

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.

© 2022 Mohr Siebeck Tübingen. www.mohrsiebeck.com

Dieses Werk ist lizenziert unter der Lizenz „Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International“ (CC-BY-NC-ND BY 4.0). Eine vollständige Version des Lizenztextes findet sich unter: <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.de>.

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

Vorwort	VII
Inhaltsverzeichnis	XI
Abkürzungsverzeichnis	XVII
Einleitung	1
<i>A. Beschreibung der Thematik</i>	1
<i>B. Methodische Herangehensweise</i>	5
<i>C. Aktueller Stand in Forschung und Rechtsprechung</i>	7
<i>D. Gang der Untersuchung</i>	10
<i>E. Begriffserläuterungen</i>	10
Kapitel 1: Die Akteurspluralität im digitalen Raum	15
<i>A. Beispielhafte Cases</i>	17
<i>B. Bedeutung und Analyse</i>	40
<i>C. Ergebnis</i>	63
Kapitel 2: Die datenschutzrechtliche Verantwortlichkeit	65
<i>A. Regelungszweck und Schutzgut des Datenschutzrechts</i>	65
<i>B. Der Verantwortliche als Herzstück des Regelungskonzepts der DSGVO</i>	111
<i>C. Die Verantwortlichkeit und ihre Voraussetzungen</i>	203
<i>D. Ergebnis</i>	244
Kapitel 3: Die klassischen Akteursrollen in Zeiten der Akteurspluralität – Weiterentwicklung oder Kontinuität?	247
<i>A. Dysfunktionalität durch organisierte Verantwortungslosigkeit</i>	248
<i>B. Die Ausweitung der Verantwortlichkeit als Lösungsansatz</i>	261

C. Ansatz 1: Die Weiterentwicklung der gemeinsamen Verantwortlichkeit	292
D. Ansatz 2: Die Schaffung einer neuen Verantwortlichkeitsfigur für Plattformen	316
E. Ergebnis	360
Kapitel 4: Fazit und Ausblick	361
A. Die einzelnen Akteursgruppen und die Diffusion von Kontrolle	361
B. Die Grundprämissen der Verantwortlichkeit	362
C. Wirksamkeit als Ideal des europäischen Datenschutzes	363
D. Die Dysfunktionalität der Verantwortlichkeit	363
E. Zwei Ansätze der Weiterentwicklung	364
F. Interdisziplinäre Erkenntnisse und ihr Mehrwert für das Recht	364
G. Ausblick	367
Literaturverzeichnis	369
Sachverzeichnis	401

Inhaltsverzeichnis

Vorwort	VII
Inhaltsübersicht	IX
Abkürzungsverzeichnis	XVII
Einleitung	1
<i>A. Beschreibung der Thematik</i>	1
<i>B. Methodische Herangehensweise</i>	5
<i>C. Aktueller Stand in Forschung und Rechtsprechung</i>	7
<i>D. Gang der Untersuchung</i>	10
<i>E. Begriffserläuterungen</i>	10
Kapitel 1: Die Akteurspluralität im digitalen Raum	15
<i>A. Beispielhafte Cases</i>	17
I. Verarbeitungen auf Plattformen	22
1. Verarbeitungen durch Diensteanbieter	27
2. Verarbeitungen durch Drittparteien	31
3. Verarbeitungen durch Plattformbetreiber	34
II. Verarbeitungen außerhalb von Plattformen	36
<i>B. Bedeutung und Analyse</i>	40
I. Der Kontrollverlust der Diensteanbieter und der Kontrollzuwachs von Plattformen	40
II. Die faktischen Regeln des Zusammenspiels von Akteuren auf Plattformen	43
1. Das Entstehen und die Entwicklung von Regeln und Kontrolle	43
2. Die Art der Durchsetzung von Regeln auf Plattformen	51
a) Vertragliche Absicherung	52
b) Technische Absicherung	57
c) Die Verzahnung der beiden Ebenen	62
<i>C. Ergebnis</i>	63

Kapitel 2: Die datenschutzrechtliche Verantwortlichkeit	65
<i>A. Regelungszweck und Schutzgut des Datenschutzrechts</i>	65
I. Die Frage des grundrechtlichen Schutzguts	66
1. Schutz personenbezogener Daten	67
a) Das europäische Datenschutzgrundrecht	67
aa) Der bisherige Meinungsstand	69
bb) Die Rekonstruktion nach Marsch	71
(1) Die Ausgestaltungsdimension aus Art. 8 GRCh	72
(2) Die abwehrrechtliche Dimension	72
(3) Die Schutzpflichten-, Drittwirkungs- und private Ausgestaltungsdimension	74
b) Das Recht auf informationelle Selbstbestimmung deutschen Vorbilds	76
2. Freier Datenverkehr	82
3. Zwischenergebnis: Konsequenzen für das private Datenschutzrecht	83
II. Die konkreten Gefahren für Individuum und Gesellschaft	85
1. Individuelle Gefahren	85
a) In der deutschen Literatur	85
aa) Gefahren durch Informationsverwendung in neuen Kontexten	85
bb) Gefahren durch Datenubiquität und Profiling	87
cc) Gefahren durch Verarbeitung besonders sensibler Daten	91
b) In der internationalen Literatur	92
c) Zwischenergebnis	98
2. Überindividuelle Gefahren	99
a) Demokratietheoretische Bedeutung	99
b) Fremdgefährdungen durch Eigengefährdungen	103
3. Abgleich mit der DSGVO	105
III. Der Regelungszweck: Risikoversorge, Gefahrenabwehr oder Rechtsgüterausgleich?	108
<i>B. Der Verantwortliche als Herzstück des Regelungskonzepts der DSGVO</i>	111
I. Die Komponenten des Regelungskonzepts	113
1. Die Instrumente des Datenschutzes	113
a) Der Selbstdatenschutz	113
b) Der Systemdatenschutz	115
c) Die (regulierte) Selbstregulierung	119
d) Regulierung zur prozeduralen Steigerung von Handlungswissen	122
e) Instrumente zur Rechtsdurchsetzung – die Besonderheit des Rechtsgebiedsdualismus	125
aa) Verwaltungrechtliche Rechtsdurchsetzung	127
(1) Bußgelder und andere Sanktionen	128

(2) Verarbeitungsbeschränkungen und andere Abhilfemaßnahmen	131
(3) Beratung und Kooperation	133
bb) Zivilrechtliche Rechtsdurchsetzung	134
(1) Schadensersatz	134
(2) Verbandsklagerecht	136
(3) Wettbewerbsrechtlicher Schutz von Marktteilnehmern	138
2. Die Steuerungswirkung	141
a) Verantwortlichkeitszuschreibung als Form von Komplexitätsmanagement	141
aa) Management von Akteurskomplexität	142
bb) Management von fachlich-technischer Komplexität	144
cc) Management von Ungewissheit	147
(1) Risikobezogene Ungewissheit	147
(2) Compliancebezogene Ungewissheit	150
b) Verantwortlichkeitszuschreibung als Form von Risikomanagement	153
c) Verantwortlichkeitszuschreibung zur Überwindung von faktischen Rechtsdurchsetzungsdefiziten	155
3. Der Anknüpfungspunkt der Steuerung	160
a) Anknüpfungspunkt Informationsverwendung	160
b) Anknüpfungspunkt Informationspreisgabe	162
4. Zwischenergebnis.	163
II. Die Grundprämissen der Verantwortlichkeit	164
1. Der Verantwortliche als zentrale, alle Umstände der Verarbeitung kennende und beeinflussende Figur	164
2. Der Verantwortliche als nach außen hin klar erkennbare Figur.	167
3. Der Verantwortliche als einfach zuordenbare Rolle.	168
4. Annex: Notwendigkeit eines Minimums an Rechtsdurchsetzung	171
5. Zwischenergebnis.	174
III. Ausmaß legislativer Gestaltungsfreiheit zwischen verfassungsrechtlicher Determinierung und rechtspolitischer Gebotenheit	176
1. Kohärentes Gesamtkonzept/Nachbesserungspflicht	177
a) Bei Erlass des Gesetzes – Untergrenze „Verhältnismäßigkeit“	178
b) Nach Erlass des Gesetzes – verfassungsrechtliche Nachbesserungspflicht	182
2. Schutz vor höheren Gefahrenpotentialen.	190
3. Prozedurale Pflichten als Kehrseite der Medaille: Beobachtungspflicht, Wirksamkeitskontrolle und Zweckmäßigkeitserwägungen	196
4. Zwischenergebnis.	202
C. Die Verantwortlichkeit und ihre Voraussetzungen	203
I. Grundlegende Bedeutung	204
II. Tatbestandsmerkmale	205

1. Die Verarbeitung	206
2. Die Zwecke der Verarbeitung	207
3. Die Mittel der Verarbeitung	207
4. Die Entscheidung über Zwecke und Mittel	207
a) Die Abgrenzung zum Auftragsverarbeiter	209
b) Die Abgrenzung zu weiteren Verantwortlichen: gemeinsam, allein oder gar nicht?	212
aa) Der Fall Wirtschaftsakademie SH	216
bb) Der Fall Fashion ID	221
c) Auswirkungen der EuGH-Linie seit Wirtschaftsakademie und Fashion ID	224
aa) Generelle Rezeption	225
bb) Die Tatbestandsmerkmale – Konkretisierung oder bleibende Unschärfe?	226
cc) Die Konsequenzen	231
(1) Die erhoffte Wirkung	231
(2) Die Übertragbarkeit auf andere Fälle	235
(3) Das Ausmaß der Verantwortlichkeit	239
III. Zwischenergebnis	243
D. Ergebnis	244

Kapitel 3: Die klassischen Akteursrollen in Zeiten der Akteurspluralität – Weiterentwicklung oder Kontinuität? 247

A. <i>Dysfunktionalität durch organisierte Verantwortungslosigkeit</i>	248
I. Die einzelnen Prämissen auf dem Prüfstand	249
1. Der Verantwortliche als zentraler, kenntnis- und einflussreicher Akteur	249
2. Der Verantwortliche als nach außen erkennbarer Akteur	253
3. Der Verantwortliche als einfach zuordenbare Rolle	258
II. Bedeutung	259
B. <i>Die Ausweitung der Verantwortlichkeit als Lösungsansatz</i>	261
I. Notwendigkeit einer extensiven Verantwortlichkeitszuschreibung	261
II. Legitimation der jeweiligen Zusatzbelastung	266
1. Fähigkeit zur Pflichtenerfüllung/Zielerreichung	266
a) Plattformbetreiber	267
aa) Eigene materielle Pflichten	267
bb) Kompensation bestehender Defizite	269
cc) Zwischenergebnis	271
b) Diensteanbieter	272
aa) Eigene materielle Pflichten	272
bb) Kompensation bestehender Defizite	275
cc) Zwischenergebnis	277

2.	Zurechnungstatbestände.	277
a)	Klassische Zurechnung im Datenschutzrecht	278
b)	Parallelen zum Polizeirecht: Nichtstörer und Zweckveranlasser	283
c)	Änderung des Bezugspunkts: Verantwortlichkeit für die eigene Schaffung eines Verarbeitungsumfelds, nicht für die Verursachung von Verarbeitungen	286
3.	Annex: Zusatzbelastung für Dienste- und Drittanbieter	290
III.	Zwischenergebnis	291
C.	<i>Ansatz 1: Die Weiterentwicklung der gemeinsamen Verantwortlichkeit</i>	292
I.	Auswirkungen und Grenzen der gemeinsamen Verantwortlichkeit	293
II.	Zielgerechte Skalierbarkeit der Verantwortlichenpflichten	296
III.	Möglichkeiten der Umgestaltung	299
1.	De lege lata.	300
2.	De lege ferenda	301
a)	Modifikation der Verantwortlichkeitszuschreibung	302
b)	Modifikation der Verantwortlichkeitsausgestaltung	304
aa)	Einzelfallunabhängige Anwendung existierender Pflichten	304
(1)	Anwendbare Pflichten	305
(2)	Nicht anwendbare Pflichten	309
bb)	Flexible Anwendung einer Auswahl- und Überwachungspflicht	310
IV.	Zwischenergebnis – Bestandsaufnahme des Ansatzes	315
D.	<i>Ansatz 2: Die Schaffung einer neuen Verantwortlichkeitsfigur für Plattformen</i>	316
I.	Notwendigkeit einer neuen Figur	318
II.	Die Voraussetzungen für die Pflichtigkeit	320
1.	Zur möglichen Notwendigkeit einer Mindestgröße	322
2.	Zur möglichen Notwendigkeit eines Mindestumsatzes	325
3.	Zur möglichen Notwendigkeit eines Mindestgrads an Geschlossenheit der Plattform	325
4.	Zwischenergebnis.	327
III.	Die konkreten Pflichten der Plattformverantwortlichkeit	328
1.	Reine Intermediärhaftung.	328
2.	Vollständiges Verantwortlichkeitskonzept	332
a)	Proaktive Pflichten	333
aa)	Privacy by design	334
(1)	Zielrichtung Verantwortliche	336
(2)	Zielrichtung Betroffene	338
bb)	Datenschutzfolgenabschätzung	340
cc)	Auswahlpflicht	340
b)	Reaktive Pflichten	341
c)	Rechtsfolgen und Haftung	344
3.	Zwischenergebnis.	346

IV. Limitierungen und Problemstellen	347
1. Zur Problematik der extraterritorialen Wirkung	347
2. Zur Problematik der Verstärkung bestehender Machtstrukturen	350
3. Zur Problematik des Verarbeitungsverhaltens der Plattformen selbst	352
4. Zur Problematik der Privatisierung der Rechtsdurchsetzung	354
V. Zwischenergebnis	358
<i>E. Ergebnis</i>	360
Kapitel 4: Fazit und Ausblick	361
<i>A. Die einzelnen Akteursgruppen und die Diffusion von Kontrolle</i>	361
<i>B. Die Grundprämissen der Verantwortlichkeit</i>	362
<i>C. Wirksamkeit als Ideal des europäischen Datenschutzes</i>	363
<i>D. Die Dysfunktionalität der Verantwortlichkeit</i>	363
<i>E. Zwei Ansätze der Weiterentwicklung</i>	364
<i>F. Interdisziplinäre Erkenntnisse und ihr Mehrwert für das Recht</i>	364
<i>G. Ausblick</i>	367
Literaturverzeichnis	369
Sachverzeichnis	401

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
AlMag	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.	Bundestagsdrucksache
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 Parlamentes 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	Goldammer'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 technologie neutrale², risikosensible³ und somit – so die Idealvorstellung – entwicklungs offene 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 technologie neutralen 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 Erlaubnisvorbehalt⁹ 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-Kommissarin *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 Gegenstände¹² bzw. des Internet of Things¹³ oder der Nutzung besonders sensibler, z. B. biometrischer oder Mobilitätsdaten.¹⁴ Ob das Festhalten der DSGVO an ihrem technikneutralen¹⁵ *one size fits all*-Konzept¹⁶ 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 Ubiquität 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 Verarbeitung²⁰ – 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-Entscheidungen²⁴ betraf die Erweiterung der Verantwortlichkeit sodann einzelne Betreiber von Websites und sog. Fanpages, die die von Facebook angebotene Infrastruktur und einzelne Bestandteile dieser nutzen und es Facebook dadurch ermöglichen, 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 ungeklärten 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 Rechtsauslegung²⁵ 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 Governance²⁶ 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-Abmann*, 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; Henrich, 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 Auftragsverarbeiters³³ 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 Auftragsverarbeiters³⁴ – 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* Internet³⁶ 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 Akteure⁴⁴ sowie die mit einer bisher fehlenden Konturierung der Qualitätsmerkmale einhergehende Unsicherheit darüber, wer alles als Verantwortlicher in Betracht kommt⁴⁵. 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 Einflussphären 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.

Stichwortverzeichnis

- Abschreckungseffekt 93, 136
AccuWeather 19 f., 32 f., 60 f.
Adtech 18 f., 257, 352
Akteurskomplexität *siehe* Akteurspluralität
Akteurspluralität 15 ff., 40 ff., 63 f., 142, 238, 249, 358, 363 f.
Algorithmen 2, 87 ff.
Amazon 20 f., 28, 53, 173, 313, 321, 353
Anonymität 101, 115, 216
APIs 28 ff., 33, 46 ff., 60 f., 336
Apple 28, 32 f., 46 ff., 58 ff., 253 ff., 270 f., 321, 339, 350 ff.
Apps 18 ff., 42 f., 46 ff., 53, 201, 238 f., 255, 269 f.
Art. 29-Datenschutzgruppe 150, 207 ff., 226 ff., 294, 299 ff.,
Auftragsverarbeiter 7 f., 129, 142, 171, 209 ff., 236, 251 f., 304, 319
Aufsichtsbehörden 15, 121 ff., 127 ff., 187, 217, 225 f., 242 f., 266, 280, 294 f.
Automatisierte Entscheidungsfindung 85, 107

Beobachtungspflicht 196 ff.
Berechtigtes Interesse 107, 114, 257
Betroffene 11 ff., 87 ff., 103 ff., 113 ff., 136 ff., 162 ff., 240 f., 303 f.
Boundary Resources 46 ff., 269 ff., 319 ff., 366 ff.
BSSID 19, 33

Cambridge Analytica 20 ff., 28 ff., 50, 102, 290
Cookies 38, 216, 263
Cloud 7 f., 252, 264
Databroker 21
Datensicherheit 49, 116, 151, 157, 161, 307

Datenschutz
– Regelungszweck 65 ff., 108 ff., 176 ff.
– Schutzgut 65 ff., 196, 279
Datenschutzfolgenabschätzung 122 ff., 149, 253, 308, 340 ff.
Datenschutzgrundrecht 67 ff., 113, 190 ff.
Datenverarbeitungen 9 ff., 40 f., 69 ff., 111, 177 f., 206 ff., 265
– Mittel der 143, 207 ff.
– Ubiquität der 77 ff., 87 ff., 280
– Zwecke der 143, 207 ff., 229, 282, 310
Datenverkehr, freier 82 ff., 109
Design 30, 48, 56 ff., 253
Diensteanbieter 16, 27 ff., 40 ff., 63 f., 250 f., 272 ff.
Distributionskanal 53 ff., 252 ff., 268, 276, 318, 338 f., 341 f.
Drittparteien 27, 31 ff., 238 ff., 255 ff., 267 ff.
Drittstaaten 349
DSGVO 2 f., 65 ff., 111 ff.

Eigengefährdung 103 ff.
Eigensicherungspflichten 287 ff.
Einwilligung 58, 107, 113 ff., 162 ff., 188 ff., 254, 263, 339 ff.
ePrivacy-RL/VO 185, 300, 356
Erforderlichkeit 178 ff.
Erlaubnisvorbehalt 2, 75 ff., 111 ff., 163, 177, 205, 280
EuGH 4 f., 9, 35 ff., 68 ff., 175 ff., 221 ff., 311 ff.

Facebook 5, 20 ff., 102 f., 173, 216 ff., 295, 321
Fashion ID 38 ff., 221 ff., 235 ff., 262 f., 294, 329
Freiheit 11, 45 ff., 71 ff., 84 ff., 99 ff., 180 f., 354 ff.

- Freiwilligkeit 38, 99, 120 f., 189, 339
 Fremdgefährdung 103 ff.
- Gefahr(en) 12 f., 66, 85 ff., 190 ff.,
 – individuelle 85 ff.
 – überindividuelle 99 ff.
 Gefahrenabwehr 108 ff., 242, 278 ff., 295
 Geschäftsmodell 15 ff., 46, 62, 212, 226,
 251, 315
 Gesellschaft 70, 96, 99 ff., 108 ff., 198
 Google 4 f., 39 f., 53 ff., 173, 270 ff.
 Governance 6, 44 ff., 123, 141 ff., 351
 Grundrechte 66 ff., 108 ff., 178 ff., 261 ff.
 – mittelbare Drittwirkung der 74 ff.
- Haftung 213, 218, 222, 239 ff., 276 f.,
 295 ff., 328 ff., 344 ff.
 Handlungsräume 40 ff., 270, 325
- Impossibility structures* 57, 117
 Informationelle Selbstbestimmung 73,
 76 ff., 99, 108, 113 ff., 192 f.
 Informationen 12 f., 77 ff., 86, 160 ff.
 Infrastruktur 5, 15 f., 56, 99, 108, 225 ff.
 Interessenabwägung 107 f., 114, 151,
 267 f.
 Interdisziplinarität 5, 16, 359, 364 ff.
 Intermediäre 23 ff., 254, 328 ff., 356 f.
 IP-Adressen 18, 39, 221, 297 f.
 IT-Sicherheit *siehe* Datensicherheit
- Kartellrecht 66, 126, 324, 350 ff.
 Kohärenzverfahren 173
 Kommunikation 4, 67 ff., 101 f., 108 ff.,
 182
 Komplexität 4 f., 141 ff., 78 f., 205, 214 f.,
 357
 Kontrolldichte 53 f., 157, 181
 Kontrolle 16, 26, 43 ff., 157, 190 ff.,
 214 ff., 249 ff.
 Kooperation 44, 133 ff., 364
- Legitimation 72, 266 ff., 290
 Lock In-Effekt 322
 Lockerungen 48 ff.
- Macht 23, 70, 95, 223 ff., 350 ff.
 Meinungsfreiheit 74, 348, 355 ff.
- Menschenwürde 96
 Meta-Regulierung 123 ff.
 Missbrauch 251 ff., 343
 Modell 46 ff., 77 ff., 87 ff., 141 ff.
- Nachbesserungspflicht 177 ff., 297
 Netzwerkeffekte 23 ff., 37, 322
- Ökosystem 22 ff., 41, 61 ff., 239
- Parametrierung 220, 227 ff.
 Paternalismus 99
 Personenbezogene Daten 8, 11, 67 ff.,
 185, 199, 203, 205 ff.
 Persönlichkeitsprofile 17 f., 29, 87 ff.
 Pixel 22, 38 ff., 255
 Pflichten 190 ff., 266 ff., 296 ff., 320 ff.,
 328 ff.
 – proaktive 333 ff.
 – reaktive 341 ff.
- Plattformen 22 ff., 43 ff., 64, 238 f., 252 f.,
 259 ff.
 Plattformbetreiber 27, 34 ff., 41 ff., 58 ff.,
 267 ff., 286 ff., 316 ff.
 Privacy 8, 92 ff., 115, 185, 324
 – by default 116, 151, 307
 – by design 116, 146, 151, 163, 170,
 268 ff., 314 ff.
 Privatsphäre 20, 63 ff., 93, 101 ff., 139,
 356
- Rechtsdurchsetzung 125 ff., 153 ff.,
 171 ff., 354 ff.
 Regelungskonzept *siehe* Regulierung
 Regulierte Selbstregulierung 119 ff.,
 149 ff., 334, 367
 Regulierung 11, 13, 62, 74, 108 ff.,
 122 ff., 157 ff., 362 ff.
 Regulierungskonzept *siehe* Regulierung
 Reveal Mobile 19 ff., 32 ff., 60
 Risiko 12 ff., 81, 108 ff., 147 ff., 153 ff.
- Sanktionen 64, 111, 128 ff., 269, 277 ff.,
 342 ff.
 Schadensersatz 134 ff., 295, 345 f.
 Selbstdatenschutz 113 ff., 159 ff.
 Sensible Daten 3, 18 ff., 91 ff.
 Schutzgut 65 ff., 83 f., 176 ff., 279

- Schutzpflichten 74 ff., 191 ff., 261 ff.
SDKs 19 ff., 46 ff., 250, 352
Social plugins 16, 37 f., 232 ff., 329
Soziale Netzwerke 8, 17, 176, 348 ff.
Steuerung 11 ff., 81, 120, 135 ff., 141 ff.,
160 ff., 231 ff., 367
Strukturprinzipien 84
Systemdatenschutz 115 ff., 163, 258
- Take it or leave it* 250 f., 273, 299, 306,
313
- Überwachungspflicht 142, 251, 310 ff.,
330, 337, 365
Ungewissheit 87 f., 94, 147 ff., 196, 237,
296, 303, 316 ff.
- Verantwortlichkeit 65 ff., 141 ff., 203 ff.,
261 ff.
– gemeinsame 212 ff., 293 ff., 299 ff.
– Grundprämissen der 164 ff.
– Plattform- 316 ff.
Verbandsklagerecht 136 ff., 172
Verhaltensregeln, genehmigte 121 ff.,
144, 152 f., 309, 338
- Verhältnismäßigkeit 110, 128, 178 ff.,
234, 299
Verschulden 129, 295, 346
Vertriebskanal *siehe* Distributionskanal
Verursachung 278 ff., 286 ff., 310, 345
Verwaltungsrecht 127 ff., 149, 156, 169
Volkszählungsurteil 76, 100, 197
Vorfeldschutz 13, 72 ff., 109, 173
- Weisungen 7 f., 129, 212, 282, 344 f.
Wirtschaftsakademie Schleswig-Holstein
9, 35, 216 ff., 255, 275, 295 ff., 305,
311
- Youtube 38, 236
- Zugangskontrolle 26, 55, 220, 348, 361 f.
Zugriffsrechte 18 ff., 33, 42 f., 60 ff.,
207 ff., 252 ff. 273 f., 336 ff.
Zurechnung 277 ff., 292, 317 f.
Zweckkongruenz 213 ff., 224, 229 f., 283,
310,
Zweckmäßigkeit 196 ff.
Zweckveranlasser 283 ff.