorgefertigten Gestaltung sind. Darüber hinaus würde die Pflicht des Art. 25 DSGVO hier eine weit zentralere Rolle einnehmen, als sie dies in ihrem Verhältnis zu den zahlreichen Pflichten, die die Rechtmäßigkeit einer Datenverarbeitung bestimmen, bisher tat. Da Plattformbetreiber im Rahmen der hier vertretenen Verantwortlichkeit gerade nicht für die Rechtmäßigkeit konkreter Datenverarbeitungen verantwortlich sind, sondern nur für den Zustand ihrer Plattform und den Umgang mit den auf ihr agierenden Akteuren, ist der Pflichtenkatalog (jedenfalls hinsichtlich der bestehenden Pflichten der DSGVO) von vornherein stark begrenzt, sodass Art. 25 DSGVO zwangsläufig an Relevanz gewinnt.

Eine solche Pflicht, angewendet auf Plattformbetreiber, würde daher Folgendes bedeuten: eine Pflicht zur einer Ausgestaltung der eigenen Plattform dergestalt, dass damit möglichst weitreichend die Datenschutzgrundsätze des Art. 5 DSGVO sowie generell alle Voraussetzungen einer datenschutzkonformen Verarbeitung erfüllt werden, wenn einzelne Diensteanbieter oder, in abgeschwächter Form, Drittparteien konkrete Datenverarbeitungen vornehmen. Der oben formulierte Idealzweck der Norm in Form einer Unterstützung der späte-

---

[263] So, allgemein zur Fixierung des Datenschutzrechts auf die rein datenverarbeitenden Akteure, schon *Roßnagel*, MMR 2005, 71 (74 f.): „Statt Regelungsadressaten ohne Einfluss zu wählen, sollten diejenigen verpflichtet werden, die auch die entsprechenden Handlungsmöglichkeiten haben." In dieselbe Richtung auch *Hansen*, in: Simitis u. a., DSGVO/BDSG, Art. 25 Rn. 21; ebenso *Richter*, DuD 2012, 576 (580); eher vermittelnd und auf die Möglichkeiten des mittelbaren Drucks auf Hersteller durch Auswahl datenschutzfreundlicher Software durch Verantwortliche hinweisend *Buss*, CR 2020, 1; auch *Bygrave*, in: Kuner u. a., GDPR, S. 578 betont die Hoffnung, so die Erwartung mittelbar an Hersteller weiterzugeben: „Thus, the regulation evinces an expectation that the duty […] will be passed […] to technology developers."

[264] So etwa *Hansen*, in: Simitis u. a., DSGVO/BDSG, Art. 25 DSGVO Rn. 17.

ren Bemühungen datenschutzkonformen Verarbeitens sowie des Erschwerens bewusster oder unbewusster datenschutzwidriger Verhaltensweisen bleibt also bestehen. Er bezieht sich aber nicht mehr auf die eigene Person oder Organisation des Normpflichtigen, sondern auf *andere* Verantwortliche in Person von Diensteanbietern und Drittparteien, sodass sich der Bezugspunkt insofern verschiebt. Konkret lassen sich dabei zwei Zielrichtungen ausmachen: eine unmittelbar auf das Verhalten und die Möglichkeitsräume von den verschiedenen Arten von auf der Plattform aktiven Verantwortlichen gerichtete ((1)) und eine auf die Stellung von Betroffenen im Verhältnis zu diesen gerichtete ((2)). In beiden Fällen kann die Pflicht sich auf die beiden der oben in Kapitel 1[265] identifizierten Kontrollebenen auswirken: die Ebene der vertraglichen ebenso wie die Ebene der technischen Absicherung.

(1) Zielrichtung Verantwortliche

Hinsichtlich der auf einer Plattform aktiven Verantwortlichen, namentlich also Diensteanbieter und Drittparteien, betrifft die Pflicht zur datenschutzfreundlichen Ausgestaltung der Plattform in erster Linie die Ausgestaltung der einzelnen Schnittstellen oder APIs, die den Zugriff auf unterschiedliche Kategorien von Nutzerdaten ermöglichen. Dies geht jedoch nur im Zusammenspiel mit den Nutzungs- und Entwicklerrichtlinien, die bestimmtes Verhalten erlauben oder verbieten bzw. die Prozesse klarstellen, nach denen gehandelt wird, sodass auch deren Ausgestaltung Teil der Gestaltungspflicht sein muss. Gilt es etwa, im Interesse des Prinzips der Datenminimierung zu garantieren, dass Diensteanbieter nur diejenigen Daten verarbeiten, die für die Erreichung des selbst formulierten Zwecks notwendig sind, muss einerseits der Aufnahmeprozess auf die Plattform oder der Prozess zur Einholung von Zugriffsberechtigungen auf Daten so ausgestaltet sein, dass die formulierten Zwecke dem Plattformbetreiber im Vorfeld mitgeteilt werden. Andererseits muss die Ausgestaltung der Zugriffsschnittstellen und -kanäle korrespondierend ausgerichtet sein, damit dem Diensteanbieter möglichst auch nur diejenigen Zugriffe auf diejenigen Datenkategorien in dem Umfang möglich sind, wie sie der mitgeteilte Zweck verlangt. Ebenso, wie die (deutsche) Übersetzung von *privacy by design* als datenschutzfreundliche *Technik*gestaltung gemeinhin als zu eng angesehen wird,[266] zeigt sich auch hier, dass die Gestaltungspflicht nicht rein technisch erfüllt werden kann, sondern zwingend auch organisatorisch-prozessuale Elemente benötigt.[267] Eine von Zugriffsberechtigungen abhängige limitierte Möglichkeit der

[265] Siehe Kapitel 1 B. II.

[266] *Hansen*, in: Simitis u. a., DSGVO/BDSG, Art. 25 DSGVO Rn. 16 weist zurecht darauf hin, dass der Begriff der „Technik" in den meisten Sprachfassungen der Norm nicht vorkommt.

[267] Vgl. *Hansen*, in: Simitis u. a., DSGVO/BDSG, Art. 25 DSGVO Rn. 16: „Demnach erstreckt sich die Gestaltungsanforderung auf die gesamte Verarbeitung einschließlich der organisatorischen Prozesse sowie der rechtlichen Ausgestaltung für den konkreten Fall."

Nutzung von Datenschnittstellen funktioniert schließlich nur dann, wenn entsprechend abgestimmte Prozesse zum Abgleich mit der ggf. erteilten Berechtigung existieren. Setzt man noch eine Ebene weiter oben an, muss ein Plattformbetreiber sich auch schon vorgelagerte Gedanken über die datenschutzadäquate Festlegung der Datenkategorien an sich sowie der Arten von Zugriffsberechtigungen machen. Dabei muss jedoch stets klar bleiben, dass die rechtliche Determinierung meist nur schwach bleibt, der Plattformbetreiber also viel Freiheit bei der Wahl eines zu ihm passenden Ausgestaltungskonzepts genießt und auch die Reichweite dessen, was von ihm verlangt wird, von den in Art. 25 DSGVO explizit genannten Kriterien des Stands der Technik, der Implementierungskosten, der Verarbeitungsumstände des Einzelfalls sowie der jeweils drohenden Risiken und ihrer Schwere und Eintrittswahrscheinlichkeiten abhängt. So muss es durchaus möglich bleiben, dass der Plattformbetreiber seiner Pflicht in ausreichendem Maße nachgekommen ist, obwohl im Einzelfall datenschutzwidrige Verarbeitungen durch einen Diensteanbieter (oder eine Drittpartei) auftreten.

In dieser Hinsicht erfüllt die Pflicht in jedem Fall die Erwartung, durch datenschutzfreundliche Gestaltung der Plattform und ihrer Nutzungsbedingungen datenschutzwidriges Fehlverhalten zu erschweren. Gleichzeitig kann es auch dabei behilflich sein, den Diensteanbieter konstruktiv in seinen Bemühungen zu unterstützen und damit, insbesondere im Verhältnis zu Drittparteien, bestehende Kontrolldefizite auszugleichen und somit auch übergeordnete Defizite auf konzeptioneller Ebene des Datenschutzes teilweise zu kompensieren. Die bereits angesprochene Absicherung eines Berechtigungsmanagements für Zugriffe auf bestimmte Datenkategorien sorgt etwa auch dafür, dass sich die fehlende Möglichkeit von Diensteanbietern, das Handeln der von ihnen einbezogenen Drittparteien effektiv zu überwachen und damit die Einhaltung der vereinbarten Bedingungen zu kontrollieren, weniger stark auswirkt. Der Plattformbetreiber kann so punktuell die Kontrolle für Diensteanbieter übernehmen bzw. die Möglichkeitsräume von Drittparteien gezielt so eingrenzen, dass eine Kontrolle nicht mehr nötig ist. Auch hier sind der Effektivität solcher Maßnahmen aber naturgemäß Grenzen gesetzt. Denkbar wäre daneben die Kompensation von Transparenzdefiziten, indem bspw. jeder Datenzugriff von Drittparteien protokolliert und den betreffenden Diensteanbietern offengelegt wird, sodass letztere in die Lage versetzt werden, die Einhaltung der von ihnen aufgestellten Kooperationsbedingungen durch die Drittparteien zu kontrollieren. Im Idealfall würden Diensteanbieter so in die Lage versetzt, ihre eigenen Auswahl- und Überwachungspflichten[268] besser erfüllen zu können.

Auf einer ähnlichen Ebene kann der Plattformbetreiber bei der Begrenzung von Möglichkeitsräumen durch Gestaltungsmaßnahmen eine kompensatorische Rolle einnehmen, indem er als verlängerter Arm für Aufsichtsbehörden agiert.

[268] Siehe *supra* bei C. III. 2. b.

Ist bspw. der Einsatz bestimmter Technologien oder ist die Nutzung bestimmter Methoden zum Einbezug von Drittparteien untersagt worden, so kann der Plattformbetreiber ihre Nutzung auf seiner Plattform global unterbieten und so (Umgehungsversuche einmal ausgenommen) einen Komplettvollzug der Anordnung erreichen, wo sonst eine Überprüfung unmittelbar bei jedem einzelnen Diensteanbieter kaum durchführbar gewesen wäre.

Neben diesen möglichkeitsraumverengenden und unterstützenden Gestaltungsausübungen wäre eine weitere Ebene der datenschutzfreundlichen Gestaltung das Setzen von Anreizen zu demonstrativ datenschutzkonformem oder sogar überobligatorisch datenschutzfreundlichem Verhalten durch die anderen Verantwortlichen. Denkbar wäre es etwa, außerordentlich datenschutzfreundliche Diensteanbieter im eigenen Distributionskanal besonders prominent zu platzieren und bei Nutzersuchen weiter oben zu listen. Diensteanbieter, die gänzlich ohne Drittparteien auskommen, könnten ebenfalls als solche gekennzeichnet und so als Positivbeispiel wahrnehmbar gemacht werden.[269]

Meist dürften keine klaren Vorgaben existieren und wäre eine Pflicht zu datenschutzfreundlicher Plattformgestaltung daher, ähnlich wie ein großer Teil der DSGVO-Pflichten auch schon klassischerweise, in großem Maße konkretisierungsbedürftig. Während dies Plattformbetreibern, wie bereits erwähnt, weitgehende Gestaltungsfreiheit geben würde, ist die Kehrseite derselben Medaille eine gewisse Rechtsunsicherheit. Es bedürfte hier daher derselben Mechanismen zur Schaffung von Rechtssicherheit und Vorhersehbarkeit, die die DSGVO im Rahmen ihrer Pflichten sowieso schon bereithält. Dazu gehört die Umsetzung von *best practice*-Verhaltensregeln gem. Art. 40 Abs. 1 DSGVO oder die Zertifizierung der eigenen Maßnahmen gem. Art. 42 DSGVO.

(2) Zielrichtung Betroffene

Gleichzeitig verlangt die Pflicht mit Blick auf die Stellung von Betroffenen eine Ausgestaltung dergestalt, dass diese ihre Selbstschutzmaßnahmen besser und leichter wahrnehmen können und Diensteanbietern, insbesondere aber Drittparteien, nicht schutzlos ausgeliefert sind. Eine solche Gestaltung kann etwa auf niedrigschwelliger Ebene darin bestehen, sicherzustellen, dass die Datenschutzerklärung eines Diensteanbieters in der App leicht auffindbar und gut sichtbar angezeigt oder verlinkt ist und vor der ersten Nutzung bzw. Verarbeitung von Daten prominent auf sie hingewiesen wird. Denkbar ist es auch, diese direkt im Distributionskanal wie AppStore von Apple oder dem Play Store von Google auf der Überblicksseite des jeweiligen Dienstes anzuzeigen, sodass Nutzer sie

[269] In diese Richtung gehen auch die kürzlich von Apple unter iOS eingeführten *privacy labels*, vgl. Nick Statt, Apple launches new App Store privacy labels so you can see how iOS apps use your data, The Verge vom 14.12.2020 (https://www.theverge.com/2020/12/14/22174017/apple-app-store-new-privacy-labels-ios-apps-public). Zuletzt abgerufen am 14.01.2022.

schon vor Installation der App bzw. des Dienstes betrachten können. Insbesondere hinsichtlich der notorisch schwer überschaubaren Drittparteien könnten hier klare Vorgaben dafür gemacht werden, wie und in welcher Detailfülle die einzelnen Drittparteien aufgeführt und mit ihren jeweiligen Datenschutzerklärungen und Kontaktadressen versehen werden müssen.[270] Eine derart zentralisierte Handhabe über den Distributionskanal des Plattformbetreibers ist auch für die Ausübung von Betroffenenrechten denkbar. So könnten Diensteanbieter verpflichtet werden, neben der Beschreibung ihres Dienstes und ggf. ihrer Datenschutzerklärung auch die direkten Links zur Ausübung von Auskunftsansprüchen oder anderen Rechten bereitzustellen. Um die grassierende Problematik gänzlich ignorierter oder nur unzureichend beantworteter Ansprüche[271] einzuhegen, käme hier auch ein Beschwerdekanal für Betroffene in Betracht, durch den Plattformbetreiber auf systematisch betroffenenrechtswidrig handelnde Diensteanbieter aufmerksam gemacht werden könnten.

Auch die Art und Weise, wie Einwilligungen eingeholt werden, könnte von Plattformbetreibern so gestaltet werden, dass eine gewisse Garantie für die Einhaltung von Mindeststandards hinsichtlich Kriterien wie Freiwilligkeit oder Informiertheit oder der leichten Ausübbarkeit des Widerrufs der Einwilligung gewährleistet wird. Zudem könnten Plattformbetreiber zu einer nutzerfreundlichen Darstellung und Konfigurierbarkeit der Gesamtheit bereits erteilter Einwilligungen der Nutzer verpflichtet werden, wozu etwa auch die regelmäßige Erinnerung daran gehören könnte, welche länger nicht genutzten Apps und Dienste trotz Nichtnutzung noch immer Daten verarbeiten dürfen.[272] So könnte zumindest einem Teil der typischen Überforderung von Nutzern mit Einwilligungen entgegengewirkt werden.

Die Entwicklungen hin zu zunehmend granularen Einzelentscheidungen für Nutzer bei der Erteilung von Berechtigungen zu Datenzugriffen, die insbesondere Apple und Google auf ihren mobilen Betriebssystemen in den vergangenen Jahren angestoßen haben,[273] zeigen einmal mehr, dass Plattformbetreiber ihre Macht in bestimmten Szenarien ohnehin bereits mittels solcher Maßnahmen

---

[270] In eine ähnliche Richtung gehend *Westerlund/Enkvist*, jipitec 2016, 2 (8).

[271] Vgl. die Studienergebnisse bei *Kröger* u. a., How do app vendors respond to subject access requests?, S. 9 f.: „[…] besides a general lack of responsiveness, the observed problems range from malfunctioning download links and authentication mechanisms over confusing data labels and file structures to impoliteness, incomprehensible language, and even serious cases of carelessness and data leakage."

[272] Vgl. *Westerlund/Enkvist*, jipitec 2016, 2 (8): „[…] an additional obligation that includes the management, storing and maintaining, of specific consents to any additional third party services […]." Eine solche Pflicht bewegte sich annähernd in die Richtung der vielfach diskutierten Datentreuhandmodelle. Siehe dazu *Ulmenstein*, DuD 2020, 528 (528 ff.); vgl. auch *Balkin*, Harv. L. Rev. 2020, 11 (13 ff.).

[273] Für eine kritische Bestandsaufnahme der Entwicklung des Berechtigungsmodells von Datenzugriffen unter Android siehe *Alepis/Patsakis*, in: Ali/Danger/Eisenbarth, Security, Privacy, and Applied Cryptography Engineering, S. 53 (53 ff.).

ausüben, die Pflichten wie die des Art. 25 Abs. 1 DSGVO bei unterstellter Anwendbarkeit von ihnen verlangen würden.

bb) Datenschutzfolgenabschätzung

Eng verknüpft mit der Pflicht zur datenschutzfreundlichen Ausgestaltung der Plattform und gewissermaßen eine Ebene über dieser angesiedelt passt auch die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung gem. Art. 35 Abs. 1 DSGVO gut zur bereits identifizierten Stellung eines Plattformbetreibers. Nimmt man als gegeben hin, dass Plattformbetreiber einer Pflicht zur datenschutzfreundlichen Ausgestaltung ihrer Plattform unterworfen sind, ist es nur konsequent, ihnen auch eine vorgelagerte Pflicht dahingehend aufzubürden, die Implikationen ihrer Gestaltungsentscheidungen hinsichtlich der Risiken für Rechte und Interessen der eigenen Nutzer durch auf der Plattform stattfindende Datenverarbeitungen abzuschätzen und mögliche Abhilfemaßnahmen zu eruieren. Die Pflicht könnte einerseits bei jeder Gestaltungsentscheidung bzgl. der Plattform insgesamt, andererseits im Einzelnen bei jeder Entscheidung über die Aufnahme eines neuen Akteurs relevant werden. Wie schon bei der Pflicht nach Art. 25 Abs. 1 DSGVO müsste hierfür bloß der Anknüpfungspunkt der Pflicht geändert werden, sodass diese sich nicht mehr, wie bisher, auf „eine Form der Verarbeitung" und das daraus erwachsende Risiko, sondern auf die Infrastruktur und Nutzungsbedingungen der Plattform im Verhältnis zu den auf dieser Ebene später stattfindenden Verarbeitungen bezieht.[274] Vorteilhaft wäre hier zudem die vorherige Konsultation gem. Art. 36 DSGVO, durch die ein direkter Austausch mit der zuständigen Aufsichtsbehörde hergestellt und die gewählten Maßnahmen der datenschutzfreundlichen und -absichernden Ausgestaltung begutachtet werden. Hinsichtlich der Anwendbarkeit der Norm wäre es im Interesse der bereits unter II. diskutierten Notwendigkeit nach Flexibilität denkbar, die Frage der Notwendigkeit der Durchführung einer Folgenabschätzung wie in der Norm vorgesehen dem einzelnen Plattformbetreiber zu überlassen. Denkbar wäre aber auch die pauschale Anwendbarkeit für jeden Plattformbetreiber mittels Aufnahme auf eine Blacklist gem. Art. 35 Abs. 4 S. 1 DSGVO oder – mit Blick auf eine homogene Anwendung der Verordnung vorzugswürdig – durch Änderung des Art. 35 Abs. 3 DSGVO und Aufnahme von Plattformbetreibern in dessen Liste.

cc) Auswahlpflicht

Mit Blick auf die ebenfalls in vielen Fällen auf Basis der Nutzungs- und Entwicklerrichtlinien stattfindenden Aufnahmekontrollen auf die Plattform bzw. in

[274] Wie eine so verstandene Datenschutzfolgenabschätzung eines nicht selbst datenverarbeitenden Akteurs aussehen könnte, zeigen *Schulz* u. a., in: Leenes/Hallinan/Gutwirth/de Hert, Data protection and privacy: data protection and democracy, S. 145 (145 ff.).

den Distributionskanal wäre eine Pflicht zur sorgfältigen Auswahl von Diensteanbietern ebenfalls passend. Wie schon oben unter C. zur Verantwortlichkeit von Diensteanbietern ausgeführt, würde dies auch vom Plattformbetreiber verlangen, die Aufnahme auf die Plattform begehrenden Diensteanbieter sorgfältig auf ihre Bemühungen zu datenschutzkonformem Verhalten hin zu untersuchen. Denkbar wäre auch hier in Anlehnung an das Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter das Vorzeigen ausreichender Garantien zu verlangen – sowohl hinsichtlich der vom Diensteanbieter selbst vorzunehmenden Datenverarbeitungen als auch hinsichtlich der von den einbezogenen Drittparteien zu erwartenden Verarbeitungen.

Die Reichweite der Pflicht, das heißt die vom Plattformbetreiber an den Tag zu legende Prüfdichte, wäre dabei in großem Maße abhängig davon, wie offen oder geschlossen die Plattform grundsätzlich ausgestaltet ist. So liegt nahe, dass auf Googles mobilem Betriebssystem Android die Prüfpflicht sich von vornherein nur auf diejenigen Apps beziehen kann, die über den eigenen Distributionskanal Play Store vertrieben werden. Apps, die von den Nutzern frei heruntergeladen und installiert werden können – eine Möglichkeit, die Google im Gegensatz zu Apple vorsieht –, können nachvollziehbarer Weise nicht kontrolliert werden. Naheliegend wäre es jedoch, bei einem solchen Minus auf Prüfungsebene ein kompensierendes Plus auf Ebene einer der anderen Pflichten zu verlangen. So könnte vom Plattformbetreiber verlangt werden, die Möglichkeit der freien Installation von Diensten standardmäßig zu deaktivieren und so von der aktiven Willensbekundung des Nutzers abhängig zu machen (so, wie es heute bspw. bereits bei Googles Android der Fall ist) und diesen explizit auf die Risiken der Installation einer solchen ungeprüften App hinzuweisen.

b) Reaktive Pflichten

Während die proaktiven Pflichten und unter diesen vor allen Dingen die Pflicht zur datenschutzfreundlichen Ausgestaltung der Plattform im Mittelpunkt der Plattformverantwortlichkeit stehen, kommen auch Pflichten in Betracht, die an bereits ausgeführte Datenverarbeitungen und insbesondere an bekannt gewordene Datenschutzverstöße anknüpfen.

Hier ist zunächst und als Gegenstück zur eben geschilderten Auswahlpflicht eine anhaltende Pflicht zur Beobachtung der auf der Plattform aktiven Diensteanbieter und ihrer Drittparteien zu nennen. Dabei muss gelten, dass bekannt gewordene Verstöße Konsequenzen nach sich ziehen müssen. Das gilt einerseits für eigene Verstöße eines Diensteanbieters – hier käme ein abgestuftes System in Betracht, das von einer Verwarnung über eine Auslistung oder Herabstufung der Anzeige im Distributionskanal und eine Verweigerung des Zugriffs auf alle nicht essenziell für die Funktionsweise des Dienstes notwendigen Nutzerdaten bis hin zum kompletten und ggf. dauerhaften Ausschluss von der

Plattform reicht. Da insbesondere die letztgenannte Maßnahme auch Nutzerinteressen betrifft, wäre dabei ein Vorgehen, das den Dienst auf der Plattform belässt und allein die Datenströme limitiert, stets vorzugswürdig und ein kompletter Ausschluss daher immer *ultima ratio*. Es gilt andererseits auch für Verstöße durch Drittparteien – hilft ein Diensteanbieter hier nicht ab, indem er die betreffende Drittpartei aus seinem Dienst ausschließt, kann der Plattformbetreiber ihn durch die eben genannten Sanktionen so lange unter Druck setzen, bis er dies tut, und die datenschutzwidrig handelnden Drittparteien global auf der gesamten Plattform flaggen und ihre Nutzung auch anderen Diensteanbietern verbieten. Die Idee des Plattformbetreibers als verlängerter Arm der Aufsichtsbehörden manifestiert sich hier erneut.

Konzeptionell ließe sich eine solche Pflicht als verschärfte Form der aus dem bereits erwähnten Rechtsregime der Intermediärshaftung bekannten *notice and takedown*-Pflichten verstehen. Damit müsste ein Plattformbetreiber über die oben beschriebenen proaktiven Pflichten hinaus spätestens dann Restriktionen gegenüber Diensteanbietern oder Drittparteien aussprechen, wenn er positives Wissen über mögliche datenschutzwidrige Verhaltensweisen des betreffenden Akteurs erlangt und diese Möglichkeit sich, ggf. nach eigenen Kontrollen und Nachprüfungen, als hinreichend wahrscheinlich erhärtet. Das initiale Wissen könnte etwa über Mitteilungen Betroffener oder der Aufsichtsbehörden erlangt werden; auch die öffentliche Berichterstattung über publik gewordenes Fehlverhalten könnte als Ansatzpunkt für weitergehende Ermittlungen durch den Plattformbetreiber dienen. Denkbar wären aber auch sog. *trusted notifiers* – privilegierte Akteursgruppen mit besonderer Expertise bei der Beurteilung der entsprechenden Rechtsfragen, die genau zu diesem Einsatz aktiv wären und deren Einschätzung erhöhte Bedeutung zukommen würde.[275] Hierfür kämen die insofern bereits über Art. 80 DSGVO in das Instrumentarium der Verordnung einbezogenen Interessenverbände wie bspw. Verbraucherschutzbehörden in Betracht, sofern sie ihre Sachkunde entsprechend unter Beweis stellen und sich etwa von einer Aufsichtsbehörde akkreditieren lassen.

Würden damit Diensteanbieter oder Drittparteien beim hinreichend wahrscheinlichen Vorliegen datenschutzwidriger Praktiken beim Abruf von Nutzerdaten auf der Plattform – zunächst temporär – von der Plattform ausgeschlos-

[275] Diese spielen teilweise bereits im Bereich der Intermediärshaftung für Inhalte auf sozialen Netzwerken und anderen Plattformen eine Rolle. Siehe etwa die Ausführungen bei *Schwemer*, CLSR 2019, 105339. Auch die Europäische Kommission hat diese Akteure bereits in ihre Empfehlungen aufgenommen. Siehe den Abschnitt 6 zu „Trusted Flaggers" bei *European Commission*, Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee Of The Regions: Tackling Illegal Content Online – Towards an enhanced responsibility of online platforms: „Compared to ordinary users, trusted flaggers can be expected to bring their expertise and work with high quality standards, which should result in higher quality notices and faster take-downs."

sen oder an der Verarbeitung nicht nutzungsrelevanter Daten gehindert, bis eine Aufsichtsbehörde oder ein Gericht über die Datenschutzwidrigkeit entschieden hat, könnte dies einen großen Schritt für das momentan vorherrschende Rechtsdurchsetzungsdefizit des Datenschutzrechts darstellen. Naturgemäß bedürfte es hier flankierender Verfahrenspflichten, die sicherstellen, dass die Rechte und Interessen betroffener Diensteanbieter und Drittparteien gewahrt würden. Ebenso müssten die einer solchen Herangehensweise inhärenten Missbrauchsrisiken berücksichtigt und Überlegungen angestellt werden, wie die Aufsichtsbehörden und Gerichte die resultierende Mehrbelastung kompensieren könnten. Hier ließe sich die reichhaltige Literatur aus dem Bereich der Intermediärshaftung und in jüngerer Vergangenheit auch dem NetzDG zur Inspiration heranziehen.[276] Als zwingend erschiene hier etwa eine Pflicht zur Anhörung des sanktionierten Akteurs vor Durchführung der Sanktion. Auch der prozessuale Ablauf der Prüfung durch den Plattformbetreiber müsste rechtlich vorgegeben und transparent sein, um durch entsprechende Verfahrensvorgaben ein möglichst hohes Niveau der Entscheidungen sicherzustellen – hier wäre etwa eine zwingende Rücksprache mit der zuständigen Aufsichtsbehörde eine naheliegende Option. Ebenso elementar wäre ein Anspruch des betroffenen Akteurs auf erneute Überprüfung der Entscheidung und ggf. Rücknahme der ausgesprochenen Sanktion. Missbräuchlichen Meldungen und Sanktionen könnte zumindest teilweise durch die bereits erwähnte Einrichtung privilegierter *trusted notifiers* entgegengewirkt werden.[277]

Würde damit die Sanktion – also etwa der Ausschluss aus der Plattform oder der verwehrte Zugriff auf nicht nutzungsrelevante Nutzerdaten – solange bestehen bleiben, bis die Frage der Datenschutzwidrigkeit rechtskräftig entschieden ist, würde das einer effektiven Umkehr nicht nur der Beweis-, sondern auch der Prozesslast gleichkommen. Diensteanbieter und Drittparteien müssten selbst auf Feststellung der Datenschutzkonformität ihres Handelns klagen, um die Rücknahme der Sanktion zu erreichen.[278] Damit wäre nicht nur der Klage- und Klärungsmüdigkeit vieler Betroffener abgeholfen, sondern in Teilen auch der notorischen Überforderung der Aufsichtsbehörden – wenngleich natürlich im selben Zuge ein Zuwachs an Aufgaben durch den Austausch mit Plattform-

[276] Siehe etwa *Hofmann*, ZUM 2017, 102 (104 ff.); auch die Vorschläge von *Sahl/Bielzer*, ZRP 2020, 02 (3 ff.) zielen in diese Richtung. Siehe zudem *Liesching*, in: Eifert/Gostomzyk, Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, S. 135 (135 ff.).

[277] Auch hier lassen sich Vorbilder solcher anerkannten Einrichtungen etwa im JMStV oder jüngst im NetzDG finden. Vgl. *Spindler*, GRUR 2018, 365 (370 ff.).

[278] Vergleichbares wurde bereits im Bereich der Durchsetzung von Schadensersatzansprüchen unter der Fluggastrechte-VO vorgeschlagen. Vgl. *Nikolas Guggenberger*, Durchsetzung nach Datenlage, FAZ Einspruch Magazin vom 02.05.2018 (https://einspruch.faz.net//einspruch-magazin/2018-05-02/577043c294a3786dc1e9c1bb21a5d316/). Zuletzt abgerufen am 14.01.2022.

betreibern und das zu erwartende Plus an Prozessen auf Aufsichtsbehörden wie auch Gerichte zukäme.

c) Rechtsfolgen und Haftung

Hinsichtlich möglicher Rechtsfolgen bei Verletzungen der eben geschilderten Pflichten und insbesondere einer möglichen Haftung von Plattformbetreibern lässt sich erneut ein Abgleich mit dem bestehenden Rechtsfolgenregime der DSGVO vornehmen. Das duale System aus zivilrechtlichen und öffentlich-rechtlichen Rechtsfolgen[279] könnte grundsätzlich weiterhin zum Tragen kommen, müsste aber teils umfassend modifiziert werden, um der Tatsache Rechnung zu tragen, dass gerade keine Verantwortlichkeit für konkrete Datenverarbeitungen, sondern allein für die Ausgestaltung der eigenen Plattform und des eigenen Umgangs mit den Akteuren auf dieser besteht.

Hinsichtlich der in Art. 58 DSGVO aufgezählten Behördenmaßnahmen würde dies bedeuten, grundsätzlich alle Untersuchungs- und Abhilfemaßnahmen sowie Genehmigungs- und Beratungsbefugnisse entsprechend anzuwenden, soweit dies möglich ist. Anweisungen zur Bereitstellung der erforderlichen Informationen (Abs. 1 lit.a) sind ebenso denkbar wie Hinweise auf oder Warnungen vor vermeintlichen Verstößen (Abs. 1 lit. d, Abs. 2 lit. a) bzw. Verwarnungen bei bereits erfolgten Verstößen, sofern diese nicht mehr auf konkrete Verarbeitungsvorgänge, sondern auf ggf. nicht oder falsch erfolgte Ausgestaltungsentscheidungen oder Handlungen gegenüber Diensteanbietern und Drittparteien beziehen.

Gleichzeitig wären auch mittelbar auf konkrete Datenverarbeitungen bezogene Maßnahmen denkbar, wenn die zuständige Aufsichtsbehörde bereits die Datenschutzwidrigkeit der Vorgänge eines Diensteanbieters oder einer Drittpartei festgestellt hat und zusätzlich zu den diesem gegenüber erlassenen Maßnahmen auch den Plattformbetreiber anweist, die betreffende Partei durch einen temporären Ausschluss oder Datenzugriffsbeschränkungen daran zu hindern, die getroffenen Maßnahmen zu ignorieren oder bis zum Beweis der erbrachten Maßnahmen weiter Daten zu verarbeiten. Zweck der Anweisung an den Plattformbetreiber wäre hier also die Absicherung der Wirksamkeit der unmittelbar an den datenschutzwidrig verarbeitenden Akteur gerichteten Maßnahme(n). Hier gälte es sodann zweierlei zu unterscheiden: Während die Verletzung eigener Pflichten neben den bereits angesprochenen Maßnahmen als *ultima ratio* auch ein Bußgeld gem. Art. 58 Abs. 1, 2 DSGVO nach sich ziehen könnte, dürfte ein solches bei einer auf die Erbringung einer Maßnahme gegen einen konkreten Verantwortlichen gerichteten Anweisung erst dann erteilt werden, wenn der Plattformbetreiber sich dieser Anweisung widersetzt.[280]

---

[279] Siehe dazu *supra* in Kapitel 2 B. I. 1. e).

[280] Dabei ist dieser Fall einer konkreten Anweisung der Aufsichtsbehörde von den im vo-

Hinsichtlich der zivilrechtlichen Rechtsfolgen, die insbesondere in der Schadensersatzpflicht des Art. 82 Abs. 1 DSGVO zu sehen sind, gilt es weiter zu differenzieren. Würde man Betroffenen einen solchen Anspruch auf Schadensersatz gegen den Plattformbetreiber für jede Verletzung einer seiner Pflichten zusprechen, drohte in Anbetracht der oft immens großen Nutzerzahlen digitaler Plattformen möglicherweise die Gefahr einer überbordenden Haftung. Richtigerweise ist daher zunächst folgende Unterscheidung zu treffen: Die Verletzung einer den Plattformbetreiber treffenden Pflicht kann mit der Existenz konkreter datenschutzwidriger Verhaltensweisen durch Diensteanbieter und Drittparteien koinzidieren und wird dies regelmäßig auch tun, muss dies aber nicht. Dass ein (klassischer) Verantwortlicher die Möglichkeit hatte, auf einer Plattform datenschutzwidrig personenbezogene Daten zu verarbeiten, kann ein Indiz für eine Verletzung von Gestaltungspflichten des Plattformbetreibers sein, muss dies aber nicht – es ist schließlich nicht seine Pflicht, eine jede datenschutzwidrige Verarbeitung auf seiner Plattform zu unterbinden.[281] Gleichzeitig kommen auch großflächige strukturelle Missstände in Betracht, die eine Pflichtverletzung des Plattformbetreibers darstellen, ohne dass im Zusammenhang damit (schon) datenschutzwidrige Vorgänge durch andere Akteure aufgetreten oder schlicht bereits bekannt geworden wären. Naheliegend ist hier zunächst, dass schon aufgrund des Erfordernisses eines materiellen oder immateriellen Schadens bei den Betroffenen ein solcher Anspruch nur dort in Betracht kommt, wo ein Zusammenhang zu konkreten datenschutzwidrigen Verarbeitungen von Daten mit Bezug zu diesen Betroffenen bestand. Auch das Kausalitätserfordernis grenzt die Fälle dann ein, indem nur solche Schäden ersatzfähig sind, die gerade durch den Pflichtverstoß verursacht wurden, also in einem hinreichend engen Verursachungszusammenhang zu diesem stehen.[282] Hinzu kommt die Exkulpationsmöglichkeit in Abs. 3 der Norm, nach der der Verantwortliche sich von der Haftung befreien kann, indem er nachweist, hinsichtlich der Pflichtverletzung

---

rangegangenen Abschnitt beschriebenen Fällen zu unterscheiden, in denen der Plattformbetreiber im Rahmen seiner *notice and takedown*-Pflicht unabhängig von einer solchen Anweisung Kenntnis von datenschutzwidrigen Praktiken erlangt und nicht pflichtgemäß tätig wird. Hier kann, je nach Einzelfall, bereits das Untätigbleiben ohne vorherige behördliche Anweisung eine Pflichtverletzung darstellen und daher bei Vorliegen aller Voraussetzungen die Erteilung eines Bußgeldes nötig machen.

[281] Diese Grundprämisse liegt dem Datenschutzrecht bereits inne, verlangt sie doch von Verantwortlichen im Rahmen vielerlei Pflichten nicht den absoluten Ausschluss jeglichen Risikos, sondern nur die Minimierung, die im Bereich des Möglichen (unter anderem nach Maßgabe des Standes der Technik) ist. Prägnant auch aus dem Komplex der Intermediärsverantwortung *Frosio*, Int J Law Info Tech 2018, 1 (9): „We should not expect perfection from intermediaries, but responsible efforts like journalists who are entitled to make mistakes, if only they seek responsibly to avoid these." Dieser paraphrasiert dabei *Thompson*, Vand J Ent & Tech L 2016, 783 (783 ff.).

[282] Vgl. *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 82 DSGVO Rn. 41–45, auch zur umstrittenen Frage, ob ein unmittelbarer oder bloß ursächlicher Zusammenhang benötigt wird.

kein Verschulden an den Tag gelegt zu haben.[283] Schon über diese beiden Elemente des Schadensersatztatbestands lässt sich eine zielgerechte Eingrenzung erreichen, ohne die Norm textlich modifizieren zu müssen.

Überzeugend wäre es somit, die Kausalität nur in solchen Fällen bzw. für denjenigen Schaden zu bejahen, der nach Verletzung einer *reaktiven* Pflicht eintritt. Hat ein Plattformbetreiber also Kenntnis von einem vermeintlich datenschutzwidrigen Handeln eines Diensteanbieters oder einer Drittpartei erlangt und geht diesem Verdacht nicht weiter nach bzw. setzt trotz Offensichtlichkeit der Datenschutzwidrigkeit oder erhärtetem Verdacht nach weiterer Nachforschung keine entsprechenden Sanktionen um, und entsteht Betroffenen gerade durch dieses Versäumnis ein (ggf. zusätzlicher) Schaden, so hat der Plattformbetreiber diesen Schaden zu ersetzen. Eine Exkulpationsmöglichkeit kommt darüber hinaus in Einzelfällen in Betracht, wenn der Plattformbetreiber etwa Rücksprache mit der zuständigen Aufsichtsbehörde gehalten und mit deren Einverständnis oder auf deren Anraten hin keine Maßnahmen ergriffen hat. In allen anderen Fällen sollte ein Schadensersatzanspruch außer Betracht bleiben. Insbesondere bei Verletzung von reinen Gestaltungspflichten bzgl. der Plattforminfrastruktur, die den später erfolgenden Verarbeitungen durch andere Akteure noch weit vorgelagert sind, wäre die Annahme eines hinreichenden (wahlweise unmittelbaren oder ursächlichen) Kausalzusammenhangs mit dem Schaden der Gesamtheit der Nutzer des jeweiligen Dienstes zu weitgehend.

Der Schadensersatzanspruch des Art. 82 Abs. 1 DSGVO sollte daher grundsätzlich auch auf Plattformverantwortliche anwendbar sein, solange durch die Art seiner Auslegung und Anwendung sichergestellt ist, dass er nur in den begrenzten aufgezählten Fällen erfüllt ist.

3. Zwischenergebnis

Sinnvoll erscheint es *in toto* also, die Plattformverantwortlichkeit als vollständiges Teilkonzept und eigenständige Verantwortlichenfigur in das bestehende Verantwortlichkeitskonzept der DSGVO zu integrieren. Dabei sollte der Anknüpfungspunkt nicht die einzelne Verarbeitung eines Akteurs auf der Plattform sein, sondern die Ausgestaltung der Plattform mitsamt ihrer Schnittstellen, Nutzungsbedingungen und Kontrollmechanismen, kurz gesagt also den Möglichkeitsräumen, die den Akteuren auf der Plattform geboten werden. Dementsprechend bietet sich die Einteilung in *proaktive* (primär Gestaltungs-)Pflichten und *reaktive* (primär Kontroll-)Pflichten an.

---

[283] Siehe *Bergt*, in: Kühling/Buchner, DSGVO/BDSG, Art. 82 DSGVO Rn. 54 ff. bzgl. des Haftungsmaßstabs.

IV. Limitierungen und Problemstellen

Auch in diesem frühen Stadium der Konzeption einer neuen Plattformverantwortlichkeit lassen sich Limitierungen und Problemstellen eines solchen Konzepts ausmachen, die hier nicht unerwähnt bleiben sollen.

1. Zur Problematik der extraterritorialen Wirkung

Ein bereits unabhängig von dem hier propagierten Konzept breit diskutiertes Problem ist das der extraterritorialen Wirkung von Gesetzen, die den inhärent grenzüberschreitenden bzw. grenzenlosen digitalen Raum[284] regulieren sollen. Art. 3 Abs. 2 DSGVO ordnet mit dem Marktortprinzip eine solche extraterritoriale Wirkung an,[285] indem er die Anwendbarkeit der Verordnung auch auf Akteure außerhalb der EU erstreckt, soweit sie Daten mit Personenbezug zu in der EU befindlichen natürlichen Personen im Zusammenhang mit angebotenen Waren oder Dienstleistungen oder der Beobachtung des Verhaltens der betroffenen Personen verarbeiten.[286] Hinsichtlich der Erfüllung der Pflichten der DSGVO und anderer extraterritorial wirkender Gesetze stellt sich für die pflichtigen Akteure die Frage, ob und wie sie die zur Erfüllung der jeweiligen Pflicht nötigen Handlungen global ausführen oder ihre Wirkung, wo möglich, auf den Jurisdiktionsraum des jeweiligen Gesetzes begrenzen.[287] Bei globaler Wirkung droht hier ein Konflikt mit anderen Gesetzgebungen, die das geforderte Verhalten ihrerseits möglicherweise verbieten bzw. schlicht eine andere Abwägungsentscheidung für denselben Sachverhalt getroffen haben. Auch dort, wo die jeweils geltende Gesetzgebung noch gar keine Regelung vorweist, ist die globale Wirkung völkerrechtlich nicht unproblematisch, droht sie doch durch eine Art Rechtsimperialismus vollendete Tatsachen zu schaffen, mit denen Staaten dann leben müssen.[288]

---

[284] Siehe bereits *Roßnagel*, ZRP 1997, 27 (27 ff.), der insofern von der Regulierung des Internets als „körperlosem Sozialraum" spricht. Zudem *Köndgen*, AcP 2006, 477 (503): „Der unbehinderte Datenverkehr im Cyberspace entzieht sich der Territorialität des Rechts."

[285] Befürwortend dazu *Hoffmann-Riem*, in: Hoffmann-Riem, Big Data: regulative Herausforderungen, S. 11 (37); ausführlich zu den einzelnen Aspekten dieser Wirkung *Thon*, RabelsZ 2020, 24 (31 ff.).

[286] Vgl. EuGH, Rs. C-507/17 (Google/CNIL), ECLI:EU:C:2019:772 Rn. 56: „Das Internet ist nämlich ein weltweites Netz ohne Grenzen […]."

[287] Kritisch gegenüber der weltweiten Durchsetzung nationaler Gesetze am Beispiel Google etwa *Daphne Keller*, Don't Force Google to Export Other Countries' Laws, The New York Times vom 10.09.2018 (https://www.nytimes.com/2018/09/10/opinion/google-right-forgotten.html). Zuletzt abgerufen am 14.01.2022.

[288] Vgl. *Vatanparast*, ZaöRV 2020, 819 (823 f.): „The EU as a global standard setter reflects its role as a post-national liberal realist power, where it must contend with both strong states, such as China and the United States (US), and non-state actors, such as corporations involved in creating private global normative oders. Global standard setting by the EU through the GDPR and its extraterritorial provisions is one such exercise of power. […] Further, uni-

Von größerer Bedeutung ist dieses Problem zuletzt vor allen Dingen im Spannungsfeld zwischen Meinungsfreiheit und Persönlichkeitsrechten, häufig im Zusammenhang mit den Praktiken sozialer Netzwerke bei der Moderation von Nutzerinhalten (sog. *content moderation*). Hier wird gemeinhin davon ausgegangen, dass es etwa bei einer Löschverpflichtung nach deutschem NetzDG ausreicht, wenn die als rechtswidrig identifizierten Inhalte für deutsche bzw. in Deutschland befindliche Nutzer des Netzwerks nicht mehr angezeigt werden.[289] Im Rahmen des Datenschutzrechts hatte der EuGH erst kürzlich über die sehr ähnliche Frage zu entscheiden, ob Google im Rahmen der Erfüllung seiner Pflicht zum Auslisten von Suchmaschinenergebnissen nach Art. 17 Abs. 1 DSGVO (sog. Recht auf Vergessen) die Ergebnisse nur innerhalb Deutschlands, der EU oder sogar weltweit auslisten muss.[290] Der Gerichtshof folgte der Linie Googles, wonach die räumliche Reichweite einer solchen Auslistung mit Blick auf andere Staaten ohne ein solches Recht oder mit einem anders ausgestalteten[291] Recht dieser Art[292] nicht über das Hoheitsgebiet der Mitgliedstaaten hinaus gehen könne, grundsätzlich aber dieses gesamte Hoheitsgebiet und nicht bloß die jeweilige nationale Version erfasse.[293] Er legte Google gleichzeitig aber die Pflicht auf, geeignete Maßnahmen zu treffen, um zu verhindern, dass Besucher aus dem Hoheitsgebiet der Mitgliedstaaten durch Ausnutzung der regionalen Begrenzung der Auslistung Zugang zu den ausgelisteten Suchergebnissen erlangen.[294]

Bezogen auf die im vorangegangenen Abschnitt ausgeführten denkbaren Pflichten im Rahmen des Konzepts einer datenschutzrechtlichen Plattformverantwortlichkeit würde dies im Grundsatz ebenso gelten. Für auf den jeweiligen Einzelfall begrenzte Maßnahmen wie die unterschiedlich prominente Darstellung von Diensteanbietern je nach der Datenschutzfreundlichkeit ihrer Dienste wäre eine solche räumlich begrenzte Anwendung wohl auch ohne weiteres möglich. Gleiches gilt für den kompletten Ausschluss bestimmter Dienste oder

---

form global standards for data protection, like international law's universalising tendency, tend to ignore uneven development and the material and economic conditions of the third world."

[289] In der Praxis wird diese Begrenzung jedoch häufig dadurch unterlaufen, dass Netzwerkbetreiber Inhalte vorrangig auf Basis ihrer Gemeinschaftsstandards löschen, um den weitergehenden prozessualen Pflichten des NetzDG zu entgehen. In diesen Fällen erfolgt die Löschung weltweit. Vgl. *Eifert*, Evaluation des NetzDG Im Auftrag des BMJV, S. 27 ff.

[290] Siehe EuGH, Rs. C-507/17 (Google/CNIL), ECLI:EU:C:2019:772.

[291] Gemeint sind damit vor allem nationale, etwa kulturell bedingte, Unterschiede hinsichtlich der jeweiligen Bedeutung von Meinungsfreiheit und Persönlichkeitsrechten, die sich in der Ausgestaltung von Normen niederschlagen.

[292] Vgl. EuGH, Rs. C-507/17 (Google/CNIL), ECLI:EU:C:2019:772 Rn. 59.

[293] Vgl. EuGH, Rs. C-507/17 (Google/CNIL), ECLI:EU:C:2019:772 Rn. 64–66.

[294] Vgl. EuGH, Rs. C-507/17 (Google/CNIL), ECLI:EU:C:2019:772 Rn. 70. Wie weit diese Pflicht reicht und ob dadurch auch Mechanismen zur Verhinderung von bspw. durch ausländische IP-Adressen einen anderen Standort simulierenden VPNs erfasst sind, ist bis dato unklar.

das Verbot der Nutzung bestimmter Drittparteien, ggf. auch für die Einschränkung der Verarbeitungsmöglichkeiten. Bereits jetzt ist es bei Plattformen mit mehr oder weniger stark moderierten Distributionskanälen wie Apples App-Store oder Googles Play Store üblich, dass bestimmte Apps auf Basis der jeweiligen nationalen Rechtslage oder aus anderen Gründen nur regional begrenzt verfügbar sind.[295]

Schwieriger dürfte sich die Lage aber bspw. bei den auf die grundsätzliche Gestaltung der Plattforminfrastruktur gerichteten Pflichten darstellen. Hier drohen ggf. erhebliche Schwierigkeiten, großflächige Änderungen am Berechtigungsmanagement bzgl. des Zugriffs auf bestimmte Datenkategorien oder am Einwilligungsmanagement gegenüber Betroffenen auf das Hoheitsgebiet der EU zu begrenzen. Für kleinere bzw. weniger finanzstarke Plattformen kann der mit einer solchen Doppelgestaltung für unterschiedliche Jurisdiktionen einhergehende Ressourcenaufwand zudem besonders belastend sein. Als Alternative „droht" das Szenario, dass Plattformen der Einfachheit halber die europäischen Vorgaben freiwillig global umsetzen – ein aus Sicht des europäischen Datenschutzes wohl zu befürwortender Ausblick, dessen Legitimität aus völkerrechtlicher Perspektive aber zumindest zweifelhaft ist.[296] Welche der beiden Möglichkeiten realistischer ist, lässt sich kaum absehen. Auch im Zuge des Wirksamwerdens der DSGVO 2018 wurden sowohl solche Stimmen von Seiten der aus Drittstaaten stammenden Unternehmen laut, die ankündigten, das Niveau der DSGVO schlicht global anzuwenden,[297] als auch solche, die teils gesellschaftsrechtliche Umstrukturierungen vornahmen, um so die zwingend von der DSGVO betroffenen Kunden klar von den restlichen abzugrenzen[298].

Letztlich ist dies ein Problem, das nicht originär mit der Entstehung einer neuen Plattformverantwortlichkeit zusammenhängt,[299] das aber mit Blick auf

---

[295] Dies konnte zuletzt im Zusammenhang mit der Corona-Warn-App beobachtet werden. Diese war zunächst nur Nutzern mit einem deutschen Appstore- oder Play Store-Konto zugänglich. Siehe *Kim Rixecker*, Corona-Warn-App: Das Problem mit ausländischen Store-Konten, t3n.de vom 20.06.2020 (https://t3n.de/news/corona-warn-app-problem-1291972/). Zuletzt abgerufen am 14.01.2022.

[296] So auch *Hornung*, in: Roßnagel/Friedewald/Hansen, Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, S. 316 (325); *Vatanparast*, ZaöRV 2020, 819 (824).

[297] Vgl. *Thuy Ong*, Microsoft expands data privacy tools ahead of GDPR, The Verge vom 24.05.2018 (https://www.theverge.com/2018/5/24/17388206/microsoft-expand-data-privacy-tools-gdpr-eu). Zuletzt abgerufen am 14.01.2022.

[298] Vgl. *David Ingrak*, Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law, Reuters vom 19.04.2018 (https://www.reuters.com/article/us-Facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P). Zuletzt abgerufen am 14.01.2022.

[299] Siehe generell und ausführlich zur Extraterritorialität der DSGVO *Koloßa*, ZaöRV 2020, 791 (791 ff.); speziell die rechtspolitischen Auswirkungen einer solchen Wirkung in den

die Neuartigkeit der mit ihr einhergehenden Pflichten das Potential hat, verstärkt zu werden.

2. Zur Problematik der Verstärkung bestehender Machtstrukturen

Digitale Plattformen sind in vielen Fällen – man denke an die bekanntesten Beispiele um Facebook, Google, Amazon und Apple – bereits jetzt in einem solchen Ausmaß marktmächtig und monopolartig, dass neben den vorliegend den Ansatz für ihre Inpflichtnahme begründeten *Möglichkeiten* dieser Macht auch ihre negativen Seiten für etwa den freien Wettbewerb, den Verbraucherschutz oder andere Rechtsgüter und Interessen im Mittelpunkt stehen und das Zentrum von Regulierungsversuchen bilden. Dass zwangsweise von Plattformbetreibern durchgesetzte Bedingungen etwa kartell- und wettbewerbsrechtlich problematisch sein und den Unmut der einzelnen Diensteanbieter hervorrufen können, zeigte jüngst der Machtkampf zwischen Apple und Epic.[300] Auch die Bevorzugung plattformeigener Apps gegenüber denen von unabhängigen Diensteanbietern beschäftigte bereits mehrfach Behörden und Gerichte.[301] *Verpflichtet* man nun mithilfe der hier vorgeschlagenen Plattformverantwortlichkeit diese Akteure auch noch, ihre Marktmacht und ihre großflächig bedeutsamen infrastrukturellen Gestaltungsentscheidungen auszuüben, so könnte damit auch eine Gefahr einhergehen, die bereits bestehenden Machtverhältnisse weiter zu zementieren und die herausgehobene Stellung einer Plattform gegenüber der auf ihr agierenden Akteure noch weiter zu erhöhen. Plattformen könnten ihre nun gesetzlich legitimierte Macht nutzen, um Maßnahmen wie den Ausschluss von Diensteanbietern oder die Beschränkung des Zugriffs auf Nutzerdaten gezielt gegenüber unliebsamen Konkurrenten auszusprechen und sich so einen wettbewerblichen Vorteil zu verschaffen.

Hierzu ist zunächst zu konstatieren, dass die Inpflichtnahme eines Plattformbetreibers mit der Zielrichtung der gezielten Nutzung seiner Machtposition unstreitig eine Verstärkung dieser Machtposition bedeutet. Nimmt man aber mit in den Blick, dass die infragestehenden Entscheidungen bzgl. der Ausgestaltung der Plattform ebenso wie die Handlungen gegenüber auf der Plattform agierenden Akteuren und teils Konkurrenten bereits jetzt schon regelmäßig getrof-

---

Blick nehmend *Vatanparast*, ZaöRV 2020, 819 (819 ff.); siehe *Bougiakiotis*, IDPL 2020, 253 (253 ff.) für einen Vorschlag, wie eine internationale Lösung aussehen könnte.

[300] Siehe zu dem konkreten Fall *Guggenberger*, The Epic Battle for the Soul of Antitrust. Zwischenzeitlich haben sich einige Entwickler zusammengeschlossen, um eine Koalition gegen die ihrer Ansicht nach unfairen Nutzungsbedingungen zu bilden. Vgl. *Patrick McGee*, Developers form coalition to fight Apple over App Store practices, Financial Times vom 24.09.2020 (https://www.ft.com/content/516a1672-0192-47ef-8a3c-4bb5cbb25132). Zuletzt abgerufen am 14.01.2022.

[301] Siehe etwa zu der Art und Weise, wie Apple eigene Apps bevorzugt, m. w. N. *Guggenberger*, Stanford Technology Law Review, 2021, 237 (254 f.).

fen und ausgeübt werden, kann ihre Einbettung in ein regulatorisches Konzept auch als Einhegung und Kanalisierung dieser Macht verstanden werden. Wo die Handlungen die Erfüllung einer Pflicht darstellen, sind sie – eine entsprechende Gestaltung der Verantwortlichkeit vorausgesetzt – auch rechtlich angreif- und überprüfbar, steht den betroffenen Akteuren also ein (Rechts-)Weg offen, wo die Entscheidungen vorher häufig rein im Ermessen und – salopp gesagt – in der Willkür des Plattformbetreibers standen. Ist also sichergestellt, dass einerseits in die Pflicht genommene Plattformbetreiber den von ihren Maßnahmen betroffenen Diensteanbietern und ggf. auch Drittparteien ein Verfahren zur Verfügung stellen müssen, welches Dinge wie eine vorherige Anhörung und ein Widerspruchsrecht beinhaltet, und dass andererseits bei verbleibenden Differenzen der Rechtsweg offensteht, so ist zumindest einigen Bedenken abgeholfen. Das oben vorgeschlagene Konzept einer zentralen Pflicht zu datenschutzfreundlicher Ausgestaltung der Plattform wäre offen genug, um dies und zudem eine an den Plattformbetreiber gerichtete Pflicht zu beinhalten, ein systematisches Governancesystem für die Auswahl und Vorbereitung seiner Einzelfallmaßnahmen zu etablieren und dieses offen zu legen.[302] Hinzu kommt, dass das Datenschutzrecht und die Behörden und Gerichte, die es anwenden und konkretisieren, mit diesen Problemen verfestigender Marktmacht nicht zwingend allein bleiben müssten. Angrenzende Rechtsgebiete wie das Kartell- und Wettbewerbsrecht könnten insbesondere bei der Beurteilung der eben geschilderten Governancesysteme und darauf basierenden Einzelfallmaßnahmen unterstützend tätig werden.[303] Das Verfahren des BKartA gegen Facebook[304] hat erst kürzlich gezeigt, wie ein solches Zusammenspiel aussehen könnte.[305] Hier besteht möglicherweise auch Potential für aufeinander abgestimmte gesetzliche Vorgaben, durch die die rechtsgebietsübergreifenden Auswirkungen der Markt-

[302] Die grundsätzliche Sicherungswirkung eines solchen Systems betonend *Evans*, Berkeley Tech. L. J. 2012, 1201 (1246): „Nevertheless, the existence of a governance system increases the likelihood that the practice that results in exclusion is pro-competitive."

[303] Siehe *Evans*, Berkeley Tech. L. J. 2012, 1201 (1243 ff.) zu den generellen kartellrechtlichen Implikationen des Ausschlusses konkurrierender Akteure von Plattformen durch Plattformbetreiber. Auch *Hoffmann-Riem*, in: Hoffmann-Riem, Big Data: regulative Herausforderungen, S. 11 (40) konstatiert eine isoliert nur begrenzt vorhandene Befähigung des Kartellrechts zur Begrenzung der negativen Effekte großer Marktmacht auf Gemeinwohlziele und appelliert: „Die Bewältigung dieser Aufgabe erfordert ein Zusammenwirken der Instrumente des Wettbewerbsrechts mit denen des sonstigen Regulierungsrechts […]."

[304] Siehe BKartA, Beschl. v. 06.02.2019, Az. B6–22/16. Die Entscheidung wurde zwischenzeitlich zunächst im einstweiligen Rechtsschutz vom OLG Düsseldorf, Beschl. v. 26.08.2019, Az. VI-Kart 1/19 (V) ausgesetzt, um dann, abermals im einstweiligen Rechtsschutz, vom BGH, Beschl. v. 23.06.2020, Az. KVR 69/19 wieder in Kraft gesetzt zu werden.

[305] Siehe hierzu *Podszun*, GRUR 2020, 1268 (1276), der das Urteil als „ein[en] ‚test case' für die Anwendung des Kartellrechts auf die ‚Giganten des Internets'" ansieht, im Rahmen dessen „in geradezu evolutionärer Weise die Annäherung an das Problem Datenschutz und Kartellrecht" gelungen sein soll.

macht digitaler Plattformen adressiert[306] und dabei „möglichst wechselseitig optimierend eingesetzt“[307] werden.[308]

3. Zur Problematik des Verarbeitungsverhaltens der Plattformen selbst

Ein weiteres Problem ist eng mit der eben geschilderten Thematik verwandt, legt den Fokus aber stärker auf originäre Aspekte des Datenschutzes: Auch Plattformbetreiber verarbeiten eigenmächtig und zu eigenen Zwecken Daten. Das betrifft einerseits die Daten der Plattformnutzer, sowohl im Rahmen der generellen Nutzung der Plattform als auch im Rahmen der Nutzung von plattformeigenen Diensten und Apps. Andererseits haben große Plattformbetreiber eigene Dienste abseits der selbst betriebenen Plattform,[309] bieten die Integration von Plugins und SDKs in andere Dienste an[310] und betreiben große Werbenetzwerke,[311] stellen also teilweise selbst diejenigen Drittparteien in Diensten auf ihrer eigenen Plattform.[312] Insbesondere Google, Facebook und Amazon sammeln über ihre verschiedensten Angebote in solchen Ausmaßen und in einer Art und Weise, deren Rechtswidrigkeit ein offenes Geheimnis ist,[313] Nutzerdaten, dass es nicht vermessen wäre, sie als eines der drängendsten Probleme des modernen Datenschutzrechts anzusehen.

Gerade sie in die Verantwortung zu nehmen für Verarbeitungen *anderer*, meist kleiner und weniger mächtiger Akteure, scheint daher auf den ersten

---

[306] Für erste Ansätze wettbewerbsfördernder Datenschutzgesesetzgebung siehe *Westerlund/Enkvist*, jipitec 2016, 2 (15 f.), die etwa Plattformbetreiber, die Nutzerdaten zwischen ihren eigenen Diensten teilen wollen, dazu verpflichten wollen, die entsprechende API öffentlich und somit auch Konkurrenunternehmen zugänglich zu machen; jüngst erst zu diesem Thema außerdem *Blankertz*, How competition impacts data privacy; *Grewe*, Missbrauchsverbot als Durchsetzungsinstrument, S. 45 ff., 226 ff., 239 ff.

[307] *Hoffmann-Riem*, in: Hoffmann-Riem, Big Data: regulative Herausforderungen, S. 11 (73), der insbesondere die Notwendigkeit für ein „abgestimmtes Zusammenspiel von Datenschutzrecht und Wettbewerbsrecht mit spezifischem Regulierungsrecht“ herausstellt.

[308] Dieses Potential wird inzwischen auch zunehmend auch auf staatlicher und zivilgesellschaftlicher Ebene gesehen. Vgl. *Kerber/Specht-Riemenschneider*, Synergies between Data Protection and Competition Law.

[309] So bietet Google bspw. seine App Maps auch auf den Endgeräten von Apple und damit auf deren Plattform iOS an.

[310] Siehe bspw. den bereits ausführlich (in Kapitel 2 C. II. 4. b) bb)) besprochenen Fall hinter der Fashion ID-Entscheidung EuGH, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629.

[311] Vgl. *Norwegischer Verbraucherrat (Forbrukerrådet)*, Out of Control: How consumers are exploited by the online advertising industry, S. 120: „The adtech industry is packed with companies that are virtually unknown entities amongst consumers. However, by far the largest actors in the adtech industry are household names, namely Google and Facebook.“

[312] Siehe *Nieborg/Poell*, New Media & Society 2018, 4275 (4287): „Next to hosting content, platforms also provide a variety of integrated services to complementors, all of which leverage the infrastructural features – ubiquity, accessibility, reliability, invisibility – of platform technologies.“

[313] Nicht zuletzt die die Fashion ID- und Wirtschaftsakademie-Entscheidungen des EuGH fußten auf der Tatsache, dass die von Facebook im Rahmen ihrer Nutzung durch die Website- bzw. Fanpage-Betreiber verarbeiteten Daten rechtswidrig verarbeitet wurden.

Blick widersprüchlich. Es ließe sich vorwerfen, ein solcher Ansatz würde die Marktmacht dieser großen Plattformen auch insofern verfestigen, als eine effektive Verantwortlichkeit, die das Datenverarbeitungsverhalten aller anderen Akteure stärker an das bestehende Recht bindet und die Rechtsdurchsetzung diesen Akteuren gegenüber verstärkt, einen umso größeren Vorsprung des eigenen Datenverarbeitungsverhaltens bedingt, das schließlich nicht von einem größeren privaten Akteur kontrolliert wird.

Hiergegen lassen sich primär zwei Punkte vorbringen. Zwar ist zunächst zu konzedieren, dass die Inpflichtnahme derjenigen Akteure, die ihrerseits großflächig Daten in oft (vermeintlich) rechtswidriger Art und Weise verarbeiten, zur Verhinderung und Eindämmung datenschutzwidriger *anderer* Akteure zunächst paradox anmutet, weil es nichts an dem erstgenannten Missstand ändert. Doch, so lässt sich die Replik formulieren, muss dies ein solcher Ansatz auch gar nicht zwingend können. Die Probleme des Datenschutzrechts sind so vielschichtig, tiefgreifend und komplex, dass ein Konzept, das den Anspruch hätte, sie alle gleichzeitig zu beheben, von vornherein zum Scheitern verurteilt wäre. Es darf daher nicht illegitim sein, dass die Verantwortlichkeit von Plattformbetreibern ein konkretes Problem – namentlich die Kontroll- und Verantwortlichkeitsdiffusion infolge zunehmend komplexer Akteurskonstellationen bei der Verarbeitung durch Diensteanbieter und Drittparteien – behandelt, während es ein weiteres im Zusammenhang mit den in die Pflicht genommenen Akteuren nicht adressiert. Der begrenzte Ausschnitt der Gesamtproblematik, der in der vorliegenden Arbeit in den Blick genommen wird, ändert daher nichts an der weiterhin bestehenden Herausforderung, das bestehende Datenschutzrecht besser gegenüber großen digitalen Plattformen bei deren Verarbeitung und Ansammlung personenbezogener Daten durchzusetzen.

Darüber hinaus ist schon die Annahme, die hier propagierte Verantwortlichkeit eines Plattformbetreibers würde dessen eigenes Verarbeitungsverhalten nicht adressieren, nur auf den ersten Blick korrekt. Das bereits geschilderte breite Spektrum an Diensten, über die große Plattformbetreiber Daten verarbeiten, führt dazu, dass insbesondere die einbezogenen Drittparteien in Diensten auf einer Plattform ebenfalls zum Plattformbetreiber gehören. Als gutes Beispiel für eine solche Personenidentität lässt sich Google anführen, das als gleichzeitig entscheidender Akteur hinter der Plattform Android einerseits und den in viele Android-Apps einbezogenen Werbenetzwerken Adsense und Doubleclick andererseits agiert.[314] Derartige Fälle können also dazu führen, dass die in die Pflicht genommenen Plattformbetreiber dazu verpflichtet werden, das Daten-

[314] Siehe *Norwegischer Verbraucherrat (Forbrukerrådet)*, Out of Control: How consumers are exploited by the online advertising industry, S. 120: „In the technical testing, all of the apps except Clue and Grindr were observed interacting with Google's advertising service DoubleClick. […] it can be difficult to know where Google as a service-provider ends and where Google as an advertising service begins."

verarbeitungsverhalten ihrer eigenen Dienste zu limitieren und kontrollieren. Möglicherweise könnte ein solcher Ansatz also mittelbar sogar dazu beitragen, auch dieses Problem in Teilen zu adressieren. Dafür wäre es nötig, durch entsprechende Offenlegungspflichten im Austausch mit den Aufsichtsbehörden sicherzustellen, dass etwa die gewählten Gestaltungsentscheidungen für Schnittstellen unterschiedslos für alle Diensteanbieter und Drittparteien gelten und keine Ausnahmen für plattformeigene Dienste gemacht werden. Jedenfalls die global auf der jeweiligen Plattform wirkenden Entscheidungen bzgl. datenschutzfreundlicher Ausgestaltung der Infrastruktur würden sich dann gleichermaßen zulasten der Plattformbetreiber und zulasten der anderen Akteure auswirken.

Die weiterhin bestehende Problematik des eigenen Datenverarbeitungsverhaltens der in die Pflicht genommenen Plattformbetreiber vermag daher nicht, als Argument gegen ihre Verantwortlichkeit durchzuschlagen.

4. Zur Problematik der Privatisierung der Rechtsdurchsetzung

Zuletzt soll ein weiter Einwand untersucht werden, der ebenfalls eng mit den beiden zuletzt diskutierten Problemen zusammenhängt. Im Rahmen der Erörterung der konkreten Pflichten wurde bereits mehrfach angesprochen, dass Plattformbetreiber in mancherlei Hinsicht als „verlängerter Arm" der Aufsichtsbehörden agieren könnten, weil sie in der Lage sind, in weitaus effizienterer Art und Weise Datenschutzverstöße zu erkennen und zu ergreifende Gegenmaßnahmen durchzusetzen sowie grundsätzlich Fehlverhalten zu verhindern bzw. von seiner Durchführung abzuhalten. Die Kehrseite dieser Medaille ist eine Abkehr der traditionell und aus guten Gründen dem Staat zustehenden Rechtsdurchsetzung[315] hin zu privaten Akteuren. Weil mit einer solchen Verschiebung diverse Gefahren einhergehen – es sei hier beispielhaft auf die Schwierigkeit der Entscheidung komplexer Rechtsfragen und auf die ggf. fehlenden Rechtsschutzmöglichkeiten der betroffenen Akteure hingewiesen –, steht dieser Trend, der in viele Bereiche des digitalen Raumes Einzug erhalten hat, teils stark in der Kritik. Insbesondere im Bereich der Intermediärshaftung und speziell im Zusammenhang mit der Moderation von Meinungsinhalten, wie sie etwa das NetzDG von sozialen Netzwerken verlangt, aber auch in anderen Bereichen wie dem des Urheberrechts,[316] wird dieser Trend zum allergrößten Teil sehr kritisch gesehen. Zentrales Argument dabei ist die grundlegende Schwierigkeit der

[315] Zur generellen Tendenz der zunehmenden Privatisierung des Rechts (und nicht nur der Rechtsdurchsetzung) im digitalen Raum siehe *Wernicke/Mehmel*, ZEuP 2020, 1 (1 ff.).

[316] Hier betrifft die Kritik vor allem die Fehleranfällig und fehlende Fähigkeit zur kontextualen Einordnung von technischen Erkennungssystemen wie Upload-Filtern, siehe *Raue/Steinebach*, ZUM 2020, 355 (358 ff.). *Hofmann*, GRUR 2018, 21 (21 ff.); *Spindler*, CR 2019, 277 (277 ff.); zu den weiteren technischen Möglichkeiten neben Upload-Filtern siehe *Specht*, GRUR 2019, 253 (255 ff.).

diffizilen und stark einzel- und kontextabhängigen Abwägung[317] zwischen der Meinungs- und ggf. Kunstfreiheit der sich äußernden Nutzer auf der einen und den Persönlichkeitsrechten der betroffenen Nutzer auf der anderen Seite.[318] Die Deutungshoheit darüber, welche Inhalte noch rechtmäßig und welche bereits rechtswidrig und daher vom Netzwerkbetreiber zu löschen sind, komme, so die Kritik, mangels gerichtlicher Überprüfung so letztlich den Netzwerkbetreibern zu, was der in einer Demokratie besonders hohen Bedeutung der Meinungsfreiheit nicht gerecht werde.[319] Je nach Ausgestaltung einer solchen Handlungsverpflichtung käme zudem das Problem hinzu, Netzwerkbetreiber könnten aus Angst vor der drohenden eigenen Haftung in Zweifelsfällen vorsichtshalber und damit vorschnell zum Ergebnis der Rechtswidrigkeit kommen und so auch viele eigentlich rechtmäßige Inhalte löschen (sog. *overblocking*).[320] Im schlimmsten Fall könne diese Tendenz zu einer Entwicklung hin zu automatisierten und unmittelbar bei oder kurz nach Erstellung des betreffenden Inhalts ansetzenden Überprüfungen führen und so eine Art „private Zensur" mit sich bringen.[321]

Eine abschließende Erörterung dieser sehr grundsätzlichen Debatte kann und soll im Rahmen dieser Arbeit nicht erfolgen. Einige dieser Einwände und Befürchtungen lassen sich jedoch legitimerweise auch auf das Datenschutzrecht und die Anwendung des hier vorgeschlagenen Konzepts der Plattformverantwortlichkeit übertragen. Wie bereits mehrfach angesprochen, belasten die im Rahmen ihrer Verantwortlichkeit ergriffenen Maßnahmen von Plattformbetreibern die Daten verarbeitenden Diensteanbieter und Drittparteien, die so in ihrer Freiheit eingeschränkt werden. Wo bisher solche Einschränkungen nur eigenmächtig im Rahmen der Befolgung eigener Pflichten oder im Einzelfall auf An-

---

317 Vgl. etwa *Kuczerawy*, CLSR 2015, 46 (48): „[…] private companies might not have enough legal knowledge to assess the (il)legality of third party content. This is particularly the case if the content is not manifestly illegal, which may occur where the subjective rights of individuals are at stake." Etwas differenzierender *Lüdemann*, in: Eifert/Gostomzyk, Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, S. 153 (160 f.), der Netzwerkbetreibern diese Fähigkeit nicht prinzipiell absprechen will, die dafür notwendigen Anreize zur Vornahme umfassender Abwägungen aber im Falle NetzDG als nicht gegeben ansieht.

318 Ausführlich zu diesem Spannungsfeld *Lang*, AöR 2018, 220 (220 ff.). In Betracht kommen im Rahmen des NetzDG zudem ähnlich schwer zu beurteilende Delikte wie Volksverhetzung gem. § 130 StGB, vgl. § 1 Abs. 3 NetzDG.

319 So etwa *Lüdemann*, in: Eifert/Gostomzyk, Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, S. 153 (158), der im Zusammenhang mit den Anreizstrukturen des NetzDG auf „den verfassungsrechtlich geschützten gesellschaftlichen Meinungsbildungsprozess, der sich nicht in der schlichten Addition individueller Grundrechtspositionen erschöpft", verweist. Ebenso *Hong*, Das NetzDG und die Vermutung für die Freiheit der Rede: „Das Netzwerkdurchsetzungsgesetz (NetzDG) verstößt gegen die grundrechtliche Vermutung für die Freiheit der Rede."

320 Siehe *Kuczerawy*, CLSR 2015, 46 (48) zu der Rolle der pflichtigen Intermediäre: „This basically makes them a judge in their own cause." Vgl. auch *Lang*, AöR 2018, 220 (232 ff.).

321 Vgl. *Kreimer*, Univ. Pa. Law Rev. 2006, 11 (41 ff.).

raten oder Anweisung von Aufsichtsbehörden vorgenommen wurden, würden sie nun durch das Verhalten anderer privater Akteure hervorgerufen, sodass die Durchsetzung des Rechts sich in Teilen weg von staatlichen Behörden und hin zu Plattformbetreibern bewegt.

Dennoch bestehen große strukturelle Unterschiede zwischen den beiden Herangehensweisen. Wo bei der klassischen Intermediärshaftung und insbesondere im Bereich des NetzDG unmittelbar die Prüfung eines Tatbestands – etwa einer Strafnorm oder einer urheberrechtlichen Schutznorm – dem privaten Akteur übertragen wird, steht hier in erster Linie die strukturelle und prozessuale Absicherung, Überprüfung und Verstärkung dessen im Vordergrund, dass die von der privaten Rechtsdurchsetzung belasteten Akteure überhaupt Maßnahmen ergreifen und Verfahren etablieren. Wenn etwa der Plattformbetreiber sicherstellt, dass nur Dienste aufgenommen werden, die eine deutschsprachige und vollständige Datenschutzerklärung vorweisen können und in den Distributionskanal aufnehmen lassen, oder wenn das Einwilligungsmanagement absichert, dass die Frage nach der Einwilligung in den Abruf bestimmter Datenkategorien in regelmäßigen Abständen erneut gestellt wird, um dem Nutzer seine Widerrufsmöglichkeit[322] vor Augen zu führen, so hat diese Art der Durchsetzung eine gänzlich andere, weit weniger invasive Qualität als die Löschung einer Meinungsäußerung. Dass ein solcher Ansatz der Verlagerung auf andere private Akteure dem Datenschutzrecht nicht völlig fremd ist, zeigt einerseits der Entwurfsprozess der zukünftigen ePrivacy-VO, innerhalb dessen unterschiedliche Arten von Pflichten für die Entwickler von Software wie Internetbrowsern vorgesehen waren, die zwischenzeitlich die Form von Gestaltungspflichten à la *privacy by design* hatten, derzeit jedoch nur noch zur Bereitstellung bestimmter leicht erkennbarer und verständlicher Einstellungen des Privatsphäreverhaltens der jeweiligen Software verpflichten.[323] Auch die im Google Spain-Urteil des EuGH etablierten Pflichten zur Löschung und Überwachung sind ein, wenngleich weniger offensichtliches, Beispiel der Nutzbarmachung der Handlungsmöglichkeiten privater Akteure.[324]

Der Vorteil des hier vorgeschlagenen komplexen Systems einer Verantwortlichkeit gegenüber eines reinen Haftungsregimes besteht also gerade darin, dass breit gefasste vorgelagerte Ausgestaltungspflichten im Mittelpunkt stehen und konkrete Einzelmaßnahmen gegenüber konkreten Akteuren die Ausnahme darstellen. Durch die bei solchen Gestaltungsmaßnahmen weniger grassierende Zeitknappheit ist ein größerer Austausch mit Aufsichtsbehörden möglich, sodass grobe Fehleinschätzungen unwahrscheinlicher werden. Das stärker

---

[322] Vgl. hierzu *Ernst*, ZD 2020, 383 (383 ff.).

[323] Siehe *Art. 29-Datenschutzgruppe*, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), S. 17 f. für eine Bestandsaufnahme mit weiteren Empfehlungen.

[324] Siehe ausführlich zu diesen Pflichten *Keller*, Berkeley Tech. L. J. 2018, 287 (289 ff.).

auf einen solchen Austausch zwischen Verantwortlichen und Aufsichtsbehörden ausgerichtete Anreizsystem der DSGVO mit den abgestuften Behördenmaßnahmen läuft nicht in Gefahr, den Fehler der pauschalen Löschanreize zu machen, der dem NetzDG mitunter vorgeworfen wird.[325] Da es zudem meist nicht um konkrete Fragen der Datenschutzwidrigkeit einzelner Maßnahmen geht, geht es hier weniger um die Deutungshoheit darüber, was rechtswidrig ist und was nicht, sondern schlicht um die infrastrukturelle Absicherung derjenigen Vorgaben, die die anderen Akteure sowieso bereits treffen. Wo es im Einzelfall doch um konkrete Maßnahmen gegen andere Verantwortliche geht, sollte das Konzept der Plattformverantwortlichkeit in der Lage sein, den betroffenen Akteuren verfahrensrechtliche Absicherungen zu geben, um ein Mindestmaß an rechtstaatlichen Garantien, wie vorherige Anhörungen und Widerspruchsmöglichkeiten sowie notfalls den Rechtsweg, zu wahren.[326] Derartige Kontrollmechanismen werden auch in der generellen Diskussion bereits vielfach erörtert.[327] Vieles hängt hier von der konkreten Pflichtengestaltung ab. Die unter III. getätigten Vorschläge sind dafür wie erwähnt nur ein erster Gedankenanstoß. Zuletzt darf auch nicht vergessen werden, dass die das Spannungsfeld zwischen Meinungsfreiheit und Persönlichkeitsrechten auszeichnende Komplexität und Sensibilität vom (einfachgesetzlichen) Datenschutzrecht bei all seiner Bedeutsamkeit meist nicht erreicht wird. Auch hier drohen zwar Interessenkonflikte und Abwägungsentscheidungen, allerdings weder in der Häufigkeit noch in der Intensität wie etwa bei Äußerungen auf sozialen Netzwerken. Nicht zuletzt darf nicht vergessen werden, dass Plattformbetreiber schon jetzt Entscheidungen mit entsprechender Wirkung treffen,[328] sodass eine geregelte Inpflicht-

---

[325] Vgl. zu diesem Vorwurf gegenüber dem NetzDG, wonach dessen Anreizstrukturen Netzwerkbetreiber in erster Linie den einfachsten Weg zur Vermeidung von Bußgeldern suchen lässt *Lüdemann*, in: Eifert/Gostomzyk, Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, S. 153 (161 f.): „Ein bloßes Bußgeldvermeidungsverhalten der Unternehmen ist – im Unterschied zu anderen Bereichen, in denen man mit dem Recht der Ordnungswidrigkeiten menschliches Verhalten vergleichsweise gut beeinflussen kann – beim Netzwerkdurchsetzung[sgesetz] aber fraglos ein deutliches Minus gegenüber einem möglichst sensiblen Löschungsmanagement von Kommunikationsinhalten." Siehe außerdem *Lang*, AöR 2018, 220 (232 ff.).

[326] So auch *Hofmann*, ZUM 2017, 102 (108), der gegen die Kritik privater Rechtsdurchsetzung einwendet: „Zwar ist es richtig, dass Intermediäre einen Streit zwischen Dritten moderieren. Durch ihre eigenen Pflichten sind sie jedoch auch selbst mit ihren Rechten betroffen. […] Messlatte ist vielmehr, ob zentrale Verfahrensstandards gewahrt sind." Siehe auch *Lang*, AöR 2018, 220 (245 ff.).

[327] Siehe etwa *Perel*, Berkeley Tech. L. J. 2020, 1 (42 ff.); vgl. zudem die Ausführungen von *Keller*, Berkeley Tech. L. J. 2018, 287 (361 ff.) zu den *notice and takedown*-Pflichten von Google im Zusammenhang mit dem Recht auf Vergessenwerden.

[328] Vgl. *Greene/Shilton*, New Media & Society 2018, 1640 (1657): „Mobile platforms are not just passive intermediaries supporting other technologies. Rather, platforms govern design by promoting particular ways of doing privacy, training devs on those practices, and (to varying degree) rewarding or punishing them based on their performance."

nahme hier nur zu einem „Mehr“ an prozessualer Absicherung und Beachtung rechtsstaatlicher Standards führen kann.

Auch diese Problematik vermag daher nicht grundlegend gegen die Konzeptionalisierung einer datenschutzrechtlichen Plattformverantwortlichkeit zu sprechen.

V. Zwischenergebnis

Die Schaffung einer neuen Verantwortlichkeitsfigur für die Betreiber digitaler Plattformen kann nach alledem ein tragfähiger Weg dafür sein, der Akteurspluralität und den mit ihr einhergehenden Komplexitäten entgegenzuwirken. Ihr großer Vorteil gegenüber einer Subsumtion unter die erweiterte Figur der gemeinsamen Verantwortlichkeit liegt in der Schaffung neuer, speziell auf die Möglichkeiten und Bedürfnisse dieser Akteursgruppe zugeschnittenen Pflichten, aber auch in der Entlastung des sowieso schon von einem (zu) breiten Anwendungsbereich und damit ungemein heterogenen Erwartungen geplagten gemeinsamen Verantwortlichkeit (I.). Der Anwendungsbereich dieser neuen Verantwortlichkeit sollte sich an der im Rahmen dieser Arbeit verwendeten Definition digitaler Plattformen orientieren.[329] Eine weitergehende Einschränkung mittels einer Bagatellgrenze wäre in Teilen möglich, bei adäquater Ausgestaltung eines Pflichtenkatalogs, der sich flexibel den tatsächlichen Fähigkeiten und Limitierungen eines jeweiligen Plattformverantwortlichen anpasst, aber nicht zwingend nötig (II.). Ein Ansatz dafür könnte eine Mischung aus proaktiven und reaktiven Pflichten sein, die in großen Teilen einzelne ergebnisoffene und stark prozessorientierte Pflichten der DSGVO aufgreift und durch neue Pflichten ergänzt. Bei entsprechender Ausgestaltung könnte dies ein vielversprechender Ansatz sein, der sicherlich nicht frei von Limitierungen und Problemstellen wäre, sich aber nicht mit unüberwindbaren Hindernissen konfrontiert sähe (III. und IV.).

Die hier präsentierten Überlegungen zu der konkreten Konzeption dieser Pflichten soll dabei nur ein erster Denkanstoß sein und Ansätze dafür geben, wie die Fähigkeiten und Verhaltensweisen von Plattformbetreibern sinnvoll im Interesse eines starken Datenschutzes utilisiert werden können. Der Fokus liegt hier insgesamt darauf, die oben identifizierten Defizite des klassischen Verantwortlichkeitskonzepts zumindest punktuell zu kompensieren. Die eben geschilderten Pflichten zeigen, wie hier bspw. die im Zuge der stetig wachsenden Bedeutung von Plattformen als digitale Räume, in denen Dienste und Apps angesiedelt sind, entstandenen Kontroll- und Transparenzdefizite der betroffenen Diensteanbieter abgemildert werden könnten. Gleiches gilt für die Rolle der

[329] Vgl. *Tiwana* u. a., Information Systems Research 2010, 675 (676) sowie die Ausführungen in Kapitel 1 A. I.

Betroffenen, deren vorausgesetzte Fähigkeit, selbstbestimmt und bewusst mit den ihnen zur Verfügung gestellten Instrumenten zum Selbstdatenschutz umzugehen, durch die Komplexität an Akteuren und die Diffusion der jeweiligen Beiträge in (noch) stärkere Mitleidenschaft gezogen wird, als dies schon seit jeher der Fall war. Durch die (im Rahmen der unterschiedlichen Pflichtenreichweiten) gleichmäßige Inanspruchnahme aller Plattformbetreiber würde zudem ein *level playing field* in Form eines vergleichbaren Datenschutzniveaus geschaffen. So könnte verhindert werden, dass das (grundsätzlich begrüßenswerte) „Vorpreschen" einzelner Akteure wie Apple datenschutzfreundliche Plattformen zu einem Luxusgut macht. Datenschutz als Wettbewerbsvorteil bietet gesellschaftlich nur dann einen Mehrwert, wenn ein Mindestniveau normativ abgesichert und garantiert ist.[330]

Um aus diesen ersten Vorüberlegungen ein in sich schlüssiges und tragfähiges Konzept zu schaffen, bedarf es weiter- und tiefgehender Überlegungen, die über den juristischen Tellerrand hinaus zwingend interdisziplinär ausgerichtet sein und so Erkenntnisse etwa aus dem Bereich der (Wirtschafts-)Informatik berücksichtigen und einfließen lassen sollten. Hierfür könnte insbesondere das Konzept der *boundary resources* von Nutzen sein, das gute Einblicke über die Dynamiken zwischen Plattformbetreibern und Diensteanbietern hinsichtlich des Zustandekommens und Revidierens von Gestaltungsentscheidungen liefert.[331] Darüber hinaus bietet die reichhaltige computerwissenschaftliche Literatur[332] zu der Entwicklung von datenschutzrelevanten Ausgestaltungsentscheidungen von Plattformbetreibern, aber auch zu noch immer bestehenden Lücken und Limitierungen, einen guten Fundus, der zeigt, welche konkreten Handlungen erwartet werden können und in welchem Ausmaß hier noch Optimierungsbedarf besteht.

Im diesem Zusammenhang besteht großes Potential für die Konturierung der bewusst ergebnisoffen gehaltenen Pflichten wie der zu *privacy by design* gem. Art. 25 Abs. 1 DSGVO, aber auch für die Notwendigkeit von Verfahrenspflichten, die die durchgehende Beteiligung von Diensteanbietern sicherstellen und so die Findung innovativer Lösungsansätze begünstigen und gleichzeitig die In-

---

330 So auch der treffende Kommentar von *Simon Hurtz*, Privatsphäre darf kein Luxusgut sein, SZ vom 28.12.2020 (https://www.sueddeutsche.de/digital/apple-facebook-iphone-tracking-1.5159538) zu der Diskrepanz zwischen den zunehmend datenschutzfreundlichen Vorkehrungen von iOS und dem fehlenden Pendant auf Seiten Androids. Zuletzt abgerufen am 14.01.2022.

331 Hierzu die ausführliche Betrachtung *supra* in Kapitel 1 B. II.

332 Siehe etwa speziell zu mobilen Plattformen *Alepis/Patsakis*, in: Ali/Danger/Eisenbarth, Security, Privacy, and Applied Cryptography Engineering, S. 53 (53 ff.); *Bartel* u. a., Automatically securing permission-based software by reducing the attack surface, S. 274 ff.; *Balebako* u. a., Little brothers watching you, S. 1 ff.; *Dimitriadis* u. a., Malevolent app pairs, S. 431 ff.; *Enck* u. a., ACM Trans. Comput. Syst. 2014, 1 (1 ff.); *Struse* u. a., in: Paternò/de Ruyter/Markopoulos/Santoro/van Loenen/Luyten, Ambient Intelligence: Proceedings of the Third International Joint Conference, Aml 2012, Pisa, Italy, November 13–15, 2012, S. 65 (65 ff.).

teressen der von einer Verantwortlichkeit für Plattformbetreiber mittelbar ebenfalls stark belasteten Diensteanbieter absichern könnten.

E. Ergebnis

In diesem Kapitel wurden die in Kapitel 1 und 2 gewonnenen Erkenntnisse über die moderne Verarbeitungsrealität im digitalen Raum einerseits und die Grundkonzeption der datenschutzrechtlichen Verantwortlichkeit mitsamt ihrer Bedeutung für das Datenschutzrecht andererseits zusammengeführt, um einen Abgleich vorzunehmen, der die Funktionsfähigkeit der Zweitgenannten unter den Bedingungen der Erstgenannten ermittelt. Als Ergebnis wurde zunächst eine Dysfunktionalität aufgedeckt (A.) und sodann hergeleitet, weshalb aufgrund der Art und Weise der Dysfunktionalität und in Fortführung der vom EuGH begonnenen Entwicklungslinie eine Ausweitung der datenschutzrechtlichen Verantwortlichkeit ein gangbarer Weg zur teilweisen Behebung der aufgedeckten Defizite sein könnte (B.). Dafür wurden zwei verschiedene Ansätze präsentiert, die zeigen, wie in unterschiedlicher Weise eine jeweilige Verantwortlichkeit der Akteursgruppen der Diensteanbieter (C.) und Plattformbetreiber (D.) aussehen könnte.

Kapitel 4

Fazit und Ausblick

Ziel dieser Arbeit war es, das europäische Datenschutzrecht in Form der DSGVO und insbesondere das ihr zugrundeliegende Verantwortlichkeitskonzept zu analysieren und auf seine Wirksamkeit in Zeiten stark veränderter Verarbeitungskonstellation hin zu untersuchen und Vorschläge für mögliche Weiterentwicklungsansätze zu machen. Dazu wurde in separaten Kapiteln zunächst die moderne Verarbeitungsrealität im Zusammenhang mit digitalen Diensten im weiteren Sinne beleuchtet und hinsichtlich der typischen Akteursgruppen systematisiert (Kapitel 1) und sodann das Datenschutzrecht, angefangen mit seinen unionsgrundrechtlichen Wurzeln und bis hin zu seinem Verantwortlichkeitskonzept und seinen Prämissen, in seine Einzelteile zerlegt und betrachtet (Kapitel 2). Daran anschließend wurde auf Basis dieser Erkenntnisse aufgezeigt, an welchen Stellen Defizite des tradierten Verantwortlichkeitskonzepts bestehen und wurden für konkrete Akteursgruppen konkrete Vorschläge hinsichtlich einer ausgeweiteten und teils neuen Verantwortlichkeit gemacht (Kapitel 3).

Im Folgenden sollen die einzelnen Erkenntnisse zusammengefasst und soll im Anschluss ein Ausblick gegeben werden.

A. Die einzelnen Akteursgruppen und die Diffusion von Kontrolle

Besucht ein Nutzer im Internet eine Website, nutzt eine App oder macht ganz allgemein Gebrauch von einem Dienst, so interagiert er unmittelbar mit dem *Diensteanbieter*. Im Rahmen dieser Nutzung werden heutzutage bei nahezu jedem Dienst personenbezogene Daten mit Bezug zum konkreten Nutzer verarbeitet. Die zunächst sehr bilaterale Beziehung zwischen Nutzer und Diensteanbieter deckt das Spektrum der beteiligten Akteure aber nur sehr unzureichend ab. In derselben Regelmäßigkeit, in der Daten verarbeitet werden, sind daran auch andere Akteure beteiligt, die als *Drittparteien* in einen Dienst einbezogen werden, um Aufgaben für den Diensteanbieter zu erbringen oder Teile des Dienstes bereitzustellen, aber auch eigene Zwecke zu verfolgen. Gleichzeitig bedingt es die moderne Plattformökonomie, dass viele Dienste nicht alleinstehend im Netz zu finden sind, sondern auf Plattformen angesiedelt sind, die den Zugang zu einer großen Nutzergruppe vermitteln, Instrumente und Unterstützung zur Entwicklung von Diensten anbieten und die Abwicklung von Auf-

gaben wie Distribution, Werbung und Zahlungen übernehmen und so den digitalen Raum und die Infrastruktur anbieten, die zum Angebot eines Dienstes notwendig sind. *Plattformbetreiber* stellen also eine dritte zu betrachtende Akteursgruppe dar.[1]

Durch diese Verteilung von Aufgaben und Beteiligungen verteilt sich auch die Kontrolle über die Verarbeitung von Nutzerdaten, die in einem rein bilateralen Verhältnis nur beim Diensteanbieter läge. Hier bedingt es die technische Art und Weise des Einbezugs von Drittparteien, dass ein großer Teil an Kontrolle und Transparenz an diese abgegeben wird. Gleichzeitig liegt die Kontrolle über die Verarbeitungsumgebung inklusive der Schnittstellen für den Zugriff auf Nutzerdaten beim jeweiligen Plattformbetreiber, sodass in der Person des Diensteanbieters insgesamt ein gewisser Kontrollverlust zu konstatieren ist. Das größte Ausmaß an Kontrolle im Rahmen der Konstellation dieser drei Akteursgruppen liegt beim Plattformbetreiber, dessen Entscheidungen global auf seiner Plattform wirken und damit Möglichkeitsräume für die beiden anderen Akteure begrenzen oder erweitern und der insofern eine herausgehobene Stellung innehat.[2]

B. Die Grundprämissen der Verantwortlichkeit

Unter Berücksichtigung der verschiedenen Regulierungsinstrumente, die die DSGVO im Pflichtenkatalog der datenschutzrechtlichen Verantwortlichkeit verankert hat, lassen sich drei *Grundprämissen* aufdecken, von deren dauerhaften Vorliegen der Verordnungsgeber ausging und die daher grundsätzlich vorliegen müssen, damit das Verantwortlichkeitskonzept seine beabsichtige Wirkung entfaltet. Damit ist gemeint, dass die von der DSGVO formulierten Tatbestandsmerkmale in Form ihrer jeweiligen Auslegung stets die Akteure in die Pflicht nehmen müssen, in deren Person sich die folgenden Prämissen erfüllen.

Die erste Grundprämisse ist die des Verantwortlichen als zentrale, alle Umstände der Verarbeitung kennende und kontrollierende Figur.[3]

Die zweite Grundprämisse ist die des Verantwortlichen als nach außen hin zu jeder Zeit klar erkennbare und erreichbare Person.[4]

Die dritte Grundprämisse ist die des Verantwortlichen als sich seiner Rolle zu jeder Zeit und insbesondere schon bei Konzeption und Vorbereitung konkreter Verarbeitungsvorgänge bewussten Person.[5]

---

[1] Siehe *supra* bei Kapitel 1 A.
[2] Siehe *supra* bei Kapitel 1 B.
[3] Siehe *supra* bei Kapitel 2 B. II. 1.
[4] Siehe *supra* bei Kapitel 2 B. II. 2.
[5] Siehe *supra* bei Kapitel 2 B. II. 3.

C. Wirksamkeit als Ideal des europäischen Datenschutzes

Grund für die herausgehobene Bedeutung dieser Prämissen und ihres Vorliegens ist, dass die grundlegende Wirksamkeit des Verantwortlichkeitskonzepts enorme Bedeutung für die Funktionsweise des Datenschutzes insgesamt hat.[6] Diese Notwendigkeit eines wirksamen Gesamtkonzepts ergibt sich in sehr begrenztem Maße aus den unionsgrundrechtlichen Vorprägungen der DSGVO, wenn eine drohende Unwirksamkeit besonders tiefgreifend ist und die Geeignetheit des Gesetzes als solche in Zweifel stellt[7] oder dazu führt, dass in besonders grundrechtssensiblen und gefährlichen Bereichen kein Schutz mehr besteht[8]. In den meisten Fällen ergibt sich eine Wirksamkeitsvorgabe insofern nur mittelbar aus Unionsgrundrechten, als den Verordnungsgeber hier Sekundärpflichten zur Etablierung entsprechender prozeduraler Absicherungen treffen, um mögliche Wirksamkeitsdefizite frühzeitig zu erkennen. Die DSGVO verschreibt sich selbst daher in ihrem Art. 97 ebenso einer regelmäßigen Überprüfung (unter anderem) ihrer Wirksamkeit, ebenso wie die EU insgesamt mit ihrer Better Regulation Agenda sich selbst zum Erlass und zur Beibehaltung wirksamer, effizienter und kohärenter Rechtsakte verpflichtet.[9]

D. Die Dysfunktionalität der Verantwortlichkeit

Die in Kapitel 1 geschilderte Akteurspluralität mit ihrer Diffusion von Kontrolle und Einflussmöglichkeiten führt zu einer Dysfunktionalität des Verantwortlichkeitskonzepts der DSGVO auf verschiedenen Ebenen. Keine der drei Akteursgruppen kann allein die an die Rolle des Verantwortlichen gestellten Erwartungen erfüllen, was sich mittelbar auch auf die Erwartungen auswirkt, die an Betroffene und Aufsichtsbehörden als zur Kontrolle und Überwachung bzw. insgesamt zur Rechtsdurchsetzung aufgeforderte Akteure gestellt sind. So führen sich Defizite auf Ebene der einzelnen Verantwortlichen bzw. bisher nicht als Verantwortliche identifizierten Akteure kaskadenartig auf weiteren Ebenen fort und machen die Verantwortlichkeit insgesamt zu einem dysfunktionalen Konzept.[10]

---

[6] Siehe *supra* bei Kapitel 2 B. I und II.
[7] Siehe *supra* bei Kapitel 2 B. III. 1.
[8] Siehe *supra* bei Kapitel 2 B. III. 2.
[9] Siehe *supra* bei Kapitel 2 B. III. 3.
[10] Siehe *supra* bei Kapitel 3. A.

E. Zwei Ansätze der Weiterentwicklung

Ein denkbarer Lösungsansatz für diese Dysfunktionalität ist die Ausweitung der Verantwortlichkeit, also die Veränderung der Kriterien dessen, *wer* als Verantwortlicher in Betracht kommt, in der Hoffnung, so wieder einen Gleichlauf zwischen Grundprämissen und Realwelt herzustellen. Hierzu kommen im Rahmen der bereits identifizierten Akteursgruppen Diensteanbieter in Bezug auf die durch Drittparteien durchgeführten Verarbeitungen sowie Plattformbetreiber in Bezug auf die Ausgestaltung ihrer verarbeitungsermöglichenden Plattforminfrastruktur und -bedingungen in Betracht.[11] Der hier gewählte Ansatz ist dabei ein zweigeteilter. Einerseits wird vorgeschlagen, Diensteanbieter in modifizierter Fortführung der neueren EuGH-Rechtsprechung als sekundäre gemeinsame Verantwortliche einzustufen und so einem abgeschwächten und passgenaueren Pflichtenkatalog zu unterwerfen.[12] Andererseits wird der Vorschlag der Konzeption einer neuen genuinen Plattformverantwortlichkeit gemacht, die sich stärker vom klassischen Modell einer Verantwortlichkeit für konkrete Akte von Datenverarbeitungen entfernt und stattdessen die Gestaltung der eigenen Plattform und die Kooperation mit den auf ihr aktiven Akteuren in den Mittelpunkt stellt.[13]

F. Interdisziplinäre Erkenntnisse und ihr Mehrwert für das Recht

Die hier unterbreiteten Vorschläge für die Weiterentwicklung der gemeinsamen Verantwortlichkeit (in Form sekundärer und primärer Verantwortlicher) einerseits und die Schaffung einer neu auszugestaltenden Plattformverantwortlichkeit andererseits bieten nach der Vorstellung des Verfassers vielversprechende Möglichkeiten zur teilweisen Bewältigung der Defizite der datenschutzrechtlichen Verantwortlichkeit, die sich durch die moderne Verarbeitungsrealität im digitalen Raum gebildet haben. Gleichzeitig ist einzuräumen, dass beide Ansätze auf unterschiedlichen Ebenen von unbestimmten Rechtsbegriffen und Generalklauseln leben, deren konkrete Ausfüllung im Einzelfall in Form von Wertungsentscheidungen noch zu leisten sein wird. Dies betrifft für die gemeinsame Verantwortlichkeit etwa die Frage, wann genau ein Akteur bloß sekundärer und wann er gleichgestellter primärer gemeinsamer Verantwortlicher ist.[14]

---

[11] Siehe *supra* bei Kapitel 3 B.

[12] Siehe *supra* bei Kapitel 3 C.

[13] Siehe *supra* bei Kapitel 3 D.

[14] Vgl. die Ausführungen bei Kapitel 3 C. III. Für die Plattformverantwortlichkeit wurde für diese Frage der Abgrenzung tauglicher Verantwortlicher bewusst ein sehr weiter Kreis gezogen und die weitere Eingrenzung auf die Ebene der Pflichtenreichweite und -verteilung verlagert.

Für beide Ansätze betrifft es zudem in großem Maße die Frage, wie weit die generalklauselartigen Sorgfalts-, Auswahl- und Überwachungspflichten[15] reichen. Hinter der Ausfüllung dieser Generalklauseln in „zur Anwendung fähige Normen“[16] verbirgt sich die Findung wertungsabhängiger Grenzen dafür, welche Handlungen den Verantwortlichen als bloß mittelbar zu Datenverarbeitungen Anderer beitragenden Akteuren zumutbar sind. Eng damit verknüpft ist die Frage, wie sich diese Handlungen in der Praxis tatsächlich auswirken und welche Effekte sie für die weiteren betroffenen Akteure zeitigen.

Bei der Beantwortung dieser Fragen stößt die Rechtswissenschaft aber an ihre Grenzen[17] und benötigt sie zusätzliche Erkenntnisse aus fachfremden Disziplinen der jeweiligen Regelungsmaterie. Zwar kann hier der Rückgriff auf grundrechtliche Vorgaben und Determinierungen[18] ebenso eine erste Annäherung leisten wie der Verweis auf der Rechtsordnung bereits vertraute Wertungsmodelle wie dem der praktischen Fähigkeit zur Erfüllung der jeweiligen Pflicht und dem Wirksamkeitsideal des Datenschutzrechts. Doch bleibt auch eine solche Annäherung naturgemäß vage und unbestimmt und verweist letztlich auf eine rechtswissenschaftsferne, soziale Praxis.[19] Die Konturierung dessen, wie weit die Fähigkeit eines Akteurs zur Erfüllung einer Pflicht tatsächlich reicht und wie stark ihn eine entsprechende Inpflichtnahme belastet, setzt ebenso Erfahrungswerte aus den Disziplinen der jeweiligen Materien voraus, wie es die vorherige Abschätzung und spätere Evaluation der Wirkungen des Regulierungsansatzes und seiner Instrumente tut.

Hier können die in Kapitel 1 hergeleiteten und im Verlauf der Arbeit regelmäßig eingebrachten Erkenntnisse der Wirtschaftsinformatik hinsichtlich des Zusammenspiels von Plattformbetreibern und den auf Plattformen heimischen Akteuren einen tragfähigen Beitrag zur Konturierung und Ausfüllung dieser Fragen leisten und können die beschriebenen Tatbestandsmerkmale und Generalklauseln eine Funktion als „Brückennormen“[20] zur Inkorporierung dieses Beitrags leisten. Das Ergebnis ist die Verarbeitung wirtschaftsinformatorischer Erkenntnisse nach juristischen Regeln.[21] Eine umfassende und auf typische

---

15 Siehe hierzu Kapitel 3 C. III. b) bb) und D. III. a).

16 *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, S. 16.

17 Vgl. *Hofmann*, JZ 2018, 746 (750): „Was aber namentlich in Grenzfällen als erlaubt oder verboten anzusehen sein soll, entzieht sich in letzter Konsequenz genuin juristischer Bewertung.“

18 Wie er in Kapitel 2 A. und B. III. durchgeführt wurde.

19 Vgl. *Hofmann*, JZ 2018, 746 (754) zu der Auflösung des zugrundeliegenden Spannungsverhältnisses: „Zu dessen Auflösung bedarf es der Absicherung durch Erkenntnisse anderer Disziplinen abhängig vom sozialen oder technischen Kontext.“

20 *Duttge*, NJW 2005, 260 (260 f.) zu einer solchen Funktion der „Sittenwidrigkeit“ im Rahmen der Einwilligung in Körperverletzungen für § 228 StGB.

21 Vgl. *Hellgardt*, Regulierung und Privatrecht, S. 739; mit den Worten von *Hofmann*, JZ 2018, 746 (754) nimmt die Rechtswissenschaft hier die moderierende Rolle eines „ehrlichen Maklers“ ein.

Einzelfälle abzielende Vornahme dieser Inkorporierung ist außerhalb des Rahmens dieser Arbeit. Sie kann aber zumindest einen Impuls zur weiteren und vertieften Auseinandersetzung geben.

So kann auf Ebene der Verantwortlichkeits*zuschreibung* etwa nach hier vertretener Ansicht das Zusammenspiel zwischen dem Verständnis einer digitalen Plattform als Anbieter einer Infrastruktur mit erweiterbarer Code-Basis und den Einfluss- und Kontrollmöglichkeiten eines solchen Plattformbetreibers im Rahmen der von ihm entwickelten und eingesetzten *boundary resources* den Weg hin zu einem genuin datenschutzrechtlichen, von benachbarten Rechtsregimen unabhängigen, Plattformbegriff ebnen, der die datenschutzrechtsspezifischen Grundsätze berücksichtigt und so konstituierend für die Definition der hier vorgeschlagenen Plattformverantwortlichkeit ist. Die durch die Linse der Wirtschaftsinformatik betrachtete Gemengelage aus verschiedenen Akteuren auf einer Plattform, die jeweils eigene Verarbeitungsbeiträge leisten, kann, kombiniert mit dem Filter der durch die jüngste EuGH-Rechtsprechung geschärften Erwartungen an die Zuschreibung gemeinsamer Verantwortlichkeit, aufzeigen, weshalb Diensteanbieter zwar gemeinsam mit Drittparteien, aber ggf. nur in eingeschränkter Weise, für deren Verarbeitungen verantwortlich sein sollten.

Auch auf Ebene der *Ausfüllung* der einer solchen Verantwortlichkeit nachgelagerten Pflichten (also der *Ausgestaltung* der Verantwortlichkeit) kann das Wissen um die konkreten technischen und faktischen Handlungsmöglichkeiten und -limitierungen aus Informatik und Wirtschaftsinformatik herangezogen werden:[22] Je leichter einsetzbar und umfassender durchsetzbar eine Maßnahme, je mehr sie den bereits praktizierten *boundary resources* eines Plattformbetreibers ähnelt und diese ggf. nur im Detail modifiziert, desto eher ist ihre Erfüllung dem Plattformbetreiber zumutbar. Die Erkenntnisse hinsichtlich der iterativen Entwicklung dieser Ressourcen im Wechselspiel mit regelmäßigen Gegenimpulsen durch die sie wahrnehmenden und von ihnen begrenzt werdenden Diensteanbieter[23] leiten zudem den Weg hin zur verfahrensrechtlichen Absicherung[24] der bei der Reichweitenbestimmung und Ausfüllung der Pflichten ebenfalls zu berücksichtigenden Interessen von datenverarbeitenden Akteuren, können also Leitlinien für die Konturierung solcher Absicherungen bieten. Dabei müssen auch die einzelfallabhängigen Unterschiede der grundlegenden Plattformausrichtungen berücksichtigt werden, da bspw. die Betreiber offener und geschlossener Plattformen auf jeweils unterschiedliche Art und Weise, aber ggf. mit ähnlichen Ergebnissen, ihren Einfluss ausüben.[25]

[22] Dazu ebenfalls *Hofmann*, JZ 2018, 746 (754) beispielhaft an der Materie des Urheberrechts: „Können auf technischem Wege urheberrechtlich geschützte, von Rechteinhabern gemeldete Inhalte leicht aufgespürt werden, spricht dies dafür, dass das Recht dies über eine entsprechende Verkehrspflicht abbildet."

[23] Siehe hierzu Kapitel 1 B. II. 1.

[24] Zur Notwendigkeit dieser siehe die Ausführungen in Kapitel 3 D. IV. 4.

[25] Siehe *Greene/Shilton*, New Media & Society 2018, 1640 (1644 ff.), die mittels kriti-

Dabei kommt dem Datenschutzrecht zugute, dass es sich ob der von ihm genutzten Instrumente regulierter Selbstregulierung besonders empfänglich für eine solche Inkorporierung interdisziplinärer Erkenntnisse zeigt. Unter anderem Zertifizierungsstellen gem. Art. 43 DSGVO und akkreditierte Stellen zur Überwachung genehmigter Verhaltensregeln (*codes of conduct*) gem. Art. 41 DSGVO könnten im Rahmen ihrer Tätigkeit zu einer gelebten Interdisziplinarität bei der Durchführung der DSGVO beitragen.

Zuletzt können die Erkenntnisse über die Handlungslogiken, Eigenmotivationen und Rollen der einzelnen Akteure im Umfeld einer Plattform[26] dabei helfen, den Eintritt erhoffter *Wirkungen* und etwaiger unbeabsichtigter Nebenwirkungen besser zu erkennen und evaluieren. Das fragile Gesamtgefüge einer Plattform, auf der Betreiber und Diensteanbieter bei gemeinsamer Wertschöpfung koexistieren, stellt insgesamt ein gesellschaftlich erwünschtes Modell dar, das durch die erweiterte Inpflichtnahme der beiden Akteure nicht aus dem Gleichgewicht gebracht werden sollte. Auch hier kann ein besseres Verständnis um die gegenseitigen Beziehungen und Abhängigkeiten dieser Akteure dazu beitragen, die Wirksamkeit der Anwendung und Durchführung der DSGVO fundiert zu bewerten[27] und bei Bedarf gegenzusteuern.

Insgesamt können die im Rahmen dieser Arbeit gewonnenen interdisziplinären Erkenntnisse um die Bedeutung digitaler Plattformen und die Zusammenhänge der auf ihnen agierenden Akteure hoffentlich einen Beitrag dazu leisten, das für den komplexen und modernen Regelungsansatz der DSGVO erforderliche Steuerungswissen[28] zu bereichern – primär hinsichtlich der hier vorgeschlagenen Entwicklungsvorschläge, ggf. aber auch für das Datenschutzrecht an sich.

G. Ausblick

Die Komplexität der Akteursbeteiligungen beim Gebrauch ganz alltäglicher, ubiquitärer Dienste und Angebote im Internet ist bereits heute unfassbar hoch. Das Ideal eines souveränen Nutzers, der sich der Implikationen seiner Nutzungen und Handlungen stets bewusst ist und entsprechende Maßnahmen ergreift, auf bestimmte Dienste verzichtet oder für datenschutzfreundlichere Angebote

scher Diskursanalyse jeweils den Austausch von iOS- und Android-Entwicklern untereinander und mit den jeweiligen Plattformbetreibern zum Thema Datenschutz und Privatheit analysiert haben.

[26] Siehe hierzu Kapitel 1 A. I.

[27] Siehe hierzu die Ausführungen zur Wirksamkeitskontrolle in Kapitel 2 B. III. 3. sowie den expliziten Bewertungsauftrag in Art. 97 Abs. 1 S. 1 DSGVO.

[28] Vgl. *Eifert*, in: Hoffmann-Riem, Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, S. 137 (140 ff.).

bezahlt, ist nicht nur aus diesem Grund zu einer bloßen Utopie verkommen. Diese Komplexität wird in der Zukunft nur zunehmen. Die vorliegende Arbeit soll in dieser Hinsicht einen Anstoß zur stärkeren Auseinandersetzung insbesondere mit den Problemen der Vielfältigkeit der stets beteiligten Akteure geben und darauf aufmerksam machen, dass die datenschutzrechtliche Verantwortlichkeit eine, wenn nicht *die* zentrale Stellschraube ist, die es im Zusammenhang damit zu betrachten gilt. Die hier unterbreiteten Vorschläge für eine moderne Weiterentwicklung der Verantwortlichkeit sollen dabei ebenfalls nur ein erster Ansatz dafür sein, wie sich diese Stellschraube in der Zukunft justieren lassen könnte. Es scheint klar, dass der Komplexität der Realität nur durch vielschichtige rechtliche Antworten beigekommen werden kann und diese Antworten nur wirksam sein können, wenn sie aufeinander Bezug nehmen und so den Interdependenzen der einzelnen Akteure und ihrer Beiträge Rechnung tragen. Der Gedanke, dass es genügt, wenn jeder für sich pflichtig ist, dass also keine Schutzlücke mehr besteht, wenn es für jede Datenverarbeitung schlicht eine verantwortliche Stelle gibt,[29] ist heute nicht mehr tragbar. Das Gegenteil zu dieser Simplifizierung ist eine überbordende Verantwortlichkeit, die jeden für alles verantwortlich macht und so die Pflichtigen ebenso überfordert wie die Rechtsdurchsetzenden. Die Mitte zwischen diesen Extremen zu finden, ist die große Herausforderung, die es für die Zukunft zu meistern gilt.

[29] So das OVG Schleswig, ZD 2014, 643 (645).

Literaturverzeichnis

Acar, Gunes/Eubank, Christian/Englehardt, Steven/Juarez, Marc/Narayanan, Arvind/Diaz, Claudia, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, S. 674–689.

Acemoglu, Daron/Makhdoumi, Ali/Malekian, Azarakhsh/Ozdaglar, Asuman, Too Much Data: Prices and Inefficiencies in Data Markets, NBER Working Paper 26296, 2019 (abrufbar unter: http://www.nber.org/papers/w26296.pdf). Zuletzt abgerufen am 14.01.2022.

Achara, Jagdish Prasad/Cunche, Mathieu/Roca, Vincent/Francillon, Aurélien, WifiLeaks: underestimated privacy implications of the access_wifi_state android permission, Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks – WiSec '14, S. 231–236.

Adam, Leonie/Micklitz, Hans-Wolfgang, Verbraucher und Online-Plattformen, in: Micklitz, Hans-Wolfgang/Joost, Gesche/Reisch, Lucia A./Zander-Hayat, Helga (Hrsg.), Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt, 2017, S. 45–102.

Adams, Andrew A., Facebook Code: Social Network Sites Platform Affordances and Privacy, J. L. Inf. & Sci. 2014, S. 158–168.

Adams, Robin/Schulz, Wolfgang/Schupp, Sibylle/Wittner, Florian, Guaranteeing privacy policies using lightweight type systems, CLSR 2019, 105337.

Arbeitsgruppe des AK I „Staatsrecht und Verwaltung" der IMK, Ergebnisbericht zum Datenschutz in Sozialen Netzwerken, 2012 (abrufbar unter: https://www.datenschutzzentrum.de/uploads/facebook/20120404-AG-SozNetzw-AK-I-IMK.pdf). Zuletzt abgerufen am 14.01.2022.

Albers, Marion, Information als neue Dimension im Recht, Rechtstheorie 2002, S. 61–89.

dies., Informationelle Selbstbestimmung, 2005.

dies., Evaluation sicherheitsbehördlicher Kompetenzen: Schritte von der symbolischen Politik zum lernenden Recht, VerwArch 2008, S. 481–508.

dies., Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Hoffmann-Riem, W. (Hrsg.), Grundlagen des Verwaltungsrechts Band II: Informationsordnung – Verwaltungsverfahren – Handlungsformen, 2. Auflage 2012, S. 107–234.

dies., Realizing the Complexity of Data Protection, in: Gutwirth, Serge/Leenes, Ronald/de Hert, Paul (Hrsg.), Reloading Data Protection, 2014, S. 213–235.

dies., Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in: Friedewald, Michael/Lamla, Jörg/Roßnagel, Alexander (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, 2017, S. 11–35.

Albrecht, Jan Philipp, Weltstandard made in EU, EuZW 2018, S. 433–434.

*Alepis, Efthim*ios*/Patsakis, Constantinos*, There's Wally! Location Tracking in Android without Permissions, Proceedings of the 3rd International Conference on Information Systems Security and Privacy 2017, S. 278–284.

dies., Hey Doc, Is This Normal?: Exploring Android Permissions in the Post Marshmallow Era, in: Ali, Sk Subidh/Danger, Jean-Luc/Eisenbarth, Thomas (Hrsg.), Security, Privacy, and Applied Cryptography Engineering, 2017, S. 53–73.

Alexander, Christian, Anwendungsbereich, Regelungstechnik und einzelne Transparenzvorgaben der P2B-Verordnung, WRP 2020, S. 945–954.

Allen, Anita, Unpopular privacy: what must we hide?, 2011.

Alsenoy, Brendan van, Allocating responsibility among controllers, processors, and „everything in between": the definition of actors and roles in Directive 95/46/EC, CLSR 2012, S. 25–43.

ders., Liability under EU Data Protection Law, jipitec 2016, S. 271–288.

Alsenoy, Brendan van/Kosta, Eleni/Dumortier, Jos, Privacy notices versus informational self-determination: Minding the gap, International Review of Law, Computers & Technology 2014, S. 185–203.

Art. 29-Datenschutzgruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, 2010 (abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_de.pdf). Zuletzt abgerufen am 14.01.2022.

dies., Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 2010 (abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_de.pdf). Zuletzt abgerufen am 14.01.2022.

dies., Opinion 03/2013 on purpose limitation, 2013 (abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf). Zuletzt abgerufen am 14.01.2022.

dies., Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 2017 (abrufbar unter: https://ec.europa.eu/newsroom/document.cfm?doc_id=44103). Zuletzt abgerufen am 14.01.2022.

dies., Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), 2017 (abrufbar unter: https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/WP243de_Art._29-Gruppe-Datenschutzbeauftragte.pdf). Zuletzt abgerufen am 14.01.2022.

dies., Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, 2017 (abrufbar unter: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236). Zuletzt abgerufen am 14.01.2022.

dies., Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014 (abrufbar unter: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf). Zuletzt abgerufen am 14.01.2022.

Aßhoff, Guido, Mysterium Abmahnwelle – Der Referentenentwurf zum Schutz vor rechtsmissbräuchlicher Abmahnung und seine Wirksamkeit in der Praxis, CR 2018, S. 720–727.

Auer-Reinsdorff, Astrid/Conrad, Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Auflage 2019 (zit. *Bearbeiter*, in: Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht).

Bäcker, Matthias, Grundrechtlicher Informationsschutz gegen Private, Der Staat 2012, S. 91–116.

ders., Das Grundgesetz als Implementationsgarant der Unionsgrundrechte, EuR 2015, S. 389–415.

Badura, Peter, Die verfassungsrechtliche Pflicht des gesetzgebenden Parlaments zur „Nachbesserung" von Gesetzen, in: Müller, Georg/Eichenberger, Kurt (Hrsg.), Staatsorganisation und Staatsfunktionen im Wandel: Festschrift für Kurt Eichenberger zum 60. Geburtstag, 1982, S. 481–492.

Baehr, Thomas, Verhaltenssteuerung durch Ordnungsrecht: das Vollzugsdefizit als Verfassungsproblem, 2005.

Balebako, Rebecca/Jung, Jaeyeon/Lu, Wei/Cranor, Lorrie Faith/Nguyen, Carolyn, „Little brothers watching you": raising awareness of data leaks on smartphones, Proceedings of the Ninth Symposium on Usable Privacy and Security 2013, S. 1–11.

Balkin, Jack M., The Fiduciary Model of Privacy, Harv. L. Rev. 2020, S. 11–33.

Bamberger, Kenneth A./Egelman, Serge/Han, Catherine/Elazari, Amit/Reyes, Irwin, Can You Pay for Privacy? Consumer Expactations and the Behavior of Free and Paid Apps, Berkeley Tech. L. J. 2020, S. 327–366.

Barnitzke, Benno, Rechtliche Rahmenbedingungen des Cloud Computing, 2014.

Bartel, Alexandre/Klein, Jacques/le Traon, Yves/Monperrus, Martin, Automatically securing permission-based software by reducing the attack surface: an application to Android, Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering – ASE 2012, S. 274–277.

Bartels, Karsten U./Backer, Merlin, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 2018, S. 214–219.

Bassini, Marco di, Data Controller: A Shifting Paradigm in the Digital Age, Bocconi Legal Papers 2019, S. 103–131.

Baumgartner, Ulrich/Gausling, Tina, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, ZD 2017, S. 308–313.

Baumgartner, Ulrich/Sitte, Konstantin, Abmahnungen von DS-GVO-Verstößen, ZD 2018, S. 555–560.

Bäumler, Helmut, Normenklarheit als Instrument der Transparenz, JR 1984, S. 361–366.

Bayamlioglu, Emre, Contesting Automated Decisions: A View of Transparency Implications, EDPL 2018, S. 433–446.

BayLDA, Facebook Custom Audience bei bayerischen Unternehmen, ZD-Aktuell 2017, 05805.

Beaucamp, Guy/Seifert, Jens, Soll der Zweckveranlasser weiterleben?, JA 2007, S. 577–580.

Becker, Carlos/Seubert, Sandra, Privatheit, kommunikative Freiheit und Demokratie, DuD 2016, S. 73–78.

Becker, Maximilian, Ein Recht auf datenerhebungsfreie Produkte, JZ 2017, S. 170–181.

Beimborn, Daniel/Miletzki, Thomas/Wenzel, Stefan, Platform as a Service (PaaS), WI 2011, S. 371–375.

Benlian, Alexander/Hilkert, Daniel/Hess, Thomas, How open is this Platform? The Meaning and Measurement of Platform Openness from the Complementers' Perspective, Journal of Information Technology 2015, S. 209–228.

Ben-Shahar, Omri/Schneider, Carl, More than you wanted to know: the failure of mandated disclosure, 2014.

Bergt, Matthias, Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, S. 555–561.

Bickenbach, Christian, Die Einschätzungsprärogative des Gesetzgebers: Analyse einer Argumentationsfigur in der (Grundrechts-)Rechtsprechung des Bundesverfassungsgerichts, 2014.

ders., Rückschaufehler in der Gesetzgebung als verfassungsgerichtliche Herausforderung, RW 2019, S. 243–261.

Bieker, Felix/Bremert, Benjamin, Identifizierung von Risiken für die Grundrechte von Individuen, ZD 2020, S. 7–14.

Bietti, Elettra, Consent as a Free Pass: Platform Power and the Limits of the Informational Turn, Pace L. Rev. 2020, S. 307–397.

Binns, Reuben, Data protection impact assessments: a meta-regulatory approach, IDPL 2017, S. 22–35.

Blanc, Nicolas, Wirtschaftsakademie Schleswig-Holstein: Towards a Joint Responsibility of Facebook Fan Page Administrators for Infringements to European Data Protection Law, EDPL 2018, S. 120–127.

Blankertz, Aline, How competition impacts data privacy, Gutachten für die Stiftung Neue Verantwortung, September 2020 (abrufbar unter: https://www.stiftung-nv.de/de/publikation/how-competition-impacts-data-privacy). Zuletzt abgerufen am 14.01.2022.

Bock, Kirsten/Engeler, Malte, Die verfassungsrechtliche Wesensgehaltsgarantie als absolute Schranke im Datenschutzrecht, DVBl 2016, S. 593–599.

Boehme-Neßler, Volker, Big Data und Demokratie – Warum Demokratie ohne Datenschutz nicht funktioniert, DVBl 2015, S. 1282–1287.

Bogdandy, Armin von/Bast, Jürgen (Hrsg.), Europäisches Verfassungsrecht: theoretische und dogmatische Grundzüge, 2. Auflage 2009 (zit. *Bearbeiter*, in: von Bogdandy/Bast, Europäisches Verfassungsrecht).

Böhret, Carl/Konzendorf, Götz, Ko-Evolution von Gesellschaft und funktionalem Staat: ein Beitrag zur Theorie der Politik, 1997.

dies., Handbuch Gesetzesfolgenabschätzung (GFA): Gesetze, Verordnungen, Verwaltungsvorschriften, 2001.

Borgesius, Frederik/Kruikemeier, Sanne/Boerman, Sophie C/Helberger, Natali, Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, EDPL 2017, S. 353–368.

Borgesius, Frederik/Möller, Judith/Kruikemeier, Sanne/Fathaigh, Ronan ó/Irion, Kristina/Dobber, Tom/Bodo, Balazs/de Vreese, Claes, Online Political Microtargeting: Promises and Threats for Democracy, ULR 2018, S. 82–96.

Born, Christian, Schadensersatz bei Datenschutzverstößen: ein ökonomisches Instrument des Datenschutzes und seine präventive Wirkung, 2001.

Bosco, Francesca/Creemers, Niklas/Ferraris, Valeria/Guagnin, Daniel/Koops, Bert-Jaap, Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities, in: Gutwirth, Serge/Leenes, Ronald/de Hert, Paul (Hrsg.), Reforming European Data Protection Law, 2015, S. 3–33.

Botta, Jonas, Der California Consumer Privacy Act: Wegbereiter eines angemessenen Datenschutzniveaus im Silicon Valley?, PinG 2019, S. 261–266.

Boudreau, Kevin/Hagiu, Andrei, Platform Rules: Multi-Sided Platforms as Regulators, in: Gawer, Annabelle (Hrsg.), Platforms, Markets and Innovation, 2009, S. 163–191.

Bougiakiotis, Emmanouil, The layered links model: an alternative approach to international privacy regulation, IDPL 2020, S. 253–268.

Brink, Stefan, Der Beratungsauftrag der Datenschutzaufsichtsbehörden, ZD 2020, S. 59–62.

Brink, Stefan/Wolff, Heinrich Amadeus (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 37. Edition (Stand: 01.08.2021) (zit. *Bearbeiter*, in: BeckOK Datenschutzrecht).

Britz, Gabriele, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft: ausgewählte Schriften von Wolfgang Hoffmann-Riem mit begleitenden Analysen, 2010, S. 561–596.

Brkan, Maja, The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning, German Law Journal 2019, S. 864–883.

Brühann, Ulf, Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG: Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs, EuZW 2009, S. 639–644.

Brühann, Ulf/Zerdick, Thomas, Umsetzung der EG-Datenschutzrichtlinie, CR 1996, S. 429–436.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, 2006.

ders., Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, S. 155–161.

Bull, Hans Peter, Informationelle Selbstbestimmung – Vision oder Illusion?: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, 2., aktualisierte Auflage 2011.

ders., Sinn und Unsinn des Datenschutzes: Persönlichkeitsrecht und Kommunikationsfreiheit in der digitalen Gesellschaft, 2015.

Bülte, Jens, Das Datenschutzbußgeldrecht als originäres Strafrecht der Europäischen Union?, StV 2017, S. 460–470.

Bumke, Christian, Die Entwicklung der Grundrechtsdogmatik in der deutschen Staatsrechtslehre unter dem Grundgesetz, AöR 2019, S. 3–80.

Bundeskartellamt, Arbeitspapier – Marktmacht von Plattformen und Netzwerken, Juni 2016 (abrufbar unter: https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.pdf%3F__blob%3DpublicationFile%26v%3D2). Zuletzt abgerufen am 14.01.2022.

Bunnenberg, Jan Niklas, Privatautonomie und Datenschutz, JZ 2020, S. 1088–1097.

ders., Privates Datenschutzrecht: Über Privatautonomie im Datenschutzrecht – unter besonderer Berücksichtigung der Einwilligung und ihrer vertraglichen Kopplung nach Art. 7 Abs. 4 DS-GVO, 2020.

Burdon, Mark, Privacy invasive geo-mashups: privacy 2.0 and the limits of first generation information privacy laws, University of Illinois Journal of Law, Technology and Policy 2010, S. 1–50.

Burrell, Jenna, How the machine ‚thinks': Understanding opacity in machine learning algorithms, Big Data & Society 2016, S. 1–12.

Busch, Christoph, Mehr Fairness und Transparenz in der Plattformökonomie?, GRUR 2019, S. 788–796.

Busch, Christoph/Dannemann, Gerhard/Schulte-Nölke, Hans, Bausteine für ein europäisches Recht der Plattformökonomie, MMR 2020, S. 667–676.

Busching, Michael, Der Schutz „privater" Informationen bei Cloud Computing, 2019.

Buss, Sebastian, Privacy by Design und Software, CR 2020, S. 1–6.

Bygrave, Lee A, The Place of Privacy in Data Protection Law, UNSW Law Journal 2001, S. 277–283.

Calliess, Christian/Ruffert, Matthias (Hrsg.), EUV/AEUV: das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta: Kommentar, 6. Auflage 2022 (zit. *Bearbeiter*, in: Calliess/Ruffert, EUV/AEUV).

Canaris, Claus-Wilhelm, Grundrechte und Privatrecht, AcP 1984, S. 201–246.

ders., Grundrechte und Privatrecht, 1999.

Cannataci, Joseph A/Mifsud-Bonnici, Jeanne Pia, Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty, Information & Communications Technology Law 2005, S. 5–15.

Cate, Fred H./Mayer-Schönberger, Viktor, Notice and consent in a world of Big Data, IDPL 2013, S. 67–73.

Chia, Pern Hui/Yamamoto, Yusuke/Asokan, N., Is this app safe?: a large scale study on application permissions and risk signals, Proceedings of the 21st international conference on World Wide Web – WWW '12 2012, S. 311–320.

Chmelik, Tomas, Social Network Sites – Soziale Netzwerke, 2016.

Choi, Yooncheol, Die Pflicht des Gesetzgebers zur Beseitigung von Gesetzesmängeln, 2002.

Christl, Wolfie, Kommerzielle digitale Überwachung im Alltag: Studie im Auftrag der Bundesarbeitskammer Wien, 2014, (abrufbar unter: https://crackedlabs.org/dl/Studie_Digitale_Ueberwachung.pdf). Zuletzt abgerufen am 14.01.2022.

Clifford, Damian/Graef, Inge/Valcke, Peggy, Pre-formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections, German Law Journal 2019, S. 679–721.

Cohen, Julie E., Examined Lives: Informational Privacy and the Subject as Object, Stanford Law Rev. 2000, S. 1373–1438.

Collin, Peter, Privatisierung und Etatisierung als komplementäre Gestaltungsprozesse: Ein historischer Rückblick auf „regulierte Selbstregulierung", JZ 2011, S. 274–282.

Conseil National du Numérique, Ambition Numérique. Pour une Politique Française et Européenne de la Transition Numérique, 2015 (abrufbar unter: https://cnnumerique.fr/files/2018-04/CNNum--rapport-ambition-numerique.pdf). Zuletzt abgerufen am 14.01.2022.

Costello, Róisín Áine, The Impacts of AdTech on Privacy Rights and the Rule of Law, TechReg 2020, S. 11–23.

Czaja, Frank, Eigensicherungspflichten von Verkehrsflughäfen: die Beteiligung der Verkehrsflughäfen an der Abwehr äußerer Gefahren für die Sicherheit des Luftverkehrs, 1995.

Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutzgrundverordnung Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, S. 307–314.

Deutsches Institut für Menschenrechte, „Zugang zu Datenschutz-Rechtsbehelfen in EU-Mitgliedstaaten" – eine Studie der EU-Grundrechteagentur, 2014 (abrufbar unter: https://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states). Zuletzt abgerufen am 14.01.2022.

Diercks, Nina, Die DSGVO entfaltet keine Sperrwirkung gegenüber den Rechtsbehelfen aus dem UWG, CR 2018, S001.

dies., Verhältnis zwischen Datenschutzrecht und UWG aus europarechtlicher Sicht, CR 2019, S. 95–100.

dies., Einsatz von Google Analytics, DSB 2020, S. 41–43.

Di Fabio, Udo, Gefahr, Vorsorge, Risiko – Die Gefahrenabwehr unter dem Einfluß des Vorsorgeprinzips, JURA 1996, S. 566–574.

ders., Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: Hailbronner, Kay (Hrsg.), Kontrolle der auswärtigen Gewalt: Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, 1997, S. 235–277.

Dijck, José van/Poell, Thomas/de Waal, Martijn, The platform society, 2018.

Dimitriadis, Antonios/Efraimidis, Pavlos S./Katos, Vasilios, Malevolent app pairs: an Android permission overpassing scheme, Proceedings of the ACM International Conference on Computing Frontiers 2016, S. 431–436.

Donos, Pelopidas Konstantinos, Datenschutz – Prinzipien und Ziele: unter besonderer Berücksichtigung der Entwicklung der Kommunikations- und Systemtheorie, 1998.

Drackert, Stefan, Die Risiken der Verarbeitung personenbezogener Daten: eine Untersuchung zu den Grundlagen des Datenschutzrechts, 2014.

Dregelies, Max, Wohin laufen meine Daten? Datenschutz bei Sportuhren und Fitnesstrackern, VuR 2017, S. 256–262.

DSK, Kurzpapier Nr. 16: Gemeinsam für die Verarbeitung Verantwortliche, Art. 26 DSGVO, 2018 (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_16.pdf). Zuletzt abgerufen am 14.01.2022.

dies., Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, 2019 (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20190405_positionierung_facebook_fanpages.pdf). Zuletzt abgerufen am 14.01.2022.

dies., Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich, 2020, (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf). Zuletzt abgerufen am 14.01.2022.

Dreier, Horst (Hrsg.), Grundgesetz: Kommentar, Band 1: Präambel, Art. 1–19, 3. Auflage 2013 (zit.: *Bearbeiter*, in: Dreier, GG Band I).

Dreyer, Stephan, Entscheidungen unter Ungewissheit im Jugendmedienschutz: Untersuchung der spielraumprägenden Faktoren gesetzgeberischer und behördlicher Entscheidungen mit Wissensdefiziten, 2018.

Dreyer, Stephan/Schulz, Wolfgang, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme? Gutachten für die Bertelsmann Stiftung, 2018 (abrufbar unter: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Bibliothek/Doi_Publikationen/BSt_DSGVOundADM_dt.pdf). Zuletzt abgerufen am 14.01.2022.

Ducuing, Charlotte/Schroers, Jessica/Kindt, Els, The Wirtschaftsakademie Fan Page Decision: A Landmark on Joint Controllership – A Challenge for Supervisory Authorities Competences, EDPL 2018, S. 547–553.

Dünkel, Heiko, Kollektiver Rechtsschutz bei Datenschutzrechtsverstößen, DuD 2019, S. 483–487.

Dürig, Günter/Herzog, Roman/Scholz, Rupert (Hrsg.), Grundgesetz: Kommentar, 95. Auflage 2021 (zit. *Bearbeiter*, in: Dürig u. a., GG).

Düsseldorfer Kreis, Beschluss zum Datenschutz in sozialen Netzwerken, 08.12.2011 (abrufbar unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/B_Datenschutz%20in%20sozialen%20Netzwerken.pdf). Zuletzt abgerufen am 14.01.2022.

Duttge, Gunnar, Der BGH auf rechtsphilosophischen Abwegen – Einwilligung in Körperverletzung und „gute Sitten", NJW 2005, S. 260–263.

Eaton, Ben/Elaluf-Calderwood, Silvia/Sørensen, Carsten/Yoo, Youngjin, Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System, MIS Quarterly 2015, S. 217–243.

Eckhardt, Jens, DS-GVO: Anforderungen an die Auftragsverarbeitung als Instrument zur Einbindung Externer, CCZ 2017, S. 111–117.

Edwards, Lilian/Finck, Michèle/Veale, Michael/Zingales, Nicolo, Data subjects as data controllers: a Fashion(able) concept?, Internet Policy Review, Blogpost vom 13.06.2019 (abrufbar unter: https://policyreview.info/articles/news/data-subjects-data-controllers-fashionable-concept/1400). Zuletzt abgerufen am 14.01.2022.

Edwards, Lilian/Veale, Michael, Slave to the Algorithm? Why a ‚right to an explanation' is probably not the remedy you are looking for, Duke Law & Technology Review 2017, S. 18–84.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO: Kommentar, 2. Auflage 2018 (zit. *Bearbeiter*, in: Ehmann/Selmayr, DSGVO).

Eichenhofer, Johannes, Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz, Der Staat 2016, S. 41–67.

Eidenmüller, Horst, Effizienz als Rechtsprinzip: Möglichkeiten und Grenzen der ökonomischen Analyse des Rechts, 3. Auflage 2005.

Eifert, Martin, Regulierte Selbstregulierung und die lernende Verwaltung, in: Hoffmann-Riem, Wolfgang (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates: Ergebnisse des Symposiums aus Anlaß des 60. Geburtstages von Wolfgang Hoffmann-Riem, 2001, S. 137–158.

ders., § 19 Regulierungsstrategien, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts Band I: Methoden, Maßstäbe, Aufgaben, Organisation, 2. Auflage 2012, S. 1319–1394.

ders. Rechenschaftspflichten für soziale Netzwerke und Suchmaschinen, NJW 2017, S. 1450–1454.

ders., Evaluation des NetzDG Im Auftrag des BMJV, 2020 (abrufbar unter: https://www.bmj.de/SharedDocs/Downloads/DE/News/PM/090920_Juristisches_Gutachten_Netz.pdf?__blob=publicationFile&v=3). Zuletzt abgerufen am 14.01.2022.

Elbrecht, Carola/Schröder, Michaela, Verbandsklagebefugnisse bei Datenschutzverstößen für Verbraucherverbände, K&R 2015, S. 361–366.

Enck, William/Gilbert, Peter/Han, Seungyeop/Tendulkar, Vasant/Chun, Byung-Gon/Cox, Landon P./Jung, Jaeyeon/McDaniel, Patrick/Sheth, Anmol N., TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones, ACM Trans. Comput. Syst. 2014, S. 1–29.

Engeler, Malte, Die Auftragsdatenverarbeitung braucht ein Reboot – mit der DSGVO in der Hauptrolle, Telemedicus, Blogpost vom 24.11.2016 (abrufbar unter: http://www.

telemedicus.info/article/3150-Die-Auftragsdatenverarbeitung-braucht-ein-Reboot-mit-der-DSGVO-in-der-Hauptrolle.html). Zuletzt abgerufen am 14.01.2022.

Entorf, Horst, Ökonomische Theorie der Kriminalität, in: Ott, Claus/Schäfer, Hans-Bernd (Hrsg.), Die Präventivwirkung zivil- und strafrechtlicher Sanktionen: Beiträge zum VI. Travemünder Symposium zur ökonomischen Analyse des Rechts vom 25. – 28. März 1998, 1999, S. 1–21.

Epping, Volker/Hillgruber, Christian (Hrsg.), Beck'scher Online-Kommentar Grundgesetz, 48. Edition 2019 (Stand: 15.08.2021) (zit. *Bearbeiter*, in: BeckOK Grundgesetz).

Erdos, David, Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU acquis, Int J Law Info Tech 2018, S. 189–225.

Ernst, Christian, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, S. 1026–1036.

Ernst, Stefan, Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, S. 1917–1919.

ders., Die Widerruflichkeit der datenschutzrechtlichen Einwilligung, ZD 2020, S. 383–385.

Etteldorf, Christina, Italien: Ermittlungen gegen Facebook im Zusammenhang mit Cambridge Analytica abgeschlossen, MMR-Aktuell 2019, 415069.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic And Social Committee and the Committee Of The Regions: Tackling Illegal Content Online – Towards an enhanced responsibility of online platforms, 2017 (abrufbar unter: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-555-F1-EN-MAIN-PART-1.PDF). Zuletzt abgerufen am 14.01.2022.

dies., Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation, 2020 (abrufbar unter: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264). Zuletzt abgerufen am 14.01.2022.

Europäischer Datenschutzbeauftragter, Leitlinien des EDSB zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" nach der Verordnung (EU) 2018/1725, 2019 (abrufbar unter: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_de.pdf). Zuletzt abgerufen am 14.01.2022.

European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, 2019 (abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en). Zuletzt abgerufen am 14.01.2022.

dass., Guidelines 4/2019 on Article 25 (Data Protection by Design and by Default), 2019 (abrufbar unter: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_de). Zuletzt abgerufen am 14.01.2022.

dass., Guidelines 07/2020 on the concepts of controller and

processor in the GDPR, Version 2.0, 2021 (abrufbar unter https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf). Zuletzt abgerufen am 14.01.2022.

dass., Guidelines 8/2020 on the targeting of social media users, 2020 (abrufbar unter: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-082020-targeting-social-media-users_de). Zuletzt abgerufen am 14.01.2022.

European Parliament, Report on online platforms and the digital single market (2016/2276(INI)), 2017 (abrufbar unter: https://www.europarl.europa.eu/doceo/document/A-8-2017-0204_EN.html). Zuletzt abgerufen am 14.01.2022.

Evans, David S., Governing Bad Behavior by Users of Multi-Sided Platforms, Berkeley Tech. L. J. 2012, S. 1201–1250.

Evans, David S./Hagiu, Andrei/Schmalensee, Richard, Invisible engines: how software platforms drive innovation and transform industries, 2006.

Fairfield, Joshua/Engel, Christoph, Privacy as a Public Good, Duke Law Journal 2015, S. 95–128.

Fatema, Kaniz/Hadziselimovic, Ensar/Pandit, H. J./Debruyne, Christophe/Lewis, Dave/O'Sullivan, Declan, Compliance through informed consent: Semantic based consent permission and data management model, 5th Workshop on Society, Privacy and the Semantic Web-Policy and Technology (PrivOn 2017). CEUR Workshop Proceedings 2017, S. 60–75.

Faust, Sebastian/Spittka, Jan/Wybitul, Tim, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen den Datenschutz, ZD 2016, S. 120–125.

Fehling, Michael, Perspektiven des Öffentlichen Wirtschaftsrechts, JZ 2016, S. 540–547.

Feldman, Dan/Haber, Eldar, Measuring and Potecting Privacy in the Always-On Era, Berkeley Tech. L. J. 2020, S. 197–250.

Felt, Adrienne Porter/Chin, Erika/Hanna, Steve/Song, Dawn/Wagner, David, Android permissions demystified, Proceedings of the 18th ACM conference on Computer and communications security – CCS '11 2011, S. 627–637.

Finck, Michèle, Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy, LSE Law, Society and Economy Working Paper 15/2017 (abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2990043). Zuletzt abgerufen am 14.01.2022.

Föhlisch, Carsten/Pilous, Madeleine, Anmerkung zu LG Düsseldorf, Urt. v. 09.03.2016, Az. 12 O 151/15, MMR 2016, S. 328–332.

fouad, Imane/Bielova, Nataliia/Legout, Arnaud/Sarafijanovic-Djukic, Natasa, Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels, Proceedings on Privacy Enhancing Technologies 2020, S. 499–518.

Franzius, Claudio, Das Recht auf informationelle Selbstbestimmung, ZJS 2015, S. 259–270.

Frenz, Walter, Handbuch Europarecht: Band 4: Europäische Grundrechte, 2009.

Frosio, Giancarlo F., Why keep a dog and bark yourself? From intermediary liability to responsibility, Int J Law Info Tech 2018, S. 1–33.

Funke, Andreas, Gleichbehandlungsgrundsatz und Verwaltungsverfahren: Die Rechtsprechung des BVerfG zu strukturell bedingten Vollzugsdefiziten, AöR 2007, 168–214.

Gawer, Annabelle/Cusumano, M. A., How companies become platform leaders, MIT Sloan Management Review 2008, S. 28–35.

Gawer, Annabelle/Henderson, Rebecca, Platform Owner Entry and Innovation in Complementary Markets: Evidence from Intel, J Economics Management Strategy 2007, S. 1–34.

Gellert, Raphaël, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights- Based and the Risk-Based Approaches to Data Protection, EDPL 2016, S. 481–492.
ders., The risk-based approach to data protection, 2020.
Gellert, Raphaël/Gutwirth, Serge, The legal construction of privacy and data protection, CLSR 2013, S. 522–530.
Geminn, Christian L., Betroffenenrechte verbessern, DuD 2020, S. 307–311.
Gersdorf, Hubertus, Funktionen der Gemeinschaftsgrundrechte im Lichte des Solange II-Beschlusses des Bundesverfassungsgerichts, AöR 1994, S. 400–426.
Ghazawneh, Ahmad/Henfridsson, Ola, Governing third-party development through platform boundary resources, International Conference on Information Systems, Conference Proceedings 2010, S. 1–17.
dies., Balancing platform control and external contribution in third-party development: the boundary resources model: Control and contribution in third-party development, Information Systems Journal 2013, S. 173–192.
dies., A Paradigmatic Analysis of Digital Application Marketplaces, Journal of Information Technology 2015, S. 198–208.
Gierschmann, Sibylle, Gemeinsame Verantwortlichkeit in der Praxis, ZD 2020, S. 69–73.
Gierschmann, Sibylle/Schlender, Katharina/Stentzel, Rainer/Veil, Winfried (Hrsg.), Kommentar Datenschutz-Grundverordnung, 2018 (zit. *Bearbeiter*, in: Gierschmann u. a., DSGVO).
Giesen, Thomas, Totaler Datenschutz in der EU: freiheitswidrig, bürokratisch und erfolglos!, NVwZ 2019, S. 1711–1718.
Gillespie, Tarleton, Platforms Intervene, Social Media + Society 2015, S. 1–2.
Glancy, Dorothy J., The Invention of the Right to Privacy, Arizona Law Review 1979, S. 1–39.
Globocnik, Jure, On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID, IIC 2019, S. 1033–1044.
Gola, Peter (Hrsg.), Datenschutz-Grundverordnung VO (EU) 2016/679 Kommentar, 2. Auflage 2018 (zit. *Bearbeiter*, in: Gola, DSGVO).
Golla, Sebastian J., Die Straf- und Bußgeldtatbestände der Datenschutzgesetze als Teil des Schutzes des informationellen Selbstbestimmungsrechts, 2015.
ders., Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, jipitec 2017, S. 70–78.
Golland, Alexander, Gemeinsame Verantwortlichkeit in mehrstufigen Verarbeitungsszenarien, K&R 2018, S. 433–438.
ders., Datenverarbeitung in sozialen Netzwerken, 2019.
ders., Gemeinsam einsam: Ein „Like“ für die gemeinsame Verantwortlichkeit?, ZD 2019, S. 381–382.
ders., Reichweite des „Joint Controllership“: Neue Fragen der gemeinsamen Verantwortlichkeit, K&R 2019, S. 533–537.
ders., Die „private“ Datenverarbeitung im Internet, ZD 2020, S. 397–403.
González Fuster, Gloria, Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection, Birkbeck Law Review 2014, S. 263–278.
Goodman, Bryce/Flaxman, Seth, European Union Regulations on Algorithmic Decision-Making and a „Right to Explanation“, AIMag 2017, S. 50–57.

Gorwa, Robert, What is platform governance?, Information, Communication & Society 2019, S. 854–871.

Grabitz, Eberhard, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Bundesverfassungsgerichts, AöR 1973, S. 568–616.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union: Kommentar, 73. Ergänzungslieferung (Stand: Mai 2021) (zit. *Bearbeiter*, in: Grabitz u. a., Das Recht der Europäischen Union).

Grafenstein, Maximilian von, The Principle of Purpose Limitation in Data Protection Laws, 2018.

Greene, Daniel/Shilton, Katie, Platform privacies: Governance, collaboration, and the different meanings of „privacy" in iOS and Android development, New Media & Society 2018, S. 1640–1657.

Greve, Holger, Drittwirkung des grundrechtlichen Datenschutzes im digitalen Zeitalter, in: Franzius, Claudio/Lejeune, Stefanie/von Lewinski, Kai/Meßerschmidt, Klaus/Michael, Gerhard/Rossi, Matthias/Schilling, Theodor/Wysk, Peter (Hrsg.), Beharren. Bewegen: Festschrift für Michael Kloepfer zum 70. Geburtstag, 2013, S. 665–677.

Grewe, Max, Missbrauchsverbot als Durchsetzungsinstrument: eine Untersuchung der Schnittstellen des Kartellrechts mit dem Datenschutz-, Lauterkeits- und AGB-Recht, 2020.

Grimm, Christoph, Gesetzesfolgenabschätzung – Möglichkeiten und Grenzen – aus der Sicht des Parlaments, ZRP 2000, S. 87–91.

Grimm, Dieter, Der Datenschutz vor einer Neuorientierung, JZ 2013, S. 585–592.

Grimm, Rüdiger, Spuren im Netz, DuD 2012, S. 88–91.

Grundy, Quinn/Chiu, Kellia/Held, Fabian/Continella, Andrea/Bero, Lisa/Holz, Ralph, Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis, BMJ 2019, S. 1–11.

Guckelberger, Annette, Veröffentlichung der Leistungsempfänger von EU-Subventionen und unionsgrundrechtlicher Datenschutz, EuZW 2011, S. 126–130.

Guggenberger, Nikolas, The Epic Battle for the Soul of Antitrust, Verfassungsblog, Blogbeitrag vom 02.09.2020 (abrufbar unter: https://verfassungsblog.de/the-epic-battle-for-the-soul-of-antitrust/). Zuletzt abgerufen am 14.01.2022.

ders., Essential Platforms, Stanford Technology Law Review, 2021, 237–343.

Gürses, Seda/van Hoboken, Joris, Privacy after the Agile Turn, in: Selinger, Evan/Polonetsky, Jules/Tene, Omer (Hrsg.), The Cambridge Handbook of Consumer Privacy, 2018, S. 579–601.

Hain, Karl-Eberhard, Der Gesetzgeber in der Klemme zwischen Übermaß- und Untermaßverbot, DVBl 1993, S. 982–984.

Hain, Karl-Eberhard/Ferreau, Frederik/Brings-Wiesen, Tobias, Regulierung sozialer Netzwerke revisited, K&R 2017, S. 433–438.

Halfmeier, Axel, Die neue Datenschutzverbandsklage, NJW 2016, S. 1126–1129.

Han, Catherine/Reyes, Irwin/Feal, Álvaro/Reardon, Joel/Wijesekera, Primal/Elazari, Amit/Bamberger, Kenneth A./Egelman, Serge, The Price is (Not) Right: Comparing Privacy in Free and Paid Apps, Proceedings on Privacy Enhancing Technologies 2020, S. 222–242.

Hanloser, Stefan, Anmerkung zu EuGH, 29.07.2019 – C-40/17 – Fashion ID, ZD 2019, S. 455–460.

Härting, Niko, Profiling: Vorschläge für eine intelligente Regulierung, CR 2014, S. 528–536.

Heberlein, Johanna, Datenschutz im Social Web: materiell-rechtliche Aspekte der Verarbeitung personenbezogener Daten durch Private in sozialen Netzwerken, 2017.
Heckmann, Dirk, Vertrauen in virtuellen Räumen?, K&R 2010, S. 1–7.
Helberger, Natali, Code and (Intellectual) Property, in: Dommering, Egbert/Asscher, Lodewijk (Hrsg.), Coding regulation: essays on the normative role of information technology, 2006, S. 219–265.
Helberger, Natali/Pierson, Jo/Poell, Thomas, Governing online platforms: From contested to cooperative responsibility, The Information Society 2018, S. 1–14.
Helbing, Thomas, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 2015, S. 145–150.
Hellgardt, Alexander, Regulierung und Privatrecht, AcP 2016, 349–351.
ders., Regulierung und Privatrecht, 2016.
Hemmert-Halswick, Maximilian, Das (vorläufige?) Ende der e-Privacy-VO, MMR-Aktuell 2019, 422777.
Hennemann, Moritz, Wettbewerb der Datenschutzrechtsordnungen, RabelsZ 2020, S. 865–895.
Hennrich, Thorsten, Cloud Computing – Herausforderungen an den Rechtsrahmen für Datenschutz, 2016.
Hense, Peter, Hi Alexa, can I trust you? Technologie, Wirtschaft und Rechtsentwicklungen bei Virtual Private Assistants, DSB 2019, S. 250–254.
Hermstrüwer, Yoan, Informationelle Selbstgefährdung: zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, 2016.
Hert, Paul de/Gutwirth, Serge, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in: Gutwirth, Serge/Poullet, Yves/de Hert, Paul/de Terwangne, Cécile/Nouwt, Sjaak (Hrsg.), Reinventing data protection?, 2009, S. 3–44.
Hert, Paul de/Papakonstantinou, Vagelis, The new General Data Protection Regulation: Still a sound system for the protection of individuals?, CLSR 2016, S. 179–194.
Hess, Thomas/Schreiner, Michel, Ökonomie der Privatsphäre, DuD 2012, S. 105–109.
Hesse, Konrad, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Auflage 1999.
Heun, Werner, Staatliche Risikosteuerung und Verfassung, RW 2011, S. 376–399.
Hijmans, Hielke, The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU, 2016.
Hildebrandt, Mireille, Smart technologies and the end(s) of law: novel entanglements of law and technology, Paperback edition 2016.
Hippel, Eric von/Katz, Ralph, Shifting Innovation to Users via Toolkits, Management Science 2002, S. 821–833.
Hirsch, Dennis D., The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?, Seattle U. L. Rev. 2011, S. 439–480.
Hladjk, Jörg, Online-Profiling und Datenschutz, 2007.
Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd (Hrsg.), Handbuch Multimedia-Recht: Rechtsfragen des elektronischen Geschäftsverkehrs, 56. Ergänzungslieferung (Stand: Mai 2021) (zit. *Bearbeiter*, in: Hoeren u. a., Handbuch Multimedia-Recht).
Hoffmann, Christian/Schulz, Sönke E., Facebook-Fanseiten deutscher Unternehmen – Verlängerung vor dem EuGH, JuWiss-Blog, Blogeintrag vom 04.03.2016 (abrufbar unter: https://www.juwiss.de/24-2016/). Zuletzt abgerufen am 14.01.2022.

Hoffmann, Christian/Schulz, Sönke E./Brackmann, Franziska, Die öffentliche Verwaltung in den sozialen Medien? Zulässigkeit behördlicher Facebook-Fanseiten, ZD 2013, S. 122–126.

Hoffmann-Riem, Wolfgang, Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen – Systematisierung und Entwicklungsperspektiven, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996, S. 261–336.

ders., Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 1998, S. 513–540.

ders., Verwaltungsrecht in der Informationsgesellschaft – Einleitende Problemskizze, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Wolfgang (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 1, Baden-Baden 2000, S. 9–58.

ders., Gesetz und Gesetzesvorbehalt im Umbruch: Zur Qualitäts-Gewährleistung durch Normen, AöR 2005, S. 5–70.

ders., Kontrolldichte und Kontrollfolgen beim nationalen und europäischen Schutz von Freiheitsrechten in mehrpoligen Rechtsverhältnissen, EuGRZ 2006, S. 492–499.

ders., Wissen, Recht und Innovation, in: Röhl, Hans Christian (Hrsg.), Wissen – zur kognitiven Dimension des Rechts, Berlin 2010, S. 159–211.

ders., Innovation und Recht, Recht und Innovation: Recht im Ensemble seiner Kontexte, 2016.

ders., Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 2017, S. 1–42.

ders., Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data: regulative Herausforderungen, 2018, S. 11–78.

Hofmann, Franz, Prozeduralisierung der Haftungsvoraussetzungen im Medienrecht – Vorbild für die Intermediärshaftung im Allgemeinen? Vortrag auf dem Symposion „Internetplattformen – Aktuelle Herausforderungen der digitalen Ökonomie an das Urheber- und Medienrecht“ am 04.11.2016 in München, ZUM 2017, S. 102–109.

ders., Disziplinarität, Intradisziplinarität und Interdisziplinarität am Beispiel der Grundsätze „mittelbarer Verantwortlichkeit“, JZ 2018, S. 746–754.

ders., Kontrolle oder nachlaufender Rechtsschutz – wohin bewegt sich das Urheberrecht?, GRUR 2018, S. 21–29.

ders., Die Plattformverantwortlichkeit nach dem neuen europäischen Urheberrecht – „Much Ado About Nothing“?, ZUM 2019, S. 617–627.

ders., Fünfzehn Thesen zur Plattformhaftung nach Art. 17 DSM-RL, GRUR 2019, S. 1219–1229.

Hofmann, Johanna M., Dynamische Zertifizierung: Datenschutzrechtliche Zertifizierung nach der Datenschutz-Grundverordnung am Beispiel des Cloud Computing, 2019.

Holleben, Kevin Max von/Knaut, Johannes, Die Zukunft der Auftragsverarbeitung – Privilegierung, Haftung, Sanktionen und Datenübermittlung mit Auslandsbezug unter der DSGVO, CR 2017, S. 299–306.

Hon, W. Kuan/Millard, Christopher/Walden, Ian, Who is responsible for ‚personal data‘ in cloud computing? – The cloud of unknowing, Part 2, IDPL 2012, S. 3–18.

Hong, Mathias, Das NetzDG und die Vermutung für die Freiheit der Rede, Verfassungsblog, Blogeintrag 09.01.2018 (abrufbar unter: https://verfassungsblog.de/das-netzdg-und-die-vermutung-fuer-die-freiheit-der-rede/). Zuletzt abgerufen am 14.01.2022.

Hoofnagle, Chris Jay, Designing for Consent, EuCML 2018, S. 162–171.

Hornung, Gerrit, Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything", in: Roßnagel, Alexander/Friedewald, Michael/Hansen, Marit (Hrsg.), Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung, 2018, S. 316–336.

ders., Erosion traditioneller Prinzipien des Datenschutzrechts durch Big Data, in: Hoffmann-Riem, Wolfgang (Hrsg.), Big Data: regulative Herausforderungen, 2018, S. 79–98.

ders., Mitlauschen bei den lieben Kleinen: Kindeswohl oder Kindesgefährdung?, VuR 2018, S. 41–43.

Hornung, Gerrit/Hartl, Korbinian, Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und Datenschutzaudit, ZD 2014, S. 219–225.

Hufen, Friedhelm, Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbstbestimmung – eine juristische Antwort auf „1984"?, JZ 1984, S. 1072–1078.

Hustinx, Peter, EU-Datenschutzrecht: Die Überprüfung der Richtlinie 95/46/EG und die vorgeschlagene Datenschutz-Grundverordnung, 2014 (abrufbar unter: https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_de). Zuletzt abgerufen am 14.01.2022.

Jacquemain, Tobias, Der deliktische Schadensersatz im europäischen Datenschutzprivatrecht, 2017.

Jandt, Silke, Datenschutz durch Technik in der DS-GVO: Präventive und repressive Vorgaben zur Gewährleistung der Sicherheit der Verarbeitung, DuD 2017, S. 562–566.

dies., Biometrische Videoüberwachung – was wäre wenn …, ZRP 2018, S. 16–19.

Jansen, Nils/Michaels, Ralf, Private Law and the State – Comparative Perceptions and Historical Observations, RabelsZ 2007, S. 345–397.

Jarass, Hans D., Grundrechte als Wertentscheidungen bzw. objektivrechtliche Prinzipien in der Rechtsprechung des Bundesverfassungsgerichts, AöR 1985, S. 363–397.

ders. (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Auflage 2021 (zit. *Bearbeiter*, in: Jarass, Grundrechtecharta).

ders., Die Bedeutung der Unionsgrundrechte unter Privaten, ZEuP 2017, S. 310–334.

Jarovsky, Luiza, Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs), EDPL 2018, S. 447–458.

Jaspers, Andreas/Jacquemain, Tobias, Datenschutz-Grundverordnung – Praxiserfahrungen und Evaluation, DuD 2020, S. 297–301.

Johannes, Paul C./Roßnagel, Alexander, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, 2016.

Jones, Laura, Die urheberrechtliche Haftung von Intermediären im Rechtsvergleich, 2020.

Jotzo, Florian, Der Schutz personenbezogener Daten in der Cloud, 2013.

Jülicher, Tim/Röttgen, Charlotte/von Schönfeld, Max, Das Recht auf Datenübertragbarkeit: Ein datenschutzrechtliches Novum, ZD 2016, S. 358–362.

Kalbhenn, Jan Christopher/Hemmert-Halswick, Maximilian, Der Regierungsentwurf zur Änderung des NetzDG, MMR 2020, S. 518–522.

Kamp, Meike/Rost, Martin, Kritik an der Einwilligung, DuD 2013, S. 80–84.

Karaboga, Murat/Masur, Philipp/Matzner, Tobias/Mothes, Cornelia/Nebel, Maxi/Ochs, Carsten/Schütz, Philip/Fhom, Hervais Simo, Selbstdatenschutz, White Paper des Forums Privatheit, 2014 (abrufbar unter: https://www.forum-privatheit.de/wp-content/

uploads/Forum_Privatheit_White_Paper_Selbstdatenschutz_2.Auflage.pdf). Zuletzt abgerufen am 14.01.2022.

Karg, Moritz, Anmerkung zu VG Schleswig, Urt. v. 09.10.2013, Az. 8 A 14/12, ZD 2014, S: 51–56.

Karpen, Ulrich, Gesetzgebungslehre – neu evaluiert, 2., erweiterte Auflage 2008.

Kartheuser, Ingemaer/Nabulsi, Selma, Abgrenzungsfragen bei gemeinsam Verantwortlichen, MMR 2018, S. 717–721.

Keller, Daphne, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Tech. L. J. 2018, S. 287–364.

Kerber, Wolfgang/Specht-Riemenschneider, Louisa, Synergies between Data Protection Law and Competition Law, 2021 (abrufbar unter: https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf). Zuletzt abgerufen am 14.01.2022.

Kersten, Jens, Anonymität in der liberalen Demokratie, JuS 2017, S. 193–203.

Kian, Bardia, Cloud Computing, 2016.

Kießling, Andrea, Nichtstörer und andere Unbeteiligte als Adressaten von Polizeiverfügungen, JURA 2016, S. 483–494.

King, Jennifer/Lampinen, Airi/Smolen, Alex, Privacy: is there an app for that?, Proceedings of the Seventh Symposium on Usable Privacy and Security – SOUPS '11 2011, S. 1–20.

Kingreen, Thorsten/Poscher, Ralf, Polizei- und Ordnungsrecht: mit Versammlungsrecht, 11. Auflage 2020.

Kipker, Dennis-Kenji/Voskamp, Friederike, Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung, DuD 2012, S. 737–742.

Kischel, Uwe, Die Kontrolle der Verhältnismäßigkeit durch den Europäischen Gerichtshof, EuR 2000, S. 380–402.

Klement, Jan Henrik, Wettbewerbsfreiheit: Bausteine einer europäischen Grundrechtstheorie, 2015.

ders., Öffentliches Interesse an Privatheit, JZ 2017, S. 161–170.

Klonick, Kate, The New Governors: The People, Rules, and Processes Governing Online Speech, Harv. L. Rev. 2018, S. 1599–1670.

Klug, Christoph, Der Datenschutzbeauftragte in der EU: Maßgaben der Datenschutzgrundverordnung, ZD 2016, S. 315–319.

Kluth, Winfried, Die Strukturierung von Wissensgenerierung durch das Verwaltungsorganisationsrecht, in: Spiecker gen. Döhmann, Indra/Collin, Peter (Hrsg.), Generierung und Transfer staatlichen Wissens im System des Verwaltungsrechts, 2008, S. 73–92.

Koch, Oliver, Der Grundsatz der Verhältnismäßigkeit in der Rechtsprechung des Gerichtshofs der Europäischen Gemeinschaften, 2003.

Köhler, Helmut, Datenschutz – eine neue Aufgabe für das Wettbewerbsrecht?, ZD 2019, S. 285–286.

Köhler, Helmut/Bornkamm, Joachim/Feddersen, Jörn (Hrsg.), Gesetz gegen den unlauteren Wettbewerb, 39. Auflage 2021 (zit. *Bearbeiter*, in: Köhler u. a., Gesetz gegen den unlauteren Wettbewerb).

Kokott, J./Sobotta, C., The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, IDPL 2013, S. 222–228.

Kolany-Raiser, Barbara/Radtke, Tristan, Microtargeting – Gezielte Wähleransprache im Wahlkampf, ABIDA-Dossier, 2018 (abrufbar unter: https://www.abida.de/sites/default/files/16_Microtargeting.pdf). Zuletzt abgerufen am 14.01.2022.

Kollmar, Frederike, Umfang und Reichweite gemeinsamer Verantwortlichkeit im Datenschutz, NVwZ 2019, S. 1740–1743.

Koloßa, Stephan, The GDPR's Extra-Territorial Scope, ZaöRV 2020, S. 791–818.

Köndgen, Johannes, Privatisierung des Rechts. Private Governance zwischen Deregulierung und Rekonstitutionalisierung, AcP 2006, 477–525.

Kosyra, Lea/Domurath, Irina, Datenschutz und Rechtsdurchsetzung, in: Micklitz, Hans-Wolfgang/Joost, Gesche/Reisch, Lucia A./Zander-Hayat, Helga (Hrsg.), Verbraucherrecht 2.0 – Verbraucher in der digitalen Welt, 2017, S. 135–172.

Kreimer, Seth F., Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link, Univ. Pa. Law Rev. 2006, S. 11–101.

Kremer, Sascha, Plugins nach dem EuGH: Cookie Consent und Joint Controller überall?, CR 2019, S. 676–688.

Krings, Dennis/Ohrtmann, Jan-Peter, Datenschutz-Folgenabschätzung in der Praxis, DSB 2019, S. 193–195.

Kröger, Jacob Leon/Lindemann, Jens/Herrmann, Dominik, How do app vendors respond to subject access requests?: a longitudinal privacy study on iOS and Android Apps, Proceedings of the 15th International Conference on Availability, Reliability and Security 2020, S. 1–10.

Krönke, Christoph, Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 2016, S. 319–351.

ders., Einführung: Regulierung in Zeiten der Digitalwirtschaft, in: Krönke, Christoph (Hrsg.), Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, 2019, S. 1–10.

Kropp, Alexander, Datenschutzsünder an den Pranger? Die Veröffentlichung von Bußgeld-Adressaten durch die Landesdatenschutzbeauftragten, PinG 2019, S. 220–226.

Kroschwald, Steffen, Kollektive Verantwortung für den Datenschutz in der Cloud: Datenschutzrechtliche Folgen einer geteilten Verantwortlichkeit beim Cloud Computing, ZD 2013, S. 388–394.

Kruse, Frauke, Die verfassungsrechtlichen Grenzen richterlicher Rechtsfortbildung, 2019.

Kuczerawy, Aleksandra, Intermediary liability & freedom of expression: Recent developments in the EU notice & action initiative, CLSR 2015, S. 46–56.

dies., General monitoring obligations: a new cornerstone of Internet regulation in the EU?, in: KU Leuven Centre for IT & IP Law (Hrsg.), Rethinking IT and IP law: celebrating 30 years CiTiP, 2019, S. 141–148.

Kühling, Jürgen, Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung, Die Verwaltung 2007, S. 153–172.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung/BDSG: Kommentar, 3. Auflage 2020 (zit. *Bearbeiter*, in: Kühling/Buchner, DSGVO/BDSG).

Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin/Nink, David/Weinzierl, Quirin/Wenzel, Michael, Die Datenschutz-Grundverordnung und das nationale Recht: Erste Überlegungen zum innerstaatlichen Regelungsbedarf, 2016.

Kuner, Christopher/Cate, Fred H./Millard, Christopher/Svantesson, Dan Jerker B., The challenge of ‚big data' for data protection, IDPL 2012, S. 47–49.

Kuner, Christopher/Bygrave, Lee A./Docksey, Christopher (Hrsg.), The EU General Data Protection Regulation (GDPR): a commentary, 2019 (zit. *Bearbeiter*, in: Kuner u. a., GDPR).

Kurtz, Christian/Wittner, Florian/Semmann, Martin/Schulz, Wolfgang/Böhmann, Tilo, The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems, Proceedings of the 52nd Hawaii International Conference on System Sciences 2019, S. 5059–5068.

Kurtz, Christian/Wittner, Florian/Semmann, Martin/Vogel, Pascal/Böhmann, Tilo, Design Goals for Consent at Scale in Digital Service Ecosystems, Proceedings of the 28th European Conference on Information Systems (ECIS) 2020, S. 1–15.

Landesbeauftragte für den Datenschutz Niedersachsen, 25. Tätigkeitsbericht 2019 (abrufbar unter: https://lfd.niedersachsen.de/download/158404). Zuletzt abgerufen am 14.01.2022.

Lang, Andrej, Netzwerkdurchsetzungsgesetz und Meinungsfreiheit, AöR 2018, S. 220–249.

Lange, Moritz, Zweckveranlassung: ein Beitrag zur Zurechnung des Verhaltens Dritter im Öffentlichen Recht, 2014.

Larenz, Karl/Canaris, Claus-Wilhelm, Methodenlehre der Rechtswissenschaft, 3., neu bearbeitete Auflage 1995.

Laue, Philip, Öffnungsklauseln in der DS-GVO – Öffnung wohin?, ZD 2016, S. 463–467.

Lee, Laureen/Cross, Samuel, (Gemeinsame) Verantwortlichkeit beim Einsatz von Drittinhalten auf Websites, MMR 2019, S. 559–563.

Lee, Sung Une/Zhu, Liming/Ross, Jeffery, Data Governance Decisions for Platform Ecosystems, Proceedings of the 52nd Hawaii International Conference on System Sciences 2019, S. 6377–6386.

Leenes, Ronald, Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology, Legisprudence 2012, S. 144–169.

Lennartz, Jannis, Verfassungsrechtliche Grenzen der Indienstnahme Privater, DÖV 2019, S. 434–440.

Lepperhoff, Niels/Petersdorf, Björn/Thursch, Sabine, Datenschutzverstöße und Vollzugsdefizite: Ergebnisse des Datenschutzbarometers 2011, DuD 2012, S. 195–199.

Lepsius, Oliver, Ziele der Regulierung, in: Fehling, Michael/Ruffert, Matthias (Hrsg.), Regulierungsrecht, 2010, S. 1055–1086.

Lessig, Lawrence, Code and other laws of cyberspace, 1999.

Lewinski, Kai von, Die Matrix des Datenschutzes: Besichtigung und Ordnung eines Begriffsfeldes, 2014.

Li, Peixuan/Zhang, Danfeng, Towards a Flow- and Path-Sensitive Information Flow Analysis, IEEE 30th Computer Security Foundations Symposium (CSF) 2017, S. 53–67.

Libert, Timothy/Nielsen, Rasmus Kleis, Third-Party Web Content on EU News Sites: Potential Challenges and Paths to Privacy Improvement, Report des Reuters Institute for the Study of Journalism, 2018 (abrufbar unter: https://ora.ox.ac.uk/objects/uuid:c57241a8-f520-46e5-9e1a-8e4a7f66c23b). Zuletzt abgerufen am 14.01.2022.

Liesching, Marc, Lösungsmodell regulierter Selbstregulierung – Zur Übertragbarkeit der JMStV-Regelungen auf das NetzDG, in: Eifert, Martin/Gostomzyk, Tobias (Hrsg.), Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, 2018, S. 135–152.

Liesem, Kerstin, Neulandvermessung – Die Regulierung von Medienintermediären im neuen Medienstaatsvertrag, ZUM 2020, S. 377–382.

Lindqvist, Jenna, New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?, Int J Law Info Tech 2018, S. 45–63.

Lindroos-Hovinheimo, Susanna, Who controls our data? The legal reasoning of the European Court of Justice in Wirtschaftsakademie Schleswig-Holstein and Tietosuojavaltuutettu v Jehovan todistajat, Information & Communications Technology Law 2019, S. 225–238.

Lorentz, Nora, Profiling – Persönlichkeitsschutz durch Datenschutz?, 2020.

Lüdemann, Jörn, Privatisierung der Rechtsdurchsetzung in sozialen Netzwerken?, in: Eifert, Martin/Gostomzyk, Tobias (Hrsg.), Netzwerkrecht: Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, 2018, S. 153–168.

Lurger, Brigitta, Die Dominanz zwingenden Rechts – die vermeintlichen und tatsächlichen Schattenseiten des EU-Verbraucherschutzrechts, ZEuP 2018, S. 788–820.

Lurtz, Helmut, Die Vorkehrungen für die „Abmahnwelle", ZD-Aktuell 2018, 06292.

Lynskey, Orla, Deconstructing Data Protection: The ‚Added-Value' of a Right to Data Protection in the EU Legal Order, ICLQ 2014, S. 569–597.

dies., The foundations of EU data protection law, 2015.

dies., Regulating ‚Platform Power', LSE Law, Society and Economy Working Papers 01/2017 (abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921021). Zuletzt abgerufen am 14.01.2022.

Mahieu, René/van Hoboken, Joris/Asghari, Hadi, Responsibility for Data Protection in a Networked World: On the Question of the Controller, „Effective and Complete Protection" and its Application to Data Access Rights in Europe, jipitec 2019, S. 85–105.

Maisch, Michael Marc, Informationelle Selbstbestimmung in Netzwerken: Rechtsrahmen, Gefährdungslagen und Schutzkonzepte am Beispiel von Cloud Computing und Facebook, 2015.

Mantz, Reto, Störerhaftung für Datenschutzverstöße Dritter: Sperre durch DS-RL und DS-GVO?, ZD 2014, S. 62–66.

Marosi, Johannes, Mehrstufige Anbieterverhältnisse im Datenschutz: letzte Station Unionsrecht?, K&R 2016, S. 389–392.

ders., Fanpages vor dem Bundesverwaltungsgericht: Kein Fan, Telemedicus, Blogbeitrag vom 27.02.2016 (abrufbar unter: http://www.telemedicus.info/article/3056-Fanpages-vor-dem-Bundesverwaltungsgericht-Kein-Fan.html). Zuletzt abgerufen am 14.01.2022.

ders., Fanpages vor dem EuGH – Keiner will's gewesen sein, JuWiss-Blog, Blogbeitrag vom 25.07.2017 (abrufbar unter: https://www.juwiss.de/87-2017/). Zuletzt abgerufen am 14.01.2022.

ders., Who controls the controllers? – Datenschutzrechtliche Verantwortlichkeit und Internet-Infrastruktur nach EuGH C-210/16, in: Maute, Lena/Mackenrodt, Mark-Oliver (Hrsg.), Recht als Infrastruktur für Innovation, 2019, S. 245–264.

Marosi, Johannes/Matthé, Luisa, Anmerkung zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388, ZD 2018, S. 357–365.

Marsch, Nikolaus, Das europäische Datenschutzgrundrecht: Grundlagen – Dimensionen – Verflechtungen, 2018.

Martensen, Jürgen, Materielle Polizeipflicht und polizeiliche Verpflichtbarkeit des Bürgers in Anscheins- und Verdachtslagen, DVBl 1996, S. 286–292.

Martin, Kirsten/Nissenbaum, Helen, What Is It About Location?, Berkeley Tech. L. J. 2020, S. 253–326.

Martini, Mario, Do it yourself im Datenschutzrecht: Der „GeoBusiness Code of Conduct" als Erprobungsfeld regulierter Selbstregulierung, NVwZ-Extra 2016, S. 1–13.

ders., Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, S. 1017–1025.

Martini, Mario/Fritzsche, Saskia, Mitverantwortung in sozialen Netzwerken – Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, NVwZ-Extra 2015, S. 1–16.

Martini, Mario/Weinzierl, Quirin, Mandated Choice: der Zwang zur Entscheidung auf dem Prüfstand von Privacy by Default (Art. 25 Abs. 2 S. 1 DSGVO), RW 2019, S. 287–316.

Martini, Mario/Wenzel, Michael, „Gelbe Karte" von der Aufsichts behörde: die Verwarnung als daten- schutzrechtliches Sanktionenhybrid, PinG 2017, S. 92–96.

Masing, Johannes, Die Mobilisierung des Bürgers für die Durchsetzung des Rechts: europäische Impulse für eine Revision der Lehre vom subjektiv-öffentlichen Recht, 1997.

Matejek, Michael/Mäusezahl, Steffen, Gewöhnliche vs. sensible personenbezogene Daten, ZD 2019, S. 551–556.

Mathiassen, Lars/Sørensen, Carsten, Towards a Theory of Organizational Information Services, Journal of Information Technology 2008, S. 313–329.

Matzner, Tobias, Why privacy is not enough privacy in the context of „ubiquitous computing" and „big data", JICES 2014, S. 93–106.

Mayer, Christian, Die Nachbesserungspflicht des Gesetzgebers, 1996.

Mayer, Jonathan R./Mitchell, John C., Third-Party Web Tracking: Policy and Technology, IEEE Symposium on Security and Privacy 2012, S. 413–427.

Mayer-Schönberger, Viktor, Delete: die Tugend des Vergessens in digitalen Zeiten, 3. Auflage 2015.

Mayer-Schönberger, Viktor/Padova, Yann, Regime change? Enabling Big Data through Europe's new General Data Protection Regulation, Colum. Sci. & Tech. L. Rev. 2016, S. 315–335.

McDonald, Aleecia M./Cranor, Lorrie Faith, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society, S. 543–564.

Meller-Hannich, Caroline/Krausbeck, Elisabeth/Wittke, René, Der Verbraucher in der Sharing Economy, VuR 2019, S. 403–412.

Meyer, Jürgen/Hölscheidt, Sven (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Auflage 2019 (zit. *Bearbeiter*, in: Meyer/Hölscheidt, GRCH).

Meyer-Ladewig, Jens/Nettesheim, Martin/von Raumer, Stefan (Hrsg.), EMRK: Europäische Menschenrechtskonvention: Handkommentar, 4. Auflage 2017 (zit. *Bearbeiter*, in: Meyer-Ladewig u. a., EMRK).

Millard, Christopher, At this rate, everyone will be a [joint] controller of personal data!, IDPL 2019, S. 217–219.

Moran, Stuart/Luger, Ewa/Rodden, Tom, Literatin: beyond awareness of readability in terms and conditions, Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct Publication 2014, S. 641–646.

Moser-Knierim, Antonie, „Facebook-Login" – datenschutzkonformer Einsatz möglich? Einsatz von Social Plug-ins bei Authentifizierungsdiensten, ZD 2013, S. 263–266.

Möstl, Markus, Die staatliche Garantie für die öffentliche Sicherheit und Ordnung: Sicherheitsgewährleistung im Verfassungsstaat, im Bundesstaat und in der Europäischen Union, 2002.

Müller, Daniel, Cloud Computing: Strafrechtlicher Schutz privater und geschäftlicher Nutzerdaten vor Innentäter-Angriffen de lege lata und de lege ferenda, 2020.

Müller, Friedrich/Christensen, Ralph, Juristische Methodik, Band I: Grundlagen Öffentliches Recht, 9., neu bearbeitete und stark erweiterte Auflage 2004.

Müller-Brehm, Jana, Forschungsstand: Microtargeting in Deutschland und Europa – Fehlende Transparenz und viele offene Fragen, Bericht des iRights.Lab für die Landesanstalt für Medien NRW, 2019, (abrufbar unter: https://www.medienanstalt-nrw.de/fileadmin/user_upload/lfm-nrw/Foerderung/Forschung/Dateien_Forschung/Forschungsmonitoring_Microtargeting_Deutschland_Europa.pdf). Zuletzt abgerufen am 14.01.2022.

Müller-Terpitz, Ralf, Einbindung von Intermediären in das medienrechtliche System der Vielfaltssicherung, AfP 2017, S. 380–384.

Murray, Andrew/Scott, Colin, Controlling the New Media: Hybrid Responses to New Forms of Power, The Modern Law Review 2002, S. 491–516.

Murswiek, Dietrich, Die staatliche Verantwortung für die Risiken der Technik: verfassungsrechtliche Grundlagen und immissionsschutzrechtliche Ausformung, 1985.

Nanevski, Aleksandar/Banerjee, Anindya/Garg, Deepak, Verification of Information Flow and Access Control Policies with Dependent Types, IEEE Symposium on Security and Privacy 2011, S. 165–179.

Nettesheim, Martin/Diggelmann, Oliver/Lege, Joachim (Hrsg.), Der Schutzauftrag des Rechts, Referate und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Berlin vom 29. September bis 2. Oktober 2010, 2011 (zit. *Bearbeiter*, in: Nettesheim u. a., VVDStRL 70).

Neun, Andreas/Lubitzsch, Katharina, EU-Datenschutz-Grundverordnung – Behördenvollzug und Sanktionen, BB 2017, S. 1538–1544.

Nieborg, David/Poell, Thomas, The platformization of cultural production: Theorizing the contingent cultural commodity, New Media & Society 2018, S. 4275–4292.

Nissenbaum, Helen, Privacy in context: technology, policy, and the integrity of social life, 2010.

Nolde, Malaika, Sanktionen nach DSGVO und BDSG-neu: Wem droht was warum?, PinG 2017, S. 114–121.

Noll, Peter, Gesetzgebungslehre, 1973.

Nolte, Georg/Wimmers, Jörg, Wer stört? Gedanken zur Haftung von Intermediären im Internet – von praktischer Konkordanz, richtigen Anreizen und offenen Fragen, GRUR 2014, S. 16–27.

Norwegischer Verbraucherrat (Forbrukerrådet), Out of Control: How consumers are exploited by the online advertising industry, 2020 (abrufbar unter: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf). Zuletzt abgerufen am 14.01.2022.

Odlyzko, Andrew, Privacy, Economics, and Price Discrimination on the Internet, in: Camp, L. Jean/Lewis, Stephen (Hrsg.), Economics of information security, 2004, S. 187–211.

Ohly, Ansgar, Die Verantwortlichkeit von Intermediären, ZUM 2015, 308 – S. 318.

ders., Die Haftung von Internet-Dienstleistern für die Verletzung lauterkeitsrechtlicher Verkehrspflichten, GRUR 2017, S. 441–451.

ders., UWG-Rechtsschutz bei Verstößen gegen die Datenschutz-Grundverordnung?, GRUR 2019, S. 686–693.

Oliveira, Marcelo Iury S./Lóscio, Bernadette Farias, What is a data ecosystem?, Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age 2018, S. 1–9.

Ondrus, Jan/Gannamaneni, Avinash/Lyytinen, Kalle, The Impact of Openness on the Market Potential of Multi-Sided Platforms: A Case Study of Mobile Payment Platforms, Journal of Information Technology 2015, S. 260–275.

Oostveen, Manon, Why privacy ≠ data protection (and how they overlap), HIIG Digital Society Blog, Blogbeitrag vom 04.05.2016 (abrufbar unter: https://www.hiig.de/en/why-privacy-≠-data-protection-and-how-they-overlap/). Zuletzt abgerufen am 14.01.2022.

Ossenbühl, Fritz, Die Kontrolle von Tatsachenfeststellungen und Prognoseentscheidungen durch das Bundesverfassungsgericht, in: Starck, Christian/Drath, Martin (Hrsg.), Bundesverfassungsgericht und Grundgesetz: Festgabe aus Anlaß des 25-jährigen Bestehens des Bundesverfassungsgerichts, 1976, S. 458–518.

Otten, Wolfgang, Eigensicherung: Möglichkeiten und Grenzen einer Verpflichtung Privater zur Sicherung gegen Einwirkungen Dritter unter besonderer Berücksichtigung des Atomrechts, 2006.

Paal, Boris P., Datenschutz – Regulierung – Wettbewerb: Online-Plattformen als Referenzgebiet, in: Körber, Torsten/Kühling, Jürgen (Hrsg.), Regulierung – Wettbewerb – Innovation, 2017, S. 143–164.

ders., Vielfaltssicherung bei Intermediären, MMR 2018, S. 567–572.

ders., Schadensersatzansprüche bei Datenschutzverstößen, MMR 2020, S. 14–19.

Paal, Boris P./Heidtke, Aron, Vielfaltssichernde Regulierung der Medienintermediäre nach den Vorschriften des Medienstaatsvertrags der Länder, ZUM 2020, S. 230–240.

Paal, Boris P./Hennemann, Moritz, Big Data im Recht, NJW 2017, S. 1697–1701.

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Beck'sche Kompakt-Kommentare Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Auflage 2021 (zit. *Bearbeiter*, in Paal/Pauly, DSGVO/BDSG).

Parker, Christine, Meta-regulation: legal accountability for corporate social responsibility, in: McBarnet, Doreen J./Voiculescu, Aurora/Campbell, Tom (Hrsg.), The new corporate accountability: corporate social responsibility and the law, 2007, S. 207–237.

Parker, Geoffrey/van Alstyne, Marshall, Platform Strategy, in: Augier, Mie/Teece, David J. (Hrsg.), The Palgrave encyclopedia of strategic management, 2018, S. 1290–1298.

Pasquale, Frank, The black box society: the secret algorithms that control money and information, 2015.

Paterson, Moira/McDonagh, Maeve, Data Protection In An Era Of Big Data: The Challenges Posed By Big Personal Data, Monash University Law Review 2018, S. 1–32.

Paun, Mara, On the Way to Effective and Complete Protection (?): Some Remarks on Fashion ID, EuCML 2020, S. 35–37.

Peers, Steve/Hervey, Tamara/Kenner, Jeff/Ward, Angela (Hrsg.), The EU Charter of Fundamental Rights, 2014 (zit. *Bearbeiter*, in: Peers u. a., The EU Charter of Fundamental Rights).

Peppet, Scott R, Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future, Northwestern University Law Review 2011, S. 1153–1203.

Perel, Maayan, Digital Remedies, Berkeley Tech. L. J. 2020, S. 1–52.

Petri, Thomas, Auftragsdatenverarbeitung – heute und morgen: Reformüberlegungen zur Neuordnung des Europäischen Datenschutzrechts, ZD 2015, S. 305–309.
ders., Anmerkung zu LG Düsseldorf, Urt. v. 09.03.2016, Az. 12 O 151/15, ZD 2016, S. 231–234.
ders., Anmerkung zu BVerwG, Beschl. v. 25.02.2016, Az. 1 C 28.14, ZD 2016, S. 393–399.
ders., Anmerkung zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388, EuZW 2018, S. 534–541.
Petrlic, Ronald/Sorge, Christoph, Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, 2017.
Peuker, Enrico, Verfassungswandel durch Digitalisierung, 2020.
Pfeifle, Anne, Alexa, what should we do about privacy? Protection privacy for users of voice-activated devices, Washington Law Review 2018, S. 421–458.
Picker, Eduard, Privatrechtssystem und negatorischer Rechtsschutz, 2., veränderte Auflage 2019.
Piltz, Carlo, Der Like-Button von Facebook, CR 2011, S. 657–664.
ders., Störerhaftung im Datenschutzrecht?, K&R 2014, S. 80–85.
ders., OLG Dresden: Kein Schadensersatz und Schmerzensgeld für Bagatellverstöße gegen die DSGVO, de lege data, Blogbeitrag vom 04.07.2019 (abrufbar unter https://www.delegedata.de/2019/07/olg-dresden-kein-schadensersatz-und-schmerzensgeld-fuer-bagatellverstoesse-gegen-die-dsgvo/). Zuletzt abgerufen am 14.01.2022.
Plath, Kai-Uwe (Hrsg.), DSGVO/BDSG: Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen von TMG und TKG, 3. Auflage 2018 (zit. *Bearbeiter*, in: Plath, DSGVO/BDSG).
Podszun, Rupprecht, Der Verbraucher als Marktakteur: Kartellrecht und Datenschutz in der „Facebook"-Entscheidung des BGH, GRUR 2020, S. 1268–1276.
Podszun, Rupprecht/de Toma, Michael, Die Durchsetzung des Datenschutzes durch Verbraucherrecht, Lauterkeitsrecht und Kartellrecht, NJW 2016, S. 2987–2994.
Pohl, Dirk, Durchsetzungsdefizite der DSGVO? Der schmale Grat zwischen Flexibilität und Unbestimmtheit, PinG 2017, S. 85–91.
Pohle, Jörg, Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung, 2018.
Polenz, Sven, Die Datenverarbeitung durch und via Facebook auf dem Prüfstand, VuR 2012, S. 207–213.
Pollmann, Tobias, A Comparative Law and Economics Analysis of the Proposed German „Model Declaratory Action", Master thesis for the European Master in Law and Economics (EMLE), 2018 (abrufbar unter: https://emle.org/wp-content/uploads/2019/07/EMLE-Thesis-Pollmann-Tobias_Website.pdf). Zuletzt abgerufen am 14.01.2022.
Poscher, Ralf, Die gefahrenabwehrrechtliche Verantwortlichkeit – Zugleich ein Beitrag zur Lehre von der rechtswidrigen Verursachung, JURA 2007, S. 801–810.
ders. Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander, Hans-Helmuth/Perron, Walter/Poscher, Ralf/Riescher, Gisela/Würtenberger, Thomas (Hrsg.), Resilienz in der offenen Gesellschaft: Symposium des Centre for Security and Society, 2012, S. 167–190.
ders., The Right to Data Protection, in: Miller, Russell A. (Hrsg.), Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, 2017, S. 129–142.
Purtova, Nadezhda, The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology 2018, S. 40–81.

Rademacher, Timo, Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?, JZ 2019, S. 702–710.

Raso, Filippo A., Innovating in uncertainty: effective compliance and the GDPR, Harvard Journal of Law & Technology Digest 2018, S. 1–12.

Raue, Benjamin/Steinebach, Martin, Uploadfilter – Funktionsweisen, Einsatzmöglichkeiten und Parametrisierung: Vortrag auf dem Symposium „FILTER(N) oder nicht? Der Einsatz von Filtertechnologien im Urheber- und Medienrecht" des Instituts für Urheber- und Medienrecht am 07.02.2020 in München, ZUM 2020, S. 355–364.

Reifert, Natascha, Codes of Conduct nach der DS-GVO: Ein Mittel für mehr Rechtssicherheit auf europäischer Ebene?, ZD 2019, S. 305–310.

Reinhardt, Jörn, Konturen des europäischen Datenschutzgrundrechts: Zu Gehalt und horizontaler Wirkung von Art. 8 GRCh, AöR 2017, 528–565.

Reuver, Mark de/Sørensen, Carsten/Basole, Rahul C., The Digital Platform: A Research Agenda, Journal of Information Technology 2018, S. 124–135.

Richter, Philipp, Datenschutz durch Technik und die Grundverordnung der EU-Kommission, DuD 2012, S. 576–580.

ders., Instrumente zwischen rechtlicher Steuerung und technischer Entwicklung, DuD 2016, S. 89–93.

Riedel, Christian G. H., Die Grundrechtsprüfung durch den EuGH, 2020.

Ritter, Franziska/Reibach, Boris/Lee, Morris, Lösungsvorschlag für eine praxisgerechte Risikobeurteilung von Verarbeitungen, ZD 2019, S. 531–535.

Robinson, Neil, Has European Data Protection Law Become Outdated?, MMR 2009, S. 725–726.

Rochet, Jean-Charles/Tirole, Jean, Platform Competition in Two-Sided Markets, Journal of the European Economic Association 2003, S. 990–1029.

Rodotà, Stefano, Data Protection as a Fundamental Right, in: Gutwirth, Serge/Poullet, Yves/de Hert, Paul/de Terwangne, Cécile/Nouwt, Sjaak (Hrsg.), Reinventing data protection?, 2009, S. 77–82.

Rössler, Beate, Der Wert des Privaten, 2001.

Roßnagel, Alexander, Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger, ZRP 1997, S. 27–30.

ders., Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, S. 71–75.

ders., Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, 2007 (abrufbar unter: https://library.fes.de/pdf-files/stabsabteilung/04548.pdf). Zuletzt abgerufen am 14.01.2022.

ders., „Technikneutrale" Regulierung: Möglichkeiten und Grenzen, in: Eifert, Martin/Hoffmann-Riem, Wolfgang (Hrsg.), Innovationsfördernde Regulierung, 2008, S. 323–337.

ders., Zusätzlicher Arbeitsaufwand für die Aufsichtsbehörden der Länder durch die Datenschutz-Grundverordnung, Gutachten im Auftrag der Aufsichtsbehörden der Länder, 2017 (abrufbar unter: https://www.datenschutzzentrum.de/uploads/dsgvo/2017-Rossnagel-Gutachten-Aufwand-Datenschutzbehoerden.pdf). Zuletzt abgerufen am 14.01.2022.

ders., Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, S. 1–5.

ders., Technik, Recht und Macht: Aufgabe des Freiheitsschutzes in Rechtsetzung und -anwendung im Technikrecht, MMR 2020, S. 222–228.

ders., Evaluation der Datenschutz-Grundverordnung: Verfahren – Stellungnahmen – Vorschläge, DuD 2020, S. 287–292.

ders., Die Evaluation der Datenschutz-Grundverordnung, MMR 2020, S. 657–661.

Roßnagel, Alexander/Geminn, Christian, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht, Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e. V. (vzbv), 2019 (abrufbar unter: https://www.vzbv.de/sites/default/files/downloads/2019/12/04/19-11-26_gutachten_evaluation_dsgvo.pdf). Zuletzt abgerufen am 14.01.2022.

Roßnagel, Alexander/Geminn, Christian L./Jandt, Silke, Datenschutzrecht 2016 – „Smart" genug für die Zukunft? Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts, 2016.

Rouvroy, Antoinette/Poullet, Yves, The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy, in: Gutwirth, Serge/Poullet, Yves/de Hert, Paul/de Terwangne, Cécile/Nouwt, Sjaak (Hrsg.), Reinventing data protection?, 2009, S. 45–76.

Rubinstein, Ira S./Good, Nathaniel, The trouble with Article 25 (and how to fix it): the future of data protection by design and default, IDPL 2020, S. 37–56.

Ruffert, Matthias, Vorrang der Verfassung und Eigenständigkeit des Privatrechts: eine verfassungsrechtliche Untersuchung zur Privatrechtswirkung des Grundgesetzes, 2001.

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina (Hrsg.), Münchener Kommentar zum Bürgerlichen Gesetzbuch: Band 7: Schuldrecht – besonderer Teil IV, 8. Auflage 2020 (zit. *Bearbeiter*, in: MüKo BGB Band VII).

Sahl, Jan Christian/Bielzer, Nils, NetzDG 2.0 – Ein Update für weniger Hass im Netz, ZRP 2020, S. 2–5.

Sandfuchs, Barbara, Privatheit wider Willen? Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht, 2015.

Schäfer, Hans-Bernd/Ott, Claus, Lehrbuch der ökonomischen Analyse des Zivilrechts, 6., aktualisierte Auflage 2020.

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, S. 1841–1847.

Schiedermair, Stephanie, Der Schutz des Privaten als internationales Grundrecht, 2012.

Schipper, Malte, Neue Instrumente des Datenschutzrechts für das Verhältnis zwischen Privatperson und Unternehmen in der Bundesrepublik Deutschland und den Vereinigten Staaten von Amerika, 2003.

Schlaich, Klaus, Die Verfassungsgerichtsbarkeit im Gefüge der Staatsfunktionen, in: Die Verfassungsgerichtsbarkeit im Gefüge der Staatsfunktionen. Besteuerung und Eigentum, Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer zu Innsbruck vom 01. bis 04. Oktober 1980, Reprint 2012.

Schmid, Christoph U., Die Instrumentalisierung des Privatrechts durch die Europäische Union: Privatrecht und Privatrechtskonzeptionen in der Entwicklung der Europäischen Integrationsverfassung, 2010.

Schmid, Daniel, Die Nutzung von Cloud-Diensten durch kleine und mittelständische Unternehmen, 2017.

Schmidt, Manfred G., Demokratietheorien: Eine Einführung, 6. Auflage 2019.

Schmidt-Preuß, Matthias, Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, in: Hailbronner, Kay (Hrsg.), Kontrolle

der auswärtigen Gewalt: Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, 1997, S. 160–227.

Schmitz, Barbara/von Dall'Armi, Jonas, Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung? Wie Daten künftig von Dienstleistern verarbeitet werden müssen, ZD 2016, S. 427–432.

Schneider, Jochen, Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, S. 303–308.

Schneider, Nadine/Kremer, Sascha, Keine Macht den Plattformen? Zur neuen P2B-Verordnung, WRP 2020, S. I–I.

Schoch, Friedrich, Die Notstandspflicht im Polizei- und Ordnungsrecht, JURA 2007, S. 676–684.

ders., Der Zweckveranlasser im Gefahrenabwehrrecht, JURA 2009, S. 360–366.

ders., Kapitel 1. Polizei- und Ordnungsrecht, in: Schoch, Friedrich (Hrsg.), Besonderes Verwaltungsrecht, 2019, S. 11–301.

Scholz, Rupert/Pitschas, Rainer, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, 1984.

Schönefeld, Jana/Thomé, Sarah, Auswirkungen der Datenschutz- Grundverordnung auf die Sanktionierungspraxis der, PinG 2017, S. 126–128.

Schönherr, Lea/Golla, Maximilian/Eisenhofer, Thorsten/Wiele, Jan/Kolossa, Dorothea/Holz, Thorsten, Unacceptable, where is my privacy? Exploring Accidental Triggers of Smart Speakers, arXiv:2008.00508 [cs] 2020.

Schreiber, Kristina, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden, ZD 2019, S. 55–60.

Schreiber, Marlene, Wettbewerbsrechtliche Abmahnung von Konkurrenten wegen Verstößen gegen DS-GVO, GRUR-Prax. 2018, S. 371–373.

Schröder, Heinrich J., Zur Erfolgskontrolle der Gesetzgebung, in: Rehbinder, Manfred/Schelsky, Helmut (Hrsg.), Zur Effektivität des Rechts, 1972, S. 271–288.

Schröder, Markus, Datenschutz als Wettbewerbsvorteil – Es ist an der Zeit!, ZD 2012, S. 193–194.

ders., Der risikobasierte Ansatz in der DS-GVO, ZD 2019, S. 503–506.

Schröder, Meinhard, Private statt administrativer Durchsetzung des öffentlichen Rechts?, Die Verwaltung 2017, S. 309–337.

ders. ‚Paradigm Shift' im Datenschutzrecht? – Wirtschaftsverwaltungsrechtliche Instrumente in der Datenschutz-Grundverordnung, in: Krönke, Christoph (Hrsg.), Regulierung in Zeiten der Digitalwirtschaft: ausgewählte Fragen des Öffentlichen Wirtschafts-, Informations- und Medienrechts, 2019, S. 13–27.

Schulz, Sebastian, Privacy by Design, CR 2012, S. 204–208.

Schulz, Sönke E., Anmerkung zu EuGH, Rs. C-210/16 (Wirtschaftsakademie Schleswig-Holstein), ECLI:EU:C:2018:388, ZD 2018, S. 357–365.

Schulz, Wolfgang, Roles and Responsibilities of Information Intermediaries, Aegis series Paper no. 1904, 2019 (abrufbar unter: https://www.hoover.org/sites/default/files/research/docs/schulz_webreadypdf.pdf). Zuletzt abgerufen am 14.01.2022.

Schulz, Wolfgang/Dankert, Kevin, Informationsintermediäre – Anknüpfungspunkte für rechtliche Regulierung, Informatik-Spektrum 2017, S. 351–354.

Schulz, Wolfgang/Held, Thorsten, Regulierte Selbstregulierung als Form modernen Regierens, Gutachten im Auftrag des Bundesbeauftragten für Angelegenheiten der Kultur und der Medien, 2002 (abrufbar unter: https://www.hans-bredow-institut.de/

uploads/media/Publikationen/cms/media/a80e5e6dbc2427639ca0f437fe76d3c4c95634ac.pdf). Zuletzt abgerufen am 14.01.2022.

Schulz, Wolfgang/Wittner, Florian/Bavendiek, Kai/Schupp, Sibylle, Modelling and Verification in GDPR's Data Protection Impact Assessment: A Case Study on the AccuWeather/Reveal Mobile Case, in: Leenes, Ronald/Hallinan, Dara/Gutwirth, Serge/de Hert, Paul (Hrsg.), Data protection and privacy: data protection and democracy, 2020, S. 145–172.

Schunicht, Barbara Elisabeth, Informationelle Selbstbestimmung in sozialen Netzwerken: mehrseitige Rechtsbeziehungen und arbeitsteilige Verantwortungsstrukturen als Herausforderung für das europäisierte Datenschutzrecht, 2018.

Schuppert, Gunnar Folke, Was ist und wozu Governance?, Die Verwaltung 2007, S. 463–512.

ders., Governance und Rechtsetzung: Grundfragen einer modernen Regelungswissenschaft, 2011.

ders., Wissen, Governance, Recht.: Von der kognitiven Dimension des Rechts zur rechtlichen Dimension des Wissens, 2019.

Schwabenbauer, Thomas, Legislative Reaktionen auf Risiken, in: Dalibor, Marcel/Fröhlich, Katja/Rodi, Katja/Schächterle, Paul/Scharrer, Jörg (Hrsg.), Risiko im Recht – Recht im Risiko: 50. Assistententagung Öffentliches Recht, Greifswald 2010, 2011, S. 157–176.

Schweitzer, Heike, Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen, in: Körber, Torsten/Kühling, Jürgen (Hrsg.), Regulierung – Wettbewerb – Innovation, 2017, S. 269–306.

dies., Vertragsfreiheit, Marktregulierung, Marktverfassung: Privatrecht als dezentrale Koordinationsordnung, AcP 2020, S. 544–586.

Schwemer, Sebastian Felix, Trusted notifiers and the privatization of online enforcement, CLSR 2019, 105339.

Schwichtenberg, Simon, „Doppeltes Netz" im Datenschutz? Die Rolle der Verbraucherverbände unter der DSGVO, PinG 2017, S. 104–108.

Seibel, Mark, Abgrenzung der „allgemein anerkannten Regeln der Technik" vom „Stand der Technik", NJW 2013, S. 3000–3004.

Selzer, Annika, Datenschutzrechtliche Zulässigkeit von Cloud-Computing-Services und deren teilautomatisierte Überprüfbarkeit: eine Betrachtung unter Anwendung der Datenschutz-Grundverordnung, 2020.

Sicko, Corinna, Gesetzesfolgenabschätzung und -evaluation: Ein Beitrag zum besseren Umgang mit dem Risikofaktor Recht, in: Dalibor, Marcel/Fröhlich, Katja/Rodi, Katja/Schächterle, Paul/Scharrer, Jörg (Hrsg.), Risiko im Recht – Recht im Risiko: 50. Assistententagung Öffentliches Recht, Greifswald 2010, 2011, S. 199–223.

Simitis, Spiros, Chancen und Gefahren der elektronischen Datenverarbeitung, NJW 1971, S. 673–682.

ders., Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S. 398–405.

ders., Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, S. 281–288.

ders. (Hrsg.), Bundesdatenschutzgesetz, 8., neu bearbeitete Auflage 2014 (zit. *Bearbeiter*, in: Simitis, BDSG).

Simitis, Spiros/Hornung, Gerrit/Spiecker gen. Döhmann, Indra/Albrecht, Jan Philipp (Hrsg.), Datenschutzrecht: DSGVO/BDSG, 2019 (zit. *Bearbeiter*, in: Simitis u. a., DSGVO/BDSG).

Singh, Jatinder/Cobbe, Jennifer/Norval, Chris, Decision Provenance: Harnessing Data Flow for Accountable Systems, IEEE Access 2019, S. 6562–6574.

Skog, Daniel A./Wimelius, Henrik/Sandberg, Johan, Digital Service Platform Evolution: How Spotify Leveraged Boundary Resources to Become a Global Leader in Music Streaming, Proceedings of the 51st Hawaii International Conference on System Sciences 2018, S. 4564–4573.

Sloot, Bart van der, Legal Fundamentalism: Is Data Protection Really a Fundamental Right?, in: Leenes, Ronald/van Brakel, Rosamunde/Gutwirth, Serge/Hert, Paul de (Hrsg.), Data Protection and Privacy: (In)visibilities and Infrastructures, 2017, S. 3–30.

Smeddinck, Ulrich, Gesetzesfolgenabschätzung und Umweltverträglichkeitsprüfung, DÖV 2004, S. 103–110.

Smulders, Ben/Paquet, Jean-Eric, The European Commission and its Better Regulation Agenda, in: Garben, Sacha/Govaere, Inge (Hrsg.), The EU better regulation agenda: a critical assessment, 2018, S. 79–103.

Solove, Daniel J., A Taxonomy of Privacy, Univ. Pa. Law Rev. 2006, S. 477–564.

ders., Privacy Self Management and the Consent Dilemma, Harv. L. Rev. 2013, S. 1880–1903.

Sørensen, Jannick/Kosta, Sokol, Before and After GDPR: The Changes in Third Party Presence at Public and Private European Websites, WWW '19: The World Wide Web Conference 2019, S. 1590–1600.

Sousa, Pedro Caro de, Horizontal Expressions of Vertical Desires: Horizontal Effect and the Scope of the EU Fundamental Freedoms, Cambridge Journal of International and Comparative Law 2013, S. 479–505.

Specht, Louisa, Zum Verhältnis von (Urheber-)Recht und Technik, GRUR 2019, S. 253–259.

Specht-Riemenschneider, Louisa/Schneider, Ruben, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, S. 503–509.

Spiecker gen. Döhmann, Indra, Kontexte der Demokratie: Parteien, Medien und Sozialstrukturen, in: Jestaedt, Matthias (Hrsg.), Fragmentierungen: Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Saarbrücken vom 04.–07. Oktober 2017, 2018, S. 9–66.

Spindler, Gerald, Selbstregulierung und Zertifizierungsverfahren nach der DS-GVO: Reichweite und Rechtsfolgen der genehmigten Verhaltensregeln, ZD 2016, S. 407–414.

ders., Rechtsdurchsetzung von Persönlichkeitsrechten, GRUR 2018, S. 365–373.

ders., Die neue Urheberrechts-Richtlinie der EU, insbesondere „Upload-Filter" – Bittersweet?, CR 2019, S. 277–291.

Spindler, Gerald/Schmitz, Peter/Liesching, Marc (Hrsg.), Telemediengesetz mit Netzwerkdurchsetzungsgesetz: Kommentar, 2. Auflage 2018 (zit. *Bearbeiter*, in: Spindler u. a., TMG/NetzDG).

Spindler, Gerald/Schuster, Fabian (Hrsg.), Recht der elektronischen Medien: Kommentar, 4. Auflage 2019 (zit. *Bearbeiter*, in: Spindler/Schuster, Recht der elektronischen Medien).

Spindler, Gerald/Thorun, Christian, Die Rolle der Ko-Regulierung in der Informationsgesellschaft: Handlungsempfehlung für eine digitale Ordnungspolitik, MMR-Beilage 2016, S. 1–28.

Spirgath, Tobias, Zur Abschreckungswirkung des Strafrechts: eine Metaanalyse kriminalstatistischer Untersuchungen, 2013.

Staben, Julian, Der Abschreckungseffekt auf die Grundrechtsausübung: Strukturen eines verfassungsrechtlichen Arguments, 2016.

Stachowiak, Herbert, Allgemeine Modelltheorie, 1973.

Stadler, Thomas, Kann man noch datenschutzkonform twittern?, Internet-Law, Blogbeitrag vom 07.01.2020 (abrufbar unter: http://www.internet-law.de/2020/01/kann-man-noch-datenschutzkonform-twittern.html). Zuletzt abgerufen am 14.01.2022.

Stein, Torsten, „Bananen-Split"? Entzweien sich BVerfG und EuGH über den Bananenstreit?, EuZW 1998, S. 261–264.

Steinbach, Armin, Gesetzgebung und Empirie, Der Staat 2015, S. 267–289.

Steinberg, Rudolf, Verfassungsgerichtliche Kontrolle der „Nachbesserungspflicht" des Gesetzgebers, Der Staat 1987, S. 161–186.

Stender-Vorwachs, Jutta, Neue Formen der Bürgerbeteiligung?, NVwZ 2012, S. 1061–1066.

Stern, Klaus, Die Schutzpflichtenfunktion der Grundrechte: Eine juristische Entdeckung, DÖV 2010, S. 241–249.

Stiemerling, Oliver/Lachenmann, Matthias, Erhebung personenbezogener Daten beim Aufruf von Webseiten: Notwendige Informationen in Datenschutzerklärungen, ZD 2014, S. 133–136.

Stoppel, Dirk André, Grundfreiheitliche Schutzpflichten der Mitgliedstaaten im Europäischen Gemeinschaftsrecht, 2002.

Strahilevitz, Lior Jacob, Information Asymmetries and the Rights to Exclude, Michigan Law Review 2006, S. 1838–1898.

Streinz, Rudolf (Hrsg.), EUV/AEUV Kommentar, 3. Auflage 2018 (zit. *Bearbeiter*, in: Streinz, EUV/AEUV).

Streinz, Rudolf/Michl, Walther, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, S. 384–388.

Strittmatter, Marc/Treiterer, Manuel/Harnos, Rafael, Praxisorientierte Überlegungen zur Bestimmung der Höhe eines materiellen und eines immateriellen Schadens, CR 2019, S. 789–797.

Struse, Eric/Seifert, Julian/Üllenbeck, Sebastian/Rukzio, Enrico/Wolf, Christopher, PermissionWatcher: Creating User Awareness of Application Permissions in Mobile Systems, in: Paternò, Fabio/de Ruyter, Boris/Markopoulos, Panos/Santoro, Carmen/van Loenen, Evert/Luyten, Kris (Hrsg.), Ambient Intelligence: Proceedings of the Third International Joint Conference, Aml 2012, S. 65–80.

Suerbaum, Joachim, Die Schutzpflichtdimension der Gemeinschaftsgrundrechte, EuR 2003, S. 390–416.

Susser, Daniel/Roessler, Beate/Nissenbaum, Helen, Online Manipulation: Hidden Influences In a Digital World, Geo. L. Tech. Rev. 2019, S. 1–45.

Sydow, Gernot (Hrsg.), Europäische Datenschutzgrundverordnung: Handkommentar, 2. Auflage 2018 (zit. *Bearbeiter*, in: Sydow, DSGVO).

Sydow, Gernot/Kring, Markus, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug, ZD 2014, S. 271–277.

Tene, Omer, Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws, Ohio State Law Journal 2013, S. 1217–1261.

Thaler, Richard H./Sunstein, Cass R., Nudge: improving decisions about health, wealth, and happiness, 2008.

Thierer, Adam, The pursuit of privacy in a world where information control is failing, Harv. J. Law Public Policy 2013, S. 410–455.

Thode, Jan-Christoph, Die neuen Compliance-Pflichten nach der Datenschutz-Grundverordnung, CR 2016, S. 714–721.

Thompson, Dennis F., Responsibility for Failures of Government: The Problem of Many Hands, The American Review of Public Administration 2014, S. 259–273.

Thompson, Marcelo, Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries, Vand J Ent & Tech L 2016, S. 783–837.

Thomson, Judith Jarvis, The Right to Privacy, Philosophy & Public Affairs 1975, S. 295–314.

Thon, Marian, Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO, RabelsZ 2020, S. 24–61.

Tilson, David/Sørensen, Carsten/Lyytinen, Kalle, Change and Control Paradoxes in Mobile Infrastructure Innovation: The Android and iOS Mobile Operating Systems Cases, Proceedings of the 45th Hawaii International Conference on System Sciences (HICSS) 2012, S. 1324–1333.

Timner, Hanno/Radlanski, Philip/Eisenfeld, Alexander, Warum das Bußgeldkonzept der Datenschutzkonferenz europa- und verfassungsrechtlich bedenklich ist, CR 2019, S. 782–788.

Tiwana, Amrit/Konsynski, Benn/Bush, Ashley A., Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics, Information Systems Research 2010, S. 675–687.

Trstenjak, Verica/Beysen, Erwin, Das Prinzip der Verhältnismäßigkeit in der Unionsrechtsordnung, EuR 2012, S. 265–285.

Trute, Hans-Heinrich, Grundlagen des Datenschutzes, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht: die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, S. 43–217.

Tzanou, Maria, Data protection as a fundamental right next to privacy? ‚Reconstructing' a not so new right, IDPL 2013, S. 88–99.

Uebele, Fabian, Datenschutzrecht vor Zivilgerichten, GRUR 2019, S. 694–703.

Ulmenstein, Ulrich Freiherr von, Datensouveränität durch repräsentative Rechtswahrnehmung, DuD 2020, S. 528–534.

Unseld, Christopher, Zur Bedeutung der Horizontalwirkung von EU-Grundrechten, 2018.

Utz, Christine/Degeling, Martin/Fahl, Sascha/Schaub, Florian/Holz, Thorsten, (Un) informed Consent: Studying GDPR Consent Notices in the Field, Proceedings of the ACM SIGSAC Conference on Computer and Communications Security 2019, S. 973–990.

Vatanparast, Roxana, Designed to Serve Mankind? The Politics of the GDPR as a Global Standard and the Limits of Privacy, ZaöRV 2020, S. 819–845.

Veil, Winfried, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip, ZD 2015, S. 347–353.

ders., Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, S. 686–696.

ders., Die Schutzgutmisere des Datenschutzrechts – Teil II, CR-online.de, Blogbeitrag vom 18.03.2019 (abrufbar unter: https://www.cr-online.de/blog/2019/03/18/die-schutzgutmisere-des-datenschutzrechts-teil-ii/). Zuletzt abgerufen am 14.01.2022.

ders., Datenschutz, das zügellose Recht – Teil II: Der Datenpaternalismus, CR-online.de, Blogbeitrag vom 21.05.2019 (abrufbar unter: https://www.cr-online.de/blog/2019/05/21/datenschutz-das-zuegellose-recht-teil-ii-der-datenpaternalismus/). Zuletzt abgerufen am 14.01.2022.

Vila, Tony/Greenstadt, Rachel/Molnar, David, Why We Can't Be Bothered To Read Privacy Policies, in: Camp, L. Jean/Lewis, Stephen (Hrsg.), Economics of information security, Boston 2004, 143–153.

Vogel, Benedikt, Datenschutzrechtliche Fragen um Smart TV-Dienste, K&R 2017, S. 441–447.

Vogelgesang, Klaus, Grundrecht auf informationelle Selbstbestimmung?, 1987.

Voigt, Paul, Konzerninterner Datentransfer, CR 2017, S. 428–433.

Voigt, Paul/Alich, Stefan, Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, S. 3541–3544.

Voigt, Paul/Reuter, Wiebke, Platform-to-Business-Verordnung: Neue Anforderungen für Anbieter von Online-Vermittlungsdiensten und Online-Suchmaschinen ab Juli 2020, MMR 2019, S. 783–787.

Volkmann, Uwe, Verbund oder Trennung – Zu einem neuen Verhältnis von Polizei- und Nachrichtendiensten, JURA 2014, S. 820–832.

Volmar, Maximilian, Digitale Marktmacht, 2019.

Wagner, Edgar, Datenschutz als Bildungsauftrag, DuD 2012, S. 83–87.

Wagner, Gerhard, Haftung von Plattformen für Rechtsverletzungen (Teil 2), GRUR 2020, S. 447–457.

Walkila, Sonya, Horizontal effect of fundamental rights in EU law, 2016.

Walter, Konrad, Rechtsfortbildung durch den EuGH – Eine rechtsmethodische Untersuchung ausgehend von der deutschen und französischen Methodenlehre, 2009.

Wank, Rolf, Grenzen richterlicher Rechtsfortbildung,1978.

Warren, Samuel D./Brandeis, Louis D., The Right to Privacy, Harvard Law Review 1890, S. 193–220.

Weber, Franziska, The law and economics of enforcing European consumer law: a comparative analysis of package travel and misleading advertising, 2014.

Wehr, Matthias, Rechtspflichten im Verfassungsstaat: verfassungs- und verwaltungsrechtliche Aspekte der Dogmatik öffentlich-rechtlicher Pflichten Privater, 2005.

Wehrt, Klaus/Mohr, Klaus, Der Einbau der ökonomischen Analyse des Rechts in ein juristisches Fallgutachten, JURA 1995, S. 536–543.

Weichert, Thilo, Informationstechnische Arbeitsteilung und datenschutzrechtliche Verantwortung: Plädoyer für eine Mitverantwortlichkeit bei der Verarbeitung von Nutzungsdaten, ZD 2014, S. 605–610.

ders., „Sensitive Daten" revisited, DuD 2017, S. 538–543.

Weiß, Steffen, Die Bußgeldpraxis der Aufsichtsbehörden in ausgewählten EU-Staaten – ein aktueller Überblick, PinG 2017, S: 97–103.

Wenhold, Céline, Nutzerprofilbildung durch Webtracking: Zugleich eine Untersuchung zu den Defiziten des Datenschutzrechts im Zeitalter von Big Data-Anwendungen, 2018.

Werkmeister, Christoph/Schröder, Elena, Anmerkung zu OVG Schleswig, Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, S. 643–647.

Wernicke, Stephan/Mehmel, Friedrich-Joachim, Privatisierung des Rechts als Folge der Digitalisierung der Wirtschaft, ZEuP 2020, S. 1–10.

Westerlund, Magnus/Enkvist, Joachim, Platform Privacy: The Missing Piece of Data Protection Legislation, jipitec 2016, S. 2–17.

Weyl, E. Glen, A Price Theory of Multi-Sided Platforms, American Economic Review 2010, S. 1642–1672.

Whitman, James Q., The Two Western Cultures of Privacy: Dignity versus Liberty, The Yale Law Journal 2004, S. 1151–1221.

Winter, Max, Demokratietheoretische Implikationen des Rechts auf informationelle Selbstbestimmung, in: Friedewald, Michael/Lamla, Jörg/Roßnagel, Alexander (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, 2017, S. 37–48.

Wischmeyer, Thomas, Regulierung intelligenter Systeme, AöR 2018, S. 2–66.

Wolff, Heinrich Amadeus, Die datenschutzrechtliche Rechtfertigungsbedürftigkeit der Verweise auf Webseiten durch Betreiber von Suchmaschinen – Anmerkung zum Google-Urteil des EuGH, BayVBl 2015, S. 9–16.

ders., Die überforderte Aufsichtsbehörde, PinG 2017, S. 109–111.

ders., Verhaltensregeln nach Art. 40 DS-GVO auf dem Prüfstand, ZD 2017, S. 151–154.

ders., UWG und DS-GVO: Zwei separate Kreise?, ZD 2018, S. 248–252.

Wollin, Sören, Störerhaftung im Immaterialgüter- und Persönlichkeitsrecht: Zustandshaftung analog § 1004 I BGB, 2018.

Wong, Rebecca, Social Networking: The Application of the Data Protection Framework Revisited, Birkbeck Law Review 2014, S. 317–348.

Wybitul, Tim/Haß, Detlef/Albrecht, Jan Philipp, Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung, NJW 2018, S. 113–118.

Wybitul, Tim/Neu, Leonie/Strauch, Martin, Schadensersatzrisiken für Unternehmen bei Datenschutzverstößen, ZD 2018, S. 202–207.

Yoo, Youngjin/Henfridsson, Ola/Lyytinen, Kalle, The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research, Information Systems Research 2010, S. 724–735.

Zalnieriute, Monika/Churches, Genna, When a ‚Like' is not a ‚Like': A New Fragmented Approach to Data Controllership, The Modern Law Review 2020, 861–876.

Zanfir, Gabriela, Forgetting About Consent. Why The Focus Should be On „Suitable Safeguards" in Data Protection Law, in: Gutwirth, Serge/Leenes, Ronald/de Hert, Paul (Hrsg.), Reloading Data Protection, 2014, S. 237–254.

Zanfir-Fortuna, Gabriela/Ianc, Sinziana, Data Protection and Competition Law: The Dawn of ‚Uberprotection', SSRN Scholarly Paper, 2018 (abrufbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3290824). Zuletzt abgerufen am 14.01.2022.

Zarsky, Tal Z., Incompatible: The GDPR in the Age of Big Data, Seton Hall L. Rev. 2017, 995–1020.

Zech, Herbert, Durchsetzung von Datenschutz mittels Wettbewerbsrecht?, WRP 2013, S. 1434–1436.

Zittrain, Jonathan, The Generative Internet, Harv. L. Rev. 2006, S. 1974–2040.

ders., Privacy 2.0, The University of Chicago Legal Forum 2008, S. 65–119.

Stichwortverzeichnis