

PHILIPP HACKER

# Datenprivatrecht

*Jus Privatum*

244

---

**Mohr Siebeck**

JUS PRIVATUM  
Beiträge zum Privatrecht

Band 244





Philipp Hacker

# Datenprivatrecht

Neue Technologien im Spannungsfeld  
von Datenschutzrecht und BGB

Mohr Siebeck

*Philipp Hacker*, geboren 1985; Studium der Rechtswissenschaften, Philosophie und Neuen deutschen Literatur in München und Salamanca; 2014 LL.M., Yale Law School; 2016 Promotion, Humboldt-Universität zu Berlin; 2016/17 Max Weber Fellow, Europäisches Hochschulinstitut, Florenz; 2017/18 A.SK Fellow, Wissenschaftszentrum Berlin; 2019/20 AXA Postdoctoral Fellow, Humboldt-Universität zu Berlin; 2020 Habilitation, Humboldt-Universität zu Berlin; seit 9/2020 Inhaber des Lehrstuhls für Recht und Ethik der digitalen Gesellschaft, Europa-Universität Viadrina, European New School of Digital Studies.

Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) – 452321320.

ISBN 978-3-16-159617-9 / eISBN 978-3-16-159618-6

DOI 10.1628/978-3-16-159618-6

ISSN 0940-9610 / eISSN 2568-8472 (Jus Privatum)

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

© 2020 Mohr Siebeck Tübingen. [www.mohrsiebeck.com](http://www.mohrsiebeck.com)

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für die Verbreitung, Vervielfältigung, Übersetzung und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das Buch wurde von epline in Böblingen aus der Stempel-Garamond gesetzt, von Gulde Druck in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

*Für Lena, Tim und Clara*



## Vorwort

Daten werden zu einem immer gewichtigeren Teil aller Austauschprozesse. In rechtlicher Hinsicht bedingt dies einerseits, dass das unionale Datenschutzrecht tief in das mitgliedsstaatliche Privatrecht hineinragt. Umgekehrt wirkt dieses aber, zumal wenn es unionsrechtlich harmonisiert ist, auch vielfältig auf das Datenschutzrecht zurück. Die vorliegende Arbeit vermisst dieses Spannungsfeld. Dabei fokussiert sie sich auf drei Basistechnologien: Tracking-Instrumente, künstliche Intelligenz und das Internet der Dinge. Sie lag im Sommersemester 2020 der Juristischen Fakultät der Humboldt-Universität zu Berlin als Habilitationsschrift vor. Das Manuskript ist auf dem Stand von Mai 2020.

Entscheidende Impulse hat die Arbeit von einer Reihe von Personen und Institutionen erhalten. Mein Dank gilt dabei in erster Hinsicht meinem akademischen Lehrer, Herrn Professor Stefan Grundmann, der mir für diese Untersuchung nicht nur alle erdenklichen Freiheiten gewährt hat, sondern auf dessen Freundschaft und umsichtigen Rat in allen Dingen ich jederzeit zählen konnte und kann. Dass wir nicht nur einige Jahre in Berlin, sondern auch ein Jahr in Florenz am Europäischen Hochschulinstitut gemeinsam verbringen konnten, war eine glückliche Fügung, welche die Forschung in meiner Postdoktorandenzeit sehr befördert hat. Herrn Professor Axel Metzger danke ich herzlich für die äußerst zügige Erstellung des Zweitgutachtens und wertvolle inhaltliche Hinweise. Insgesamt konnte ich aus dem Schwerpunkt, den die Juristische Fakultät der Humboldt-Universität zu Berlin auf die Erforschung der Digitalisierung legt, zahlreiche Anregungen mitnehmen, etwa aus Gesprächen mit Herrn Professor Lars Klöhn, Frau Professorin Eva Inés Oberfell, Herrn Professor Gerhard Wagner und Herrn Professor Herbert Zech sowie mit meinen Co-Habilitanden, Dr. Michael Denga, Frau Professorin Linda Kuschel, Dr. Jan-Erik Schirmer, Dr. Sven Asmussen und Dr. Valentin Jentsch.

Meine eigene Forschungstätigkeit im Schnittbereich von Recht und Technologie hat von einer Reihe von Förderungen profitiert, für die ich überaus dankbar bin. Forschungsstipendien der Humboldt-Universität, des Europäischen Hochschulinstituts und des Wissenschaftszentrums Berlin sowie Forschungsprojekte am University College London haben mir eine vertiefte und interdisziplinäre Beschäftigung mit den rechtlichen Herausforderungen digitaler Technologien ermöglicht. Dass die Arbeit selbst im Jahr 2019 zügig niedergeschrieben werden konnte, verdanke ich einem AXA Postdoctoral Fellow-



ship, mit dem ich an die Humboldt-Universität zurückkehrte. Der DFG danke ich für die Gewährung einer Publikationsbeihilfe, der Deutschen Stiftung für Recht und Informatik für die Auszeichnung dieser Arbeit mit dem DSRI-Wissenschaftspreis.

Zahllose Gesprächspartner haben die Arbeit und meine Forschung in dieser Zeit überaus befruchtet. Herr Professor Klaus Hopt hat meinen Werdegang immer wieder mit umsichtigen Ratschlägen begleitet. Gleiches gilt für Herrn Professor Hans-W. Micklitz, Herrn Professor Klaus Ulrich Schmolke und Herrn Professor Mattias Kumm. Frau Professorin Marietta Auer danke ich für ein weitsichtiges Gespräch am Wissenschaftskolleg. Technische und mathematische Problemstellungen konnte ich mit meinen interdisziplinären Co-Autoren angehen, dem Mathematiker Professor Emil Wiedemann und den Informatikern Professor Felix Naumann und Meike Zehlike, woraus mehrfach fruchtbare Kooperationen erwachsen.

Besonders herzlich danke ich schließlich meinen Freunden und, vor allem, meiner Familie. Meine Mutter hat das gesamte Manuskript Korrektur gelesen – all errors remain entirely my own, wie man in amerikanischen Aufsätzen zu sagen pflegt. Meine Frau und meine zwei Kinder schließlich haben glücklicherweise immer wieder für die nötige Entschleunigung und die fröhlichste aller denkbaren Ablenkungen von der Wissenschaft gesorgt. Ihnen ist diese Arbeit gewidmet.

Berlin, im Mai 2020

Philipp Hacker

# Inhaltsübersicht

Vorwort .....	VII
Inhaltsverzeichnis .....	XI
§1 <i>Einführung</i> .....	1
A. Daten in der Dauerschleife .....	1
B. Datenprivatrecht .....	4
C. Regulatorisches und ermöglichendes Privatrecht .....	8
D. Problemaufriss und Aufbau der Untersuchung .....	12
Teil 1: Technische und ökonomische Grundlagen .....	23
§2 <i>Technische Grundlagen moderner Informationsverarbeitungssysteme</i> .....	25
A. Tracking-Instrumente .....	25
B. Künstliche Intelligenz: Techniken maschinellen Lernens .....	29
C. Das Internet der Dinge .....	37
D. Konvergenzprozesse: Auf dem Weg zum <i>Internet of Everything</i> .....	43
§3 <i>Technisch-ökonomische Problemstellungen und rechtliche Herausforderungen</i> .....	47
A. Erste rechtliche Herausforderung: Multirelationalität vernetzter Datenanalyse .....	47
B. Zweite rechtliche Herausforderung: Ambivalenz vernetzter Datenerhebung und -verarbeitung .....	56
C. Dritte rechtliche Herausforderung: Ermöglichung der Durchsetzung heterogener Datenschutzpräferenzen .....	76
D. Leitfälle und Leitfragen für die weiteren Teile der Arbeit .....	77
E. Ergebnisse von §3 .....	82

Teil 2: Datenschutzrecht und allgemeines Privatrecht .....	85
§4 <i>Vernetzte Datenerhebung und -analyse im Datenschutzrecht</i> .....	87
A. Datenschutzrechtliche Grundlagen .....	87
B. Ermöglichende Strukturen im Datenschutzrecht .....	159
C. Regulatorische Strukturen im Datenschutzrecht .....	270
D. Ergebnisse von §4 .....	309
§5 <i>Vernetzte Datenerhebung und -analyse im allgemeinen Privatrecht</i> ...	313
A. Zum Verhältnis von unionalem Datenschutzrecht und mitgliedstaatlichem Privatrecht .....	314
B. Ermöglichende Strukturen im allgemeinen Privatrecht .....	343
C. Regulatorische Strukturen im allgemeinen Privatrecht .....	397
D. Ergebnisse von §5 .....	538
 Teil 3: Reformperspektiven .....	 545
§6 <i>Präferenzverwirklichung durch Technikgestaltung</i> .....	547
A. Autonomie, Informiertheit und Datenschutzpräferenzen .....	548
B. Minimierung von Datenschutzrisiken durch Technik .....	553
C. Entscheidungsunterstützung durch Recht .....	577
D. Ergebnisse von §6 .....	655
 Teil 4: Schluss .....	 657
§7 <i>Lösungsansätze für die drei rechtlichen Herausforderungen, de lege        lata und de lege ferenda</i> .....	659
A. Erste rechtliche Herausforderung: Multirelationalität von Daten .....	659
B. Zweite rechtliche Herausforderung: Ambivalenz von Nutzen und Risiken .....	662
C. Dritte rechtliche Herausforderung: Heterogenität von Datenschutzpräferenzen .....	666
§8 <i>Wesentliche Ergebnisse der Arbeit in zehn Thesen</i> .....	669
 Literaturverzeichnis .....	 673
Sachregister .....	741

# Inhaltsverzeichnis

Vorwort .....	VII
Inhaltsübersicht.....	IX
§1 <i>Einführung</i> .....	1
A. Daten in der Dauerschleife .....	1
B. Datenprivatrecht .....	4
C. Regulatorisches und ermöglichendes Privatrecht .....	8
D. Problemaufriss und Aufbau der Untersuchung .....	12
I. Regulierende und ermöglichende Strukturen im Datenprivatrecht	12
II. Kurzüberblick über die drei Hauptteile der Arbeit .....	15
1. Technische und ökonomische Grundlagen (Teil 1) .....	16
2. Datenschutzrecht und allgemeines Privatrecht (Teil 2).....	17
3. Reformperspektiven (Teil 3) .....	20
Teil 1: Technische und ökonomische Grundlagen .....	23
§2 <i>Technische Grundlagen moderner Informationsverarbeitungssysteme</i>	25
A. Tracking-Instrumente .....	25
I. Cookies .....	26
II. Fingerprinting-Techniken .....	28
III. Sonstige eindeutige Kennungen .....	28
B. Künstliche Intelligenz: Techniken maschinellen Lernens .....	29
I. Begriffe .....	29
II. Strategien und Modelle maschinellen Lernens .....	31
1. Lernstrategien .....	31
a) Überwachtes Lernen ( <i>supervised learning</i> ) .....	31
b) Verstärkungslernen ( <i>reinforcement learning</i> ) .....	33
c) Unüberwachtes Lernen ( <i>unsupervised learning</i> ).....	33
2. Maschinelles Lernen als Optimierungsproblem: Tiefe neuronale Netze .....	34
III. Technische Autonomie, Daten und Inferenzen .....	35

C.	Das Internet der Dinge .....	37
I.	Vier Charakteristika von IoT-Geräten .....	39
II.	Vier Schichten des IoT .....	41
D.	Konvergenzprozesse: Auf dem Weg zum <i>Internet of Everything</i> .....	43
§3	<i>Technisch-ökonomische Problemstellungen und rechtliche Herausforderungen</i> .....	47
A.	Erste rechtliche Herausforderung: Multirelationalität vernetzter Datenanalyse .....	47
I.	Techno-physische Vernetzung: Internet der Dinge .....	47
II.	Ökonomische Folgerungen: Daten als Gegenleistung .....	49
1.	Daten als funktionales Geldäquivalent .....	49
a)	Austausch ohne monetäre Gegenleistung .....	50
b)	Wertschöpfung an Daten .....	51
aa)	Optimierung von Modellen .....	51
bb)	Daten als Input für Modelle .....	51
cc)	Datenhandel .....	52
2.	Systematisierung: Kategorien von Daten als Gegenleistung .....	53
a)	Datenbasiertes Grundmodell .....	53
aa)	Vollkommen datenfinanzierte Modelle .....	53
bb)	Freemium-Modelle .....	53
b)	Monetäres Grundmodell .....	54
aa)	Rabattmodelle .....	54
bb)	Data on top-Modelle .....	54
III.	Die Multirelationalität von personenbezogenen Daten .....	55
B.	Zweite rechtliche Herausforderung: Ambivalenz vernetzter Datenerhebung und -verarbeitung .....	56
I.	Potenzial .....	57
1.	Individuelle Ebene .....	57
a)	Präferenz Erfüllung .....	57
b)	Zeitersparnis .....	57
c)	Kaufkraftsteigerung .....	58
2.	Sozialer Nutzen .....	58
II.	Datenschutzrechtliche Risiken .....	58
1.	Vier Typen von Marktversagen .....	59
a)	Informationsasymmetrie: Mangelnde Kenntnis der Datenverarbeitung .....	60
aa)	Informationsüberlastung .....	60
bb)	Rationale Ignoranz .....	61
b)	Verhaltensökonomische Effekte bei der Datenbewertung .....	62
c)	Negative Externalitäten durch Kollektiveffekte .....	64
aa)	Adverse Inferenz .....	65
bb)	Ähnlichkeitsbasierte Inferenz .....	66

d) Unschärfe des Datenpreissignals . . . . .	67
e) Zusammenfassung zum Marktversagen . . . . .	70
2. Soziale Risiken . . . . .	70
a) Verhaltens- und Freiheitsverengung ( <i>chilling effects</i> ) . . . . .	71
b) Unentziehbarkeit . . . . .	73
c) Mangelndes Bewusstsein der Datenerhebung . . . . .	74
d) Diskriminierung . . . . .	75
C. Dritte rechtliche Herausforderung: Ermöglichung der Durchsetzung heterogener Datenschutzpräferenzen . . . . .	76
D. Leitfälle und Leitfragen für die weiteren Teile der Arbeit . . . . .	77
I. Drei paradigmatische Leitfälle . . . . .	77
1. Datenweiterleitung an Drittunternehmen . . . . .	77
2. Datenerhebung durch Drittanbieter ( <i>third-party tracking</i> ) . . . . .	79
3. Datenerhebung bei Dritten . . . . .	80
II. Leitfragen . . . . .	81
E. Ergebnisse von § 3 . . . . .	82

## Teil 2: Datenschutzrecht und allgemeines Privatrecht . . . . . 85

### § 4 Vernetzte Datenerhebung und -analyse im Datenschutzrecht . . . . . 87

A. Datenschutzrechtliche Grundlagen . . . . .	87
I. Rechtsgrundlagen des Datenschutzrechts im Kurzüberblick . . . . .	88
1. Europäische Ebene . . . . .	88
a) DS-GVO . . . . .	88
b) ePrivacy-Instrumente . . . . .	89
c) Sonstige Instrumente . . . . .	90
2. Nationale Ebene . . . . .	91
a) BDSG . . . . .	92
b) UWG . . . . .	92
c) Sonstige Regelungen . . . . .	93
II. Anwendbarkeit der DS-GVO . . . . .	93
1. Territoriale Anwendbarkeit . . . . .	93
a) Art. 3 Abs. 1 DS-GVO: Niederlassungsprinzip . . . . .	94
aa) Der Begriff der Niederlassung . . . . .	95
bb) Verarbeitung im Rahmen der Tätigkeit der Niederlassung . . . . .	96
b) Art. 3 Abs. 2 DS-GVO: Marktortprinzip . . . . .	98
aa) Art. 3 Abs. 2 lit. a DS-GVO: Marktangebot . . . . .	99
(1) Dienstleistung oder Ware . . . . .	100
(2) Spezifisches Angebot . . . . .	100
bb) Art. 3 Abs. 2 lit. b DS-GVO: Verhaltensbeobachtung . . . . .	102

2. Sachliche Anwendbarkeit .....	103
a) Grundtatbestand: Art. 2 Abs. 1 DS-GVO .....	103
aa) Personenbezogene Daten.....	104
(1) Bezug zu einer Person .....	104
(2) Identifizierbarkeit einer konkreten Person .....	105
(a) Grundsätzliche Kriterien.....	105
(aa) (Re-)Identifizierungsstrategien.....	106
(bb) Die Rechtssache <i>Breyer</i> .....	107
(cc) Der 26. Erwägungsgrund der DS-GVO: Illegale Re-Identifizierung .....	108
(dd) Folgerungen.....	110
(b) Anwendung auf die drei Leitfälle .....	111
(aa) Datenweiterleitung an Dritte (personalisierte Werbung) .....	112
α. Namenlose Profile .....	112
β. Machine-to-machine-Kommunikation ...	113
(bb) Datenerhebung durch Dritte ( <i>third-party tracking</i> ) .....	114
(cc) Datenerhebung bei Dritten .....	117
(3) Ergebnis zu personenbezogenen Daten.....	117
(4) Regelung nicht personenbezogener Daten .....	117
bb) Spezifische Verarbeitungsformen .....	119
(1) Ganz oder teilweise automatisierte Verarbeitung ....	119
(2) Speicherung oder Speicherungsabsicht in Dateisystem .....	119
b) Ausnahmen: Art. 2 Abs. 2–3 DS-GVO .....	120
aa) Kein Anwendungsbereich des Unionsrechts, Art. 2 Abs. 2 lit. a DS-GVO .....	120
(1) Die Fälle <i>Österreichischer Rundfunk</i> und <i>Lindqvist</i> – Argumente des EuGH und Kritik .....	121
(2) Der Anwendungsbereich des Unionsrechts nach der DS-GVO .....	123
(a) Die klassischen Kriterien der Eröffnung des Anwendungsbereichs des Unionsrechts .....	124
(b) Die partielle Fortgeltung der EuGH-Rechtsprechung.....	125
(aa) Fortgeltung des Falls <i>Österreichischer           Rundfunk</i> .....	125
(bb) Keine Fortgeltung des Falls <i>Lindqvist</i> .....	126
(3) Folgerungen.....	126
bb) Weitere Ausnahmen .....	127
3. Ergebnis zur Anwendbarkeit der DS-GVO.....	128
III. Datenschutzrechtliche Grundkonzepte .....	128

1. Stufen datenschutzrechtlicher Verantwortlichkeit in vernetzten Umgebungen . . . . .	129
a) Relevanz der Bestimmung der Verantwortlichkeit . . . . .	129
b) Typen von Verantwortlichkeit . . . . .	130
aa) Alleinige Verantwortlichkeit . . . . .	130
bb) Gemeinsame Verantwortlichkeit . . . . .	130
cc) Zwischenstufen: Die Rechtssache <i>Wirtschaftsakademie Schleswig-Holstein</i> . . . . .	132
dd) Anwendung auf die drei Leitfälle . . . . .	133
(1) Datenerhebung durch Drittanbieter ( <i>third-party tracking</i> ) . . . . .	133
(a) Die Rechtsprechung des EuGH . . . . .	133
(aa) Kriterien . . . . .	133
α. Cookies: Nochmals <i>Wirtschaftsakademie Schleswig-Holstein</i> . . . . .	133
β. Social Plug-Ins: Die Rechtssache <i>Fashion ID</i> . . . . .	136
(bb) Rechtsfolgen . . . . .	137
α. Geltung der DSRL (Altfälle) . . . . .	137
β. Art. 26 Abs. 3 DS-GVO . . . . .	137
(b) Plädoyer für eine abgestufte Verantwortung im Rahmen der DS-GVO . . . . .	138
(aa) Kriterien . . . . .	138
(bb) Rechtsfolgen . . . . .	140
α. Notwendigkeit einer teleologischen Reduktion . . . . .	141
β. Subsidiäre Anwendung von § 275 Abs. 1 oder 2 BGB . . . . .	141
γ. Konsequenzen für einzelne Betroffenenrechte . . . . .	143
(2) Datenübermittlung an Drittunternehmen (personalisierte Werbung) . . . . .	143
(a) Werbenetzwerke ( <i>ad exchanges</i> ) . . . . .	144
(b) Weiterleitung im Internet der Dinge . . . . .	145
(3) Datenerhebung bei Dritten . . . . .	145
c) Datenschutzrechtliche Störerhaftung als dritte Kategorie? . . . . .	146
d) Ergebnis zur Verantwortlichkeit . . . . .	148
2. Grundsätze der Datenverarbeitung . . . . .	148
a) Rechtscharakter der Grundsätze . . . . .	148
b) Die Grundsätze des Art. 5 Abs. 1 DS-GVO im Einzelnen . . . . .	150
aa) Art. 5 Abs. 1 lit. a Var. 1 DS-GVO: Legalität . . . . .	150
bb) Art. 5 Abs. 1 lit. a Var. 2 DS-GVO: Treu und Glauben ( <i>fairness</i> ) . . . . .	150



(1) Rechtsbereichsübergreifende Fairness jenseits von Transparenz . . . . .	151
(2) Inhaltliche Ausfüllung . . . . .	152
cc) Art. 5 Abs. 1 lit. a Var. 3 DS-GVO: Transparenz . . . . .	154
dd) Art. 5 Abs. 1 lit. b DS-GVO: Zweckbindung . . . . .	155
ee) Art. 5 Abs. 1 lit. c DS-GVO: Datenminimierung . . . . .	156
ff) Art. 5 Abs. 1 lit. d-f DS-GVO: Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit . . . . .	158
c) Zusammenfassung zu den Grundsätzen der Datenverarbeitung . . . . .	159
B. Ermöglichende Strukturen im Datenschutzrecht . . . . .	159
I. Die Einwilligung und ihre Schranken: Reibungspunkte zwischen Privatautonomie und Regulierung . . . . .	161
1. Ermöglichungscharakter . . . . .	161
2. Zum Verhältnis von Einwilligung und Vertrag . . . . .	162
3. Grundtatbestand: Art. 6 Abs. 1 lit. a DS-GVO . . . . .	164
a) Allgemeiner Begriff der Einwilligung, Art. 4 Nr. 11 DS-GVO . . . . .	165
aa) Unmissverständlichkeit . . . . .	165
(1) Grundsatz: Ausdrücklich oder konkludent . . . . .	165
(a) Dimensionen der Unmissverständlichkeit . . . . .	165
(aa) Aktives Tun . . . . .	165
(bb) Gesonderte Einwilligung . . . . .	167
(b) Anwendung auf die drei Leitfälle . . . . .	170
(aa) Datenweiterleitung an Dritte (personalisierte Werbung) . . . . .	170
(bb) Datenerhebung durch Dritte ( <i>third-party tracking</i> ) . . . . .	171
(cc) Datenerhebung bei Dritten . . . . .	171
(2) Ausnahme: Nur ausdrücklich . . . . .	172
bb) Bestimmtheit . . . . .	172
cc) Informiertheit . . . . .	174
(1) Transparenz . . . . .	175
(2) Erkenntnismöglichkeit . . . . .	176
(3) Anwendung auf die drei Leitfälle . . . . .	177
(a) Datenweiterleitung an Dritte . . . . .	177
(b) Datenerhebung durch Dritte . . . . .	178
(c) Datenerhebung bei Dritten . . . . .	179
dd) Freiwilligkeit . . . . .	180
(1) Klares Ungleichgewicht und mangelnde Alternativen . . . . .	180
(2) Gesonderte Einwilligung? . . . . .	181
(3) Kopplungsverbot, Art. 7 Abs. 4 DS-GVO . . . . .	181
(a) Erforderlichkeit zur Vertragserfüllung . . . . .	182

(aa) Verhältnis zu Art. 6 Abs. 1 lit. b DS-GVO . . .	182
(bb) Drei Lesarten . . . . .	183
α. Ökonomischer Erforderlichkeitsmaßstab	183
β. Objektiver Erforderlichkeitsmaßstab . . . . .	184
γ. Subjektiver Erforderlichkeitsmaßstab . . . . .	185
(b) Abhängigkeit der Vertragserfüllung von der Einwilligung . . . . .	186
(aa) Die Relevanz der Marktmacht . . . . .	187
α. Literaturansichten . . . . .	187
β. Stellungnahme: Marktmacht als gewichtiger indirekter Bewertungsfaktor .	188
(bb) Dienst gegen monetäre Zahlung als zumutbare Alternative . . . . .	189
(c) Rechtsfolge: Widerlegliche Vermutung . . . . .	190
(aa) Widerlegung durch funktional äquivalentes Marktangebot . . . . .	191
(bb) Widerlegung durch hypothetische wirksame Leistungspflicht . . . . .	192
(cc) Beschränkung des Kopplungsverbots auf dringliche Angewiesenheit? . . . . .	192
(d) Grundrechtskonformität des Kopplungsverbots ..	193
(4) Weitere Abwägungsgesichtspunkte . . . . .	195
(a) Täuschung, Drohung und Zwang . . . . .	195
(b) Einwilligung im Beschäftigtenverhältnis, § 26 Abs. 2 BDSG . . . . .	195
(5) Anwendung auf die drei Leitfälle . . . . .	196
(a) Daten als Gegenleistung . . . . .	196
(aa) Vertragsinhalt bei „Daten als Gegenleistung“ mit datenbasiertem Grundmodell . . . . .	196
α. Legitimation durch Nutzerpflichten? . . . . .	197
β. Ablehnung aus teleologischer Perspektive	199
γ. Rekurs auf Verarbeiterpflichten . . . . .	200
(bb) Rabattmodell . . . . .	201
(cc) Data on top-Modell . . . . .	202
(b) Datenerhebung durch Dritte ( <i>tracking walls</i> ) . . . . .	202
(c) Datenerhebung bei Dritten . . . . .	202
(6) Zusammenfassung zur Freiwilligkeit . . . . .	203
ee) Einwilligung und Genehmigungsmöglichkeit . . . . .	204
b) Besondere Voraussetzungen, Art. 7–9 DS-GVO . . . . .	205
aa) Separierungsgebot, Art. 7 Abs. 2 S. 1 DS-GVO . . . . .	205
bb) Widerruf, Art. 7 Abs. 3 DS-GVO . . . . .	206
(1) Datenschutzrechtliche Rechtsfolgen . . . . .	206

(2) Vertraglicher Ausschluss oder Erschweris des Widerrufs? .....	208
(3) Vertragsrechtliche Folgen des Widerrufs .....	211
(a) Schadensersatz des Verantwortlichen .....	211
(aa) Anspruch auf Datenüberlassung .....	213
α. Nichtüberlassung von Daten .....	213
β. Überlassung von inkorrekten Daten .....	217
(bb) Anspruch auf Einwilligung .....	223
α. Bestehen des Anspruchs .....	223
β. Durchsetzbarkeit des Anspruchs .....	223
γ. Keine Pflichtverletzung durch Widerruf der Einwilligung .....	224
δ. Pflichtverletzung durch Nichtüberlassung von Daten oder Überlassung inkorrektur Daten .....	224
(cc) Zusammenfassung zum Schadensersatzanspruch bei Widerruf der Einwilligung .....	224
(b) Zurückbehaltungs- und Vertragslösungsrecht des Verantwortlichen .....	225
(aa) Synallagmatische Verknüpfung .....	225
α. Zurückbehaltungsrecht .....	225
β. Rücktritt, Kündigung und Wegfall der Geschäftsgrundlage .....	226
(bb) Konditionale Verknüpfung .....	228
(4) Zusammenfassung zum Widerruf .....	229
cc) Minderjährige, Art. 8 DS-GVO .....	230
(1) Mangelnder Gleichlauf mit dem BGB .....	231
(2) Partielle Auflösung durch Auslegung .....	233
dd) Sensitive Daten, Art. 9 DS-GVO .....	235
(1) Regelungsstruktur .....	235
(2) Unmittelbar und mittelbar sensitive Daten .....	236
c) Allgemeine Wirksamkeitsvoraussetzungen nach dem BGB ..	238
4. Cookies und andere Geräte-Identifizierer: Von der ePrivacy-Richtlinie über die DS-GVO zur ePrivacy-VO .....	238
a) Regelung nach der ePrivacy-Richtlinie .....	238
aa) Gesetzliche Grundlagen .....	239
(1) Art. 5 Abs. 3 ePrivacy-Richtlinie .....	239
(2) Deutsches Recht .....	240
bb) Voraussetzungen der Cookie-Einwilligung .....	241
(1) Das Erfordernis aktiver und gesonderter Einwilligung .....	241
(a) Rechtsprechung und Literatur bis 2019 .....	241

(b) Die Rechtssache <i>Planet49</i> . . . . .	242
(c) Folgen für das deutsche Recht . . . . .	243
(2) Informiertheit der Einwilligung . . . . .	244
(3) Freiwilligkeit der Einwilligung . . . . .	244
b) Maßgeblichkeit der DS-GVO bis zum Inkrafttreten der ePrivacy-VO . . . . .	245
aa) Die DS-GVO als Maßstab für Einwilligungen . . . . .	246
(1) Anwendbarkeit der DS-GVO . . . . .	246
(2) Konsequenzen ( <i>tracking walls</i> ) . . . . .	248
bb) Rückgriff auf andere Erlaubnistatbestände der DS-GVO	248
c) Ausblick: Die Regelung der ePrivacy-VO . . . . .	249
aa) Einwilligung durch Browsereinstellungen, Art. 9 Abs. 2 ePrivacy-VO-KommE . . . . .	251
bb) Möglichkeit der Verhinderung von <i>third-party</i> <i>tracking</i> , Art. 10 ePrivacy-VO-KommE . . . . .	251
cc) Regelung von <i>tracking walls</i> , Art. 8 Abs. 1a ePrivacy-VO-EP . . . . .	253
5. Eine kurze Kritik der Einwilligung . . . . .	255
a) Mangelnder direkter Nutzen für Betroffene . . . . .	255
aa) Rationale Ignoranz . . . . .	256
bb) Verhaltensökonomische Effekte . . . . .	256
cc) Faktische Grenzen der Einwilligung im IoT-Kontext . . . . .	257
b) Nutzen für Informationsintermediäre . . . . .	257
6. Zusammenfassung zur Einwilligung . . . . .	258
II. Vertragserforderliche Datenverarbeitung, Art. 6 Abs. 1 lit. b DS-GVO . . . . .	260
1. Ermöglichungs- bzw. Permissivitätscharakter . . . . .	260
2. Tatbestand . . . . .	261
a) Zivilrechtliche Wirksamkeit des Vertrags . . . . .	262
b) Erforderlichkeit . . . . .	262
aa) Vertragserfüllung . . . . .	262
bb) Erforderlichkeitsmaßstab . . . . .	263
(1) Subjektiver Erforderlichkeitsmaßstab . . . . .	263
(2) Relevanz von Nutzerpflichten? . . . . .	264
3. Konsequenzen für das Verhältnis zu Art. 7 Abs. 4 DS-GVO und für die drei Leitfälle . . . . .	264
4. Eine kurze Kritik der vertragserforderlichen Datenverarbeitung . . . . .	265
III. Datenübertragung, Art. 20 DS-GVO . . . . .	266
1. Ermöglichungscharakter . . . . .	267
2. Tatbestand . . . . .	267
3. Limitationen . . . . .	268

IV. Zusammenfassung zu den Ermöglichungsstrukturen im Datenschutzrecht .....	269
C. Regulatorische Strukturen im Datenschutzrecht .....	270
I. Erlaubnistatbestand, Art. 6 Abs. 1 lit. f DS-GVO .....	271
1. Relevanz .....	271
a) Ökonomische Relevanz .....	272
b) Rechtliche Relevanz .....	272
2. Tatbestand .....	273
a) Berechtigte Interessen .....	273
aa) Interessen des/der Verantwortlichen .....	273
bb) Interessen Dritter .....	274
b) Erforderlichkeit der Datenverarbeitung zur Interessenwahrung .....	275
c) Abwägung .....	275
aa) Überwiegen .....	275
bb) Wertungskriterien .....	276
(1) Grundsätzliche Wertungskriterien .....	276
(2) Residualwirkung privatautonomer Gestaltung .....	278
3. Anwendung auf die drei Leitfälle .....	279
a) Datenweiterleitung an Dritte ( <i>ad exchanges</i> und personalisierte Werbung) .....	279
aa) Grundsätzliche Abwägung .....	280
bb) Marktmacht .....	281
cc) Überraschungseffekt .....	282
b) Datenerhebung durch Dritte .....	283
c) Datenerhebung bei Dritten .....	283
4. Rechtssichere Operationalisierung für die beteiligten Akteure	284
5. Zusammenfassung zu Art. 6 Abs. 1 lit. f DS-GVO .....	286
II. Die Änderung der Verarbeitungszwecke, Art. 6 Abs. 4 DS-GVO	287
1. Relevanz .....	287
2. Kein eigener Erlaubnistatbestand .....	287
III. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO .....	289
1. Relevanz .....	290
2. Rechtfertigung .....	291
4. Verpflichtungsgrad .....	293
4. Inhaltliche Ausformung .....	294
a) Art. 25 Abs. 1 DS-GVO .....	294
b) Art. 25 Abs. 2 DS-GVO .....	295
c) Operationalisierung .....	296
5. Anwendung auf die drei Leitfälle .....	297
a) Datenweiterleitung an Dritte .....	297
b) Datenerhebung durch Dritte .....	298

c) Datenerhebung bei Dritten .....	300
IV. Co-Regulierung .....	300
1. Allgemeine Funktionen und Relevanz der Co-Regulierung . . .	301
2. Datenschutz-Folgenabschätzung, Art. 35 DS-GVO .....	302
a) Relevanz .....	302
b) Norminhalt .....	304
c) Anwendung auf die drei Leitfälle .....	305
aa) Datenweiterleitung an Dritte .....	305
bb) Datenerhebung durch Dritte .....	306
cc) Datenerhebung bei Dritten .....	306
3. Verhaltensregeln und Zertifizierungsverfahren .....	306
a) Genehmigte Verhaltensregel, Art. 40f. DS-GVO .....	307
b) Genehmigtes Zertifizierungsverfahren, Art. 42f. DS-GVO ..	309
D. Ergebnisse von §4 .....	309
§5 <i>Vernetzte Datenerhebung und -analyse im allgemeinen Privatrecht</i> . . .	313
A. Zum Verhältnis von unionalem Datenschutzrecht und mitgliedstaatlichem Privatrecht .....	314
I. Anwendungsvorrang des Unionsrechts .....	315
1. Direkte Kollision .....	318
a) Tatbestandliche Erfassung auf beiden Ebenen .....	318
b) Abschließende Regelung auf Unionsebene: Risikospezifität zum Ersten .....	319
2. Indirekte Kollision .....	320
a) Allgemeine Grenzen des Effektivitätsgrundsatzes .....	322
b) Methodische Ausfüllung des Effektivitätsgrundsatzes .....	322
aa) Zweistufige Prüfung .....	323
(1) Risikospezifität zum Zweiten .....	324
(2) Zielkompatibilität .....	324
bb) Folgerung: Sachgerechte Ergänzung des Unionsrechts durch nationales Recht .....	325
cc) Methodisches Ergebnis .....	325
c) Operationalisierung für das Datenprivatrecht .....	326
aa) Ziele des unionalen Datenschutzrechts .....	326
bb) Unionsrechtskompatible nationale Zielsetzungen .....	328
(1) Binnenmarktkompatibilität .....	329
(2) Datenschutzkompatibilität .....	330
(3) Sonstige Zielsetzungen .....	331
d) Ergebnis zur indirekten Kollision .....	332
3. Zusammenfassung zum Anwendungsvorrang .....	332
II. Sachintegration ebenengleichen Rechts .....	333
1. Rechtsbereichsübergreifende Auslegung .....	335
a) Die Fälle <i>Pereničová und Perenič</i> sowie <i>Bankia</i> .....	336

b) Die Ausstrahlungswirkung im Unionsrecht .....	337
2. Konkurrierende Rechtsfolgebestimmungen .....	339
a) Kein grundsätzlicher Vorrang des Datenschutzrechts .....	339
b) Grundrechtlich geprägte Normenkoordination .....	340
aa) Explizite Regelung eines Wertungsvorrangs .....	341
bb) Impliziter Wertungsvorrang: Risikospezifizität zum Dritten .....	341
(1) Abschließende Adressierung eines Risikos im Datenschutzrecht .....	341
(2) Adressierung eines zusätzlichen Risikos in anderen Rechtsbereichen .....	342
III. Zusammenfassung zum Verhältnis von Datenschutzrecht und Privatrecht .....	342
B. Ermöglichende Strukturen im allgemeinen Privatrecht .....	343
I. Einwilligung und Datenüberlassung als Gegenleistung .....	345
II. Privatrechtliche Rechtsgeschäftslehre und datenschutzrechtlicher Einwilligungstatbestand .....	348
1. Die Rechtsnatur der Einwilligung und der Rückgriff auf nationales Recht .....	348
a) Die Einwilligung als geschäftsähnliche Handlung .....	349
b) Punktuelle Rückgriffsmöglichkeit .....	350
aa) Keine allgemeine Rechtsgeschäftslehre in der DS-GVO	351
bb) Keine vollständige Präklusion nationaler Regelungen: Wahrung des Effektivitätsgrundsatzes .....	353
cc) Die Bedeutung der Rechtssachen <i>Rabobank</i> und <i>Schyns</i>	354
dd) Punktuelle Ergänzung der DS-GVO durch nationales Recht .....	355
2. Einzelne Probleme der Rechtsgeschäftslehre .....	356
a) Einwilligungsfähigkeit .....	356
b) Subjektiver Tatbestand, insbesondere Einwilligungsbewusstsein .....	357
c) Abgabe und Zugang .....	359
aa) Abgabe .....	359
bb) Zugang .....	360
d) Stellvertretung .....	362
e) Die Behandlung von Willensmängeln .....	364
aa) Widerrechtliche Drohung .....	364
(1) Fortbestehendes Interesse der betroffenen Person .....	365
(2) Doppelwirkung im Mehrebenenrecht? .....	366
bb) Arglistige Täuschung .....	367
cc) Erklärungs- und Inhaltsirrtum .....	367
(1) Grundsätzliche Entbehrlichkeit neben dem Widerruf	368
(2) Anfechtung im Fall von § 142 Abs. 2 BGB .....	369

dd) Beachtlicher Motivirrtum .....	369
3. Zusammenfassung zu Rechtsgeschäftslehre und Einwilligung	369
III. Vertragsschluss und DS-GVO .....	371
1. Ermöglichungsstrukturen zwischen Erstanbieter und Primärnutzer .....	371
2. Drittbezogene Ermöglichungsstrukturen .....	372
a) Einbeziehung von Drittanbietern .....	373
aa) Mehrseitiger Vertrag .....	374
(1) Grundsätzlich nur ausdrücklicher Vertragsschluss ...	375
(2) Ausnahmsweise konkludenter Vertragsschluss bei salientem Hinweis .....	376
bb) Bilateraler Vertrag mit Drittanbieter kraft Stellvertretung .....	377
cc) Vertrag zugunsten Dritter .....	378
dd) Bedingung zugunsten Dritter .....	379
(1) Datenschutzrechtliche Irrelevanz der drittbegünstigenden Bedingung .....	379
(2) Folgen für die Vertragsauslegung .....	380
ee) Zusammenfassung zur Einbeziehung von Drittanbietern .....	381
b) Einbeziehung von Drittnutzern und unbeteiligten Dritten ..	381
aa) Eigener Vertrag kraft Nutzung .....	381
(1) Bewusste Nutzung .....	382
(a) Angebot des Anbieters .....	382
(b) Annahme durch den Drittnutzer .....	384
(aa) Bestimmung der Identität des Anbieters ....	384
(bb) Erklärungsbewusstsein bei kurzzeitiger Nutzung .....	385
α. Mangelndes Erklärungsbewusstsein bei § 151 S. 1 BGB .....	385
β. Besonderheiten im Rahmen digitaler Austauschprozesse .....	387
(cc) Unmissverständlichkeit der Annahme bei nicht primär nutzungsorientierter Handlung	388
(c) Lösungsmöglichkeiten .....	390
(2) Erhebung bei Unbeteiligten .....	391
(3) Zusammenfassung zum eigenen Vertrag mit Drittnutzern .....	391
bb) Vertrag zugunsten Dritter .....	392
cc) Vertrag mit Schutzwirkung zugunsten Dritter .....	392
(1) Tatbestandliche Voraussetzungen .....	393
(2) Vereinbarkeit mit Unionsrecht .....	394
dd) Drittschadensliquidation .....	395



3. Zusammenfassung zu Vertragsschluss und DS-GVO .....	395
C. Regulatorische Strukturen im allgemeinen Privatrecht .....	397
I. § 134 BGB: Erstreckung der Datenschutzrechtswidrigkeit auf das Rechtsgeschäft? .....	397
1. Verträge mit Betroffenen: Entkopplung von Datenschutzrecht und Vertragsrecht .....	398
a) Vorrang der datenschutzrechtlichen Abwicklung .....	400
b) Umkehrung der Schutzrichtung der DS-GVO .....	402
c) Überlegenheit gegenüber anderen dogmatischen Figuren ....	404
aa) Halbseitige Teilnichtigkeit .....	404
bb) Rechtliche Unmöglichkeit, Geschäftsgrundlage und Nichtigkeit nach § 134 BGB .....	406
(1) Anspruch auf Überlassung von Daten .....	407
(2) Anspruch auf Einwilligung.....	408
(a) Partielle Verknüpfung von Einwilligung und Vertrag .....	409
(aa) Wirksame Einwilligung als Geschäftsgrundlage .....	409
(bb) Keine Verletzung des Effektivitätsgrundsatzes .....	411
(cc) Rechtsfolgen für den Vertrag .....	412
(b) Modifikationen der Rückabwicklung .....	413
2. Verträge zwischen Dritten: Kopplung von Datenschutzrecht und Vertragsrecht .....	414
a) Nichtigkeit nach § 134 BGB .....	414
b) Einordnung der bisherigen Rechtsprechung .....	415
3. Zusammenfassung .....	417
II. Inhaltskontrolle im weiteren Sinne .....	417
1. AGB-Kontrolle .....	418
a) Anwendbarkeit neben der DS-GVO .....	419
b) Sachliche Anwendbarkeit: Vertragsbedingungen .....	422
c) Einbeziehungskontrolle .....	423
aa) Zumutbare Möglichkeit der Kenntniserhebung, § 305 Abs. 2 Nr. 2 BGB .....	423
bb) Überraschende Klauseln, § 305c Abs. 1 BGB .....	424
(1) Datenschutzrechtlicher Überraschungseffekt? .....	425
(2) Einbeziehung Dritter .....	426
d) Transparenzkontrolle .....	426
e) Inhaltskontrolle .....	430
aa) Kontrollfähigkeit, § 307 Abs. 3 S. 1 BGB .....	430
(1) Grundsatz: Mangelnde Kontrollfähigkeit des Hauptgegenstands des Vertrags und des Preis-/ Leistungsverhältnisses .....	430

(2) Zur Kontrollfähigkeit der Einwilligung . . . . .	433
(3) Zur Kontrollfähigkeit von Vertragsklauseln . . . . .	434
(a) Kontrollfähigkeit der Verpflichtung zur Datenüberlassung oder Einwilligung . . . . .	434
(aa) Monetäres Grundmodell: Preisnebenabreden	435
(bb) Datenbasiertes Grundmodell: Preishauptabreden und teleologische Reduktion . . . . .	435
α. Gründe für fehlende Kontrollfähigkeit nach Art. 4 Abs. 2 der Klauselrichtlinie . . .	436
β. Marktversagen bei der Kontrolle des „Datenpreises“ . . . . .	437
(b) Kontrollfähigkeit des Preis-/ Leistungsverhältnisses . . . . .	439
(c) Kontrollfähigkeit von Leistungsbeschreibungen . .	440
(4) Ergebnis . . . . .	441
bb) Grundsätze der unangemessenen Benachteiligung . . . . .	442
(1) § 307 Abs. 2 Nr. 1 BGB . . . . .	442
(a) Datenschutzrecht allgemein als Maßstab . . . . .	442
(b) Grundsätze der Datenverarbeitung als spezieller Maßstab . . . . .	443
(2) § 307 Abs. 2 Nr. 2 BGB . . . . .	445
(3) § 307 Abs. 1 S. 1 BGB . . . . .	445
(a) Die Rechtsprechung von EuGH und BGH . . . . .	445
(b) Unangemessenheitskriterien für Hauptleistungspflichten . . . . .	447
(aa) Der <i>Aziz</i> -Test . . . . .	448
(bb) Der relevante Referenzakteur . . . . .	450
(c) Ergebnis . . . . .	452
cc) Anwendung auf die drei Leitfälle . . . . .	454
(1) Datenweiterleitung an und Datenerhebung durch Dritte . . . . .	454
(a) Einwilligung . . . . .	454
(b) Vertragsklauseln . . . . .	455
(aa) Verpflichtung zur Einwilligung . . . . .	456
(bb) Verpflichtung zur Datenüberlassung . . . . .	456
(cc) Weite vertragliche Leistungspflichten . . . . .	456
(2) Vertragliche Einbindung Dritter . . . . .	459
dd) Erweiterung der §§ 308 f. BGB . . . . .	459
f) Rechtsfolgen: Das Schicksal des Vertrags . . . . .	459
aa) Deutsche Rechtsprechung und Literatur zu § 306 BGB . .	460
bb) Die Rechtsprechung des EuGH . . . . .	461

(1) Geltungserhaltende Reduktion und selektive Streichung der Klausel . . . . .	461
(2) Gesamtnwirksamkeit des Vertrags . . . . .	462
(3) Vertragliche Lückenfüllung . . . . .	463
cc) Lösungen für das Datenprivatrecht . . . . .	464
(1) Unwirksame Einwilligung . . . . .	465
(2) Unwirksame Hauptleistungspflicht . . . . .	465
(3) Unwirksame weite Nebenleistungspflicht . . . . .	468
g) Wechselwirkungen mit der DS-GVO . . . . .	469
aa) Keine Grundlage der Datenverarbeitung nach Art. 6 Abs. 1 lit. a, b DS-GVO . . . . .	469
bb) Auswirkungen auf Art. 6 Abs. 1 lit. f DS-GVO . . . . .	469
cc) Rechtsgebietsübergreifende Fairness: Auswirkungen auf Art. 5 Abs. 1 lit. a Var. 2 DS-GVO . . . . .	470
dd) Methodisches Ergebnis . . . . .	473
h) Zusammenfassung zur AGB-Kontrolle . . . . .	473
2. § 138 BGB . . . . .	476
a) Anwendbarkeit neben der DS-GVO . . . . .	476
aa) Verträge . . . . .	476
bb) Einwilligung . . . . .	477
(1) Preis-/Leistungs-Verhältnis: Datenbasierte <i>laesio</i> <i>enormis</i> . . . . .	478
(a) Risikospezifizität gegenüber Art. 5 Abs. 1 lit. c DS-GVO . . . . .	479
(b) Risikospezifizität gegenüber Art. 5 Abs. 1 lit. a Var. 2 DS-GVO . . . . .	480
(2) Sonstige Sittenwidrigkeitstatbestände . . . . .	480
b) Tatbestand der Sittenwidrigkeit: Wucherähnliches Geschäft . . . . .	483
aa) Einwilligung . . . . .	486
(1) Der unsichere Marktwert von Leistung und Gegenleistung . . . . .	486
(2) Qualitative Abwägung . . . . .	487
(a) Bestimmbarer Marktwert der Anbieterleistung . . . . .	487
(b) Kein bestimmbarer Marktwert der Anbieterleistung . . . . .	488
(c) Die Rolle des Referenzakteurs – Maßvolle Personalisierung . . . . .	489
bb) Vertrag . . . . .	491
cc) Ergebnis zum wucherähnlichen Geschäft . . . . .	491
c) Rechtsfolge . . . . .	492
d) Wechselwirkungen mit der DS-GVO . . . . .	493
e) Zusammenfassung zu § 138 BGB . . . . .	493

3. § 242 BGB .....	494
a) Anwendbarkeit der erweiterten Inhaltskontrolle:	
Dogmatik des BGB .....	495
b) Anwendbarkeit bei Rechtsmissbrauch und als	
Ausübungskontrolle: Anwendungsvorrang der DS-GVO? ..	496
aa) Einwilligung .....	497
bb) Vertrag .....	499
c) Wechselwirkungen mit der DS-GVO .....	500
d) Zusammenfassung zu § 242 BGB .....	502
III. Haftung .....	502
1. Anwendbarkeit zivilrechtlicher Haftungsnormen neben der	
DS-GVO .....	503
2. Vertragliche Haftung .....	506
a) Wesentliche Pflichten der DS-GVO als vertragliche	
Nebenpflichten nach § 241 Abs. 2 BGB .....	507
aa) Rechtslage im Bereich der Anlageberatung .....	507
bb) Übertragung auf datenschutzrechtliche Sachverhalte ...	508
b) Die Anwendbarkeit von § 278 BGB im Rahmen der	
Datenverarbeitung .....	509
aa) Tatbestandsvoraussetzungen .....	509
bb) Kein Anwendungsvorrang der DS-GVO .....	510
c) Zur Anwendbarkeit von § 280 Abs. 1 BGB .....	512
d) Zusammenfassung zu vertraglichen Nebenpflichten .....	514
3. Haftung aus <i>culpa in contrahendo</i> und Bereicherungsrecht ...	514
4. Deliktische Haftung .....	515
a) § 823 Abs. 1 BGB i. V. m. sonstigen, datenschutzbezogenen	
Rechten .....	516
aa) Das unionale Datenschutzgrundrecht .....	516
bb) Das deutsche allgemeine Persönlichkeitsrecht im	
weiteren Sinne .....	519
(1) Recht auf informationelle Selbstbestimmung .....	520
(a) Art. 82 DS-GVO als <i>lex specialis</i> im Allgemeinen	520
(b) Der Bereich der Öffnungsklauseln .....	521
(2) Recht auf Gewährleistung der Integrität und	
Vertraulichkeit von informationstechnischen	
Systemen .....	523
(3) Allgemeines Persönlichkeitsrecht .....	525
(a) Vorrang von § 823 Abs. 1 BGB i. V. m. dem	
allgemeinen Persönlichkeitsrecht nach dem	
Bundesverfassungsgericht? .....	525
(b) Vorrang von Art. 82 DS-GVO nach dem	
Unionsrecht .....	526

(aa) Untrennbarkeit von Datenschutzrecht und Äußerungsrecht im datenverarbeitenden Bereich . . . . .	526
(bb) Differenzen zwischen Grundrechten und Haftungsrecht . . . . .	528
(cc) Mangelnde Risikospezifität . . . . .	529
(c) Zusammenfassung zum Verhältnis von allgemeinem Persönlichkeitsrecht und Art. 82 DS-GVO . . . . .	533
b) § 823 Abs. 2 BGB i. V. m. Normen der DS-GVO . . . . .	533
c) § 824 BGB . . . . .	534
d) § 826 BGB . . . . .	535
e) § 831 BGB . . . . .	537
f) Zusammenfassung zu deliktischen Ansprüchen . . . . .	537
D. Ergebnisse von § 5 . . . . .	538
Teil 3: Reformperspektiven . . . . .	545
§ 6 <i>Präferenzverwirklichung durch Technikgestaltung</i> . . . . .	547
A. Autonomie, Informiertheit und Datenschutzpräferenzen . . . . .	548
B. Minimierung von Datenschutzrisiken durch Technik . . . . .	553
I. <i>Privacy-enhancing technologies</i> . . . . .	555
1. Relevante nutzerbasierte Techniken (Selbstdatenschutz) . . . . .	556
a) Verschlüsselung . . . . .	556
b) Identity-Management-Systeme . . . . .	558
c) Anti-Tracking-Tools . . . . .	559
2. Rechtlicher Rahmen . . . . .	561
a) Allgemeine Kriterien . . . . .	562
b) Unterstützungspflicht . . . . .	562
c) Tolerierungspflicht . . . . .	563
3. Anreize und Beschränkungen . . . . .	564
II. Rechtmäßigkeitskontrolle durch maschinelles Lernen . . . . .	566
1. Relevante Techniken . . . . .	567
a) Automatisierte Kontrolle der Datenschutzerklärung . . . . .	567
aa) Modelle zur Unterstützung von Nutzern . . . . .	568
bb) Modelle zur Unterstützung von Aufsichtsbehörden . . . . .	570
b) Automatisierte Kontrolle der Nutzungsbedingungen . . . . .	571
2. Rechtlicher Rahmen . . . . .	572
3. Anreize und Beschränkungen . . . . .	573
III. Zusammenfassung zur Minimierung von Datenschutzrisiken durch Technik . . . . .	576

C. Entscheidungsunterstützung durch Recht .....	577
I. Verbesserung der Einwilligung und der Präferenzkommunikation ..	578
1. Transparenzbasierte Ansätze .....	578
a) Verbesserungsmöglichkeiten .....	579
aa) Kognitive Optimierung des Inhalts .....	579
(1) Verständlichkeit der Sprache .....	579
(2) Staffelung der Information auf mehreren Ebenen ( <i>multi-layered notices</i> ) .....	580
(a) Empirischer Nutzen .....	581
(b) Pflicht nach der DS-GVO? .....	583
(3) Icons .....	585
bb) Timing: Kontextualisierung und Zeitabhängigkeit .....	587
b) Bewertung .....	588
2. Verhaltensbasierte Ansätze: <i>privacy nudges</i> .....	590
a) Interventionsmöglichkeiten .....	590
b) Bewertung .....	591
3. Technologiebasierte Ansätze: Wege zu einer automatisierten Kommunikation von Datenschutzpräferenzen .....	593
a) Technische Möglichkeiten .....	594
aa) Manuelles Datenschutz-Dashboard .....	594
bb) Automatisierte Kontrollinstrumente .....	597
b) Bewertung .....	599
aa) Potenzial .....	599
bb) Limitationen .....	600
(1) Technische Ebene: Technikreife .....	601
(2) Ökonomische Ebene: Anreize und Präferenzen .....	601
(a) Kontrolle und Veröffentlichungsbereitschaft .....	602
(b) Formung und Modellierung von Präferenzen .....	603
(3) Regulatorische Ebene .....	604
c) Eingeschränkter rechtlicher Reformbedarf .....	605
aa) Rechtssichere automatisierte und autonome Kommunikation von Präferenzen .....	605
(1) Einwilligungsregime nach der DS-GVO .....	605
(a) Automatisierte Einwilligung .....	606
(aa) Schwach autonome Datenschutzassistenten ..	606
(bb) Browser-Spezifikationen .....	608
(b) Autonome Einwilligung .....	608
(aa) Grundsätze der Zurechnung der Erklärung zum Nutzer .....	609
(bb) Dogmatische Umsetzung: §§ 164 ff. BGB analog .....	610

(2) Automatisierter und autonomer Widerspruch gegen bestimmte Formen der Datenverarbeitung, Art. 21 f. DS-GVO .....	613
(a) Art. 21 f. Abs. 2 DS-GVO .....	613
(b) Art. 21 Abs. 1 S. 1 und Abs. 6 DS-GVO .....	614
(c) Art. 22 Abs. 1 DS-GVO .....	615
(3) Entwicklungsperspektiven .....	615
bb) Interoperabilität durch Datenschutz-Schnittstelle .....	616
4. Zusammenfassung zur Verbesserung der Einwilligung und der Präferenzkommunikation .....	618
a) Bewertung der verschiedenen Ansätze .....	618
b) Rechtlicher Reformbedarf .....	619
II. Verbesserung reeller Wahlmöglichkeiten: Das Recht auf eine datenschonende Option .....	620
1. Grundidee: Datenschonende Option und <i>privacy score</i> .....	621
a) Datenschonende Option <i>de lege lata</i> und <i>de lege ferenda</i> ...	621
b) Grundlegender Inhalt des Vorschlags: Drei Weichenstellungen .....	622
aa) Pflichtangebot der datenschonenden Option .....	623
bb) Verbindung mit <i>privacy scores</i> .....	623
cc) Sektorspezifizität .....	624
c) Argumente .....	624
aa) Marktergänzende Alternativen zur Durchsetzung von Datenschutzpräferenzen .....	624
bb) Rechtssicherheit für Anbieter und Nutzer mit niedrigen Datenschutzpräferenzen .....	626
cc) Aktive Wahl statt rationaler Ignoranz .....	626
dd) Förderung von rationalen Entscheidungen und Reduzierung von Preisunschärfe durch <i>privacy scores</i> ...	627
2. Tatsächliche Voraussetzungen .....	628
a) Hinreichende Zahlungsbereitschaft .....	628
aa) Zahlungsbereitschaft und Salienz .....	629
bb) Datenschonende Option als Minderheitenschutz .....	632
b) Berechnung des <i>privacy score</i> .....	632
3. Implementierung der Wahlmöglichkeit .....	634
a) Wahlmöglichkeiten .....	635
aa) Vertraglich erforderliche vs. nicht erforderliche Daten ...	635
bb) Wahl der Cookies .....	636
(1) Typen von Cookies .....	636
(2) Datenschonende Cookies .....	637
b) Ausübung der Wahl ( <i>agreement technologies</i> ) .....	638
4. Sektorspezifizität .....	639
a) Soziale Netzwerke .....	640

b) Suchmaschinen .....	641
c) IoT-Geräte, besonders autonome Fahrzeuge .....	642
5. Einwände .....	643
a) Wirkungslosigkeit .....	643
aa) Wirksamkeit für Altnutzer .....	644
bb) Wirksamkeit trotz Datenerhebung an anderer Stelle .....	644
cc) Strategische Nutzung bei sensiblen Daten .....	645
b) Zwei-Klassen-Datengesellschaft .....	645
aa) Pareto-Verbesserung .....	646
bb) Preiskontrolle .....	646
cc) Kein Recht auf völlig kostenlose Leistung .....	649
c) Mangelnde Stabilität von Präferenzen .....	649
d) Mangelnde Rationalität .....	650
6. Grundrechtskonformität .....	650
a) Betroffene unionale Grundrechtspositionen .....	650
b) Rechtfertigung .....	651
7. Zusammenfassung zum Recht auf eine datenschonende Option	654
D. Ergebnisse von § 6 .....	655

Teil 4: Schluss .....	657
-----------------------	-----

§ 7 <i>Lösungsansätze für die drei rechtlichen Herausforderungen</i> , de lege lata und de lege ferenda .....	659
--	-----

A. Erste rechtliche Herausforderung: Multirelationalität von Daten .....	659
I. Regulatorische Dimension .....	660
II. Ermöglichende Dimension .....	662
B. Zweite rechtliche Herausforderung: Ambivalenz von Nutzen und Risiken .....	662
I. Marktversagen .....	663
II. Soziale Risiken .....	664
C. Dritte rechtliche Herausforderung: Heterogenität von Datenschutzpräferenzen .....	666
I. Das Dilemma individueller Kontrolle .....	666
II. Ein Lösungsvorschlag in drei Schritten .....	666

§ 8 <i>Wesentliche Ergebnisse der Arbeit in zehn Thesen</i> .....	669
---	-----

Literaturverzeichnis .....	673
----------------------------	-----

Sachregister .....	741
--------------------	-----





## § 1 Einführung

Das neue unionale Datenschutzrecht ist, entgegen mancher Befürchtung,<sup>1</sup> kein *law of everything*. Vielmehr müssen unterschiedliche Rechtsmaterien ineinandergreifen, um eine sachgerechte Regelungsstruktur im Schnittbereich von Datenschutzrecht und Privatrecht aufzubauen. Die Bestimmung des Verhältnisses dieser Rechtsmaterien, insbesondere von Datenschutzrecht und bürgerlichem Recht, ist ein zentrales Anliegen dieser Untersuchung. Denn die Verschränkung unterschiedlicher Technologieformen fordert mehr denn je ein rechtsbereichsübergreifendes Verständnis von juristischer Dogmatik und ein interdisziplinär fundiertes Konzept von Regulierung.

### A. Daten in der Dauerschleife

Die Kombination unterschiedlicher Technologieformen schreitet rasant voran. Ob Tracking-Instrumente, künstliche Intelligenz oder das Internet der Dinge:<sup>2</sup> Neue Technologien konvergieren zunehmend gegen ein umfassendes *Internet of Everything*,<sup>3</sup> in dessen Rahmen nicht nur analoge und virtuelle Sphären kurzgeschlossen,<sup>4</sup> private und öffentliche Räume verschränkt,<sup>5</sup> sondern

---

<sup>1</sup> Purtova, 10 *Law, Innovation and Technology* 2018, 40 (41, 75 ff.); siehe auch Lynskey, 21 *German Law Journal* 2020, 80 (82); kritisch Clifford, *The Legal Limits to the Monetisation of Online Emotions*, 2019 Rn. 196–199.

<sup>2</sup> Zu diesen Basistechnologien ausführlich unten, § 2 A.–C.

<sup>3</sup> Überblick über den Stand der Entwicklung bei Breiner/Sriram/Subrahmanian, AAAI Spring Symposium Series 2018, 107 (107 ff.); Velasquez et al., 9 *Journal of Internet Services and Applications* 2018, 14 (14 ff.); Di Martino et al., in: Di Martino et al. (Hrsg.), *Internet of Everything*, 2018, 1 (1 ff.); zum Entwicklungspotenzial DeNardis, *The Internet in Everything*, 2020, 3 ff.; Shojafar/Sookhak, *International Journal of Computers and Applications* 2019, DOI: 10.1080/1206212X.2019.1575621, 1 (1); Miraz et al., 10 *Future Internet* 2018, Article 68, 1 (5); Botta et al., 56 *Future Generation Computer Systems* 2016, 684 (688); Miraz et al., *IEEE Internet Technologies and Applications (ITA)* 2015, 219 (220 f.); Sriram, 17(3) *IT Professional* 2015, 60; Abdelwahab et al., 1 *IEEE Internet of Things Journal* 2014, 276 (276); Jara/Ladid/Gómez-Skarmeta, 4 *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 2013, 97 (98); Evans, *The Internet of Everything*, Cisco Internet Business Solutions Group (IBSG), Report, 2012, 3 ff.; siehe auch unten, § 2 D.

<sup>4</sup> DeNardis, *The Internet in Everything*, 2020, 8–11; Hildebrandt, *Smart Technologies and the End(s) of Law*, 2015, 41 f.

<sup>5</sup> Siehe etwa Hacker, 7 *International Data Privacy Law* 2017, 266 (272); zur Smart City repräsentativ Madaan/Abad/Sastry, 34 *Computer Law & Security Review* 2018, 125 (128 ff.);

auch Marktprozesse neu integriert werden.<sup>6</sup> Motor dieser Dynamik ist nicht zuletzt der bereits seit einigen Jahren zu konstatierende Einsatz personenbezogener Daten als funktionales Geldäquivalent.<sup>7</sup> Schon an der zunehmenden Nutzung von autonomen und vernetzten Fahrzeugen<sup>8</sup> oder von Gesichtserkennungssoftware durch private und öffentliche Akteure<sup>9</sup> zeigt sich jedoch, dass die technische Entwicklung mittlerweile weit darüber hinausgeht. Mit der wachsenden Vernetzung von Alltagsgeräten, onlinebasierten Dienstleistungen und öffentlichen Infrastrukturen entstehen genuin techno-physische Architekturen,<sup>10</sup> die durch eine Dauerschleife von einander durchdringenden, sich gegenseitig verstärkenden Analyse-Systemen gekennzeichnet sind:<sup>11</sup> Tracking-Technologien erheben Daten, die mithilfe von Techniken maschinellen Lernens analysiert und zur Steuerung von Geräten des Internets der Dinge eingesetzt werden, die ihrerseits wiederum neue Daten erheben und in den Zyklus einspeisen. Die Systeme sind entwicklungs-offen,<sup>12</sup> doch der Kreis der Daten schließt sich.

Die Integration dieser Prozesse in ein *Internet of Everything* ist nicht unumstritten. Die Utopie der einen<sup>13</sup> ist, wie so häufig, die Dystopie der ande-

---

*Cobbe/Morison*, in: Slautsky (Hrsg.), *The Conclusions of the Chaire Mutations de l'Action Publique et du Droit Public*, 2019.

<sup>6</sup> Siehe nur *Goldfarb/Greenstein/Tucker*, in: Goldfarb/Greenstein/Tucker (Hrsg.), *Economic Analysis of the Digital Economy*, 2015, 1, sowie die weiteren Beiträge in diesem Band; ferner *Urbach*, in Schmidt-Kessel/Kramme, *Geschäftsmodelle in der digitalen Welt*, 2017, 39; siehe auch die Nachweise in § 2, Fn. 99 zum *consumer preference modeling*.

<sup>7</sup> Siehe unten, § 3 A.II.

<sup>8</sup> Dazu etwa *Abeck et al.*, *INFORMATIK* 2019, 125 (125 ff.); *Crane/Loguel/Pilz*, 23 *Michigan Telecommunications and Technology Law Review*, 2016, 191 (199 f.).

<sup>9</sup> Siehe nur die (kritische) Debatte über den zunehmenden Einsatz von Gesichtserkennungssoftware in westlichen Demokratien: *Europäische Kommission*, Weißbuch zur Künstlichen Intelligenz, COM(2020) 65 final, 25 f.; *Coester/Fuhlert*, *DuD* 2020, 48 (49 ff.); *Hill*, *The Secretive Company That Might End Privacy as We Know It*, *New York Times* (18.1.2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; *Garvie*, *Garbage In, Garbage Out. Face Recognition on Flawed Data*, *Center on Privacy & Technology*, Georgetown Law, Report, 2019; *Draper*, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, *New York Times* (13.3.2018), <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>; *Garvie/Bedoyal/Frankle*, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, *Center on Privacy & Technology*, Georgetown Law, Report, 2016; zur VR China *Zoll*, *Überwachung mit Gesichtserkennung: Made in China, erprobt in Xinjiang und weltweit exportiert*, *NZZ* (3.12.2019), <https://www.nzz.ch/international/china-nutzt-gesichtserkennung-fuer-ueberwachung-und-exportiert-sie-ld.1525690>; zur Technologie grundlegend *Lawrence et al.*, 8 *IEEE Transactions on Neural Networks* 1997, 98; siehe auch *Y. Sun et al.*, *Deepid3: Face recognition with very deep neural networks*, Working Paper, 2015, <https://arxiv.org/abs/1502.00873>; *Goodfellow/Bengio/Courville*, *Deep Learning*, 2016, 23 f.; *Ranjan et al.*, 35 *IEEE Signal Processing Magazine* 2018, 66.

<sup>10</sup> Siehe nur *DeNardis*, *The Internet in Everything*, 2020, 25 ff.; vgl. auch *Grünberger*, *AcP* 218 (2018), 213 (235).

<sup>11</sup> Siehe unten, § 3 D.

<sup>12</sup> *Breiner/Sriram/Subrahmanian*, *AAAI Spring Symposium Series* 2018, 107 (107 f.).

<sup>13</sup> Repräsentativ *Evans*, *The Internet of Everything*, *Cisco Internet Business Solutions*

ren.<sup>14</sup> Welchen Weg die technische Entwicklung letztlich nehmen wird, lässt sich naturgemäß nur schwer prognostizieren; umso dringlicher ist jedoch deren rechtliche Begleitung. Gesichert scheint dabei einzig, dass die Tendenz zu einer zunehmenden Kombination von Datensätzen<sup>15</sup> und Technologieformen geht.<sup>16</sup> Man muss nicht das Menetekel des chinesischen Sozialkreditsystems<sup>17</sup> an die Wand malen, um zu erkennen, dass darin gesellschaftliche und ökonomische Kräfte liegen, denen nachgerade revolutionäres Potenzial innewohnt.<sup>18</sup> So hat etwa der Einsatz von Daten als Zahlungsmittel die unmittelbare Folge, dass – ökonomisch gesprochen – die Budgetrestriktionen von Verbrauchern erheblich erweitert werden.<sup>19</sup> Darin liegt nicht zuletzt ein tendenziell egalitärer Impetus: Daten kann jede Person in ähnlichem Umfang als Geldäquivalent einsetzen.<sup>20</sup> Zugleich stellt diese Entwicklung eine immense Herausforderung für ihre datenschutz- und freiheitskonforme Ausgestaltung dar, insbesondere auch deshalb, weil die Präferenzen hinsichtlich des Einsatzes von Daten als Zahlungsmittel erheblich zwischen den Nutzern divergieren.<sup>21</sup>

Zugleich ist der beschriebene Prozess durch die Besonderheit gekennzeichnet, dass die Selbstentäußerung von Privatheit in ganz erheblichem Maße durch eine (untechnisch gesprochen<sup>22</sup>) freiwillige Offenlegung von personenbezogenen Daten angetrieben wird.<sup>23</sup> Angesichts der zunehmenden Unentziehbarkeit aus der Dauerschleife von Datenerhebung, -analyse und datenbasierter Aktuation stellt sich jedoch die Frage, ob sich die bisherigen rechtlichen Kategorien, die selbstbestimmtes Handeln in digitalen Kontexten garantieren sollten – ins-

---

Group (IBSG), Report, 2012, 3ff.; *Breiner/Srivam/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (107f.).

<sup>14</sup> Siehe etwa *Zuboff*, *The Age of Surveillance Capitalism*, 2019, besonders deutlich in Kapitel 11 II. und Kapitel 12 VII.; *Auer*, *Zum Erkenntnisziel der Rechtstheorie*, 2018, 63; früh bereits nuanciert kritisch *Picard*, *Affective Computing*, 1997, 118f., 244; Analyse des *Internet of Everything* als Machtstruktur und Governance-Herausforderung bei *DeNardis*, *The Internet in Everything*, 2020, 17ff., 212ff.

<sup>15</sup> *Bruneteau et al.*, *Usage-Based Insurance*. Global Study, 2016, 15.

<sup>16</sup> Siehe nochmals unten, §2 D.

<sup>17</sup> Dazu nur *Liang et al.*, *10 Policy & Internet* 2018, 415; *Genzsch*, in: *Loitsch* (Hrsg.), *China im Blickpunkt des 21. Jahrhunderts*, 2019, 129.

<sup>18</sup> *DeNardis*, *The Internet in Everything*, 2020, 59ff.; *Hildebrandt*, *Smart Technologies and the End(s) of Law*, 2015, 45ff.; kritische Zuspitzung bei *Zuboff*, *The Age of Surveillance Capitalism*, 2019, vor allem Kapitel 13.

<sup>19</sup> Siehe unten, §3 B.I.1.c).

<sup>20</sup> Vgl. den provokativen Vorschlag bei *Arrieta-Ibarra et al.*, 108 *AEA Papers and Proceedings* 2018, 38 (39f.) zu *data as labor*; dass manche personenbezogenen Daten stärker nachgefragt werden und mehr Wert haben als andere, ist zwar nicht in Abrede zu stellen, siehe nur *Bundesverband der digitalen Wirtschaft*, *Data Economy*, 2018, 15f. sowie unten, §3 A.II.1.b). Allerdings dürften diese Wertunterschiede tendenziell orthogonal zu den hergebrachten Kategorien sozio-ökonomischer Stratifikation liegen.

<sup>21</sup> Siehe unten, §3 C.

<sup>22</sup> Zum spezifisch datenschutzrechtlichen Begriff der Freiwilligkeit in diesem Kontext näher unten, §4 B.I.3.dd).

<sup>23</sup> *Auer*, *Zum Erkenntnisziel der Rechtstheorie*, 2018, 61 f.; siehe auch unten, §4 B.I.5.

besondere die Einwilligung – nicht endgültig überholt haben. Die vorliegende Untersuchung wird zeigen, dass diese Frage, entgegen zahlreicher Grabesreden auf die Einwilligung,<sup>24</sup> nicht uneingeschränkt bejaht werden kann. Allerdings können und müssen die gesetzlich bereits angelegten Formen datensouveränen Handelns technisch und regulatorisch unterstützt werden, um wenigstens eine maschinell medierte Residualform von Privatautonomie unter den Bedingungen der digitalen Wirtschaft, und zumal des sich ankündigenden *Internet of Everything*, zu erhalten.<sup>25</sup> Dies impliziert jedoch zugleich, dass neue, datenverarbeitende Technologien nicht nur als Risiko, sondern auch als Chance für Selbstbestimmung und Datenschutz angesehen werden sollten.

## B. Datenprivatrecht

Diese Technologien machen an den etablierten Grenzen tradierter Rechtsgebiete keinen Halt. Vielmehr verlangen sie nach einer rechtsgebietsübergreifenden Integration ganz unterschiedlicher, teils rein national, teils unionsrechtlich geprägter Normgruppen. Einerseits ist dabei das Datenschutzrecht von unabweislicher Relevanz, da die genannten Technologien jedenfalls typischerweise mit der Verarbeitung personenbezogener Daten operieren. Zugleich werden sie jedoch, sofern sie von nicht-öffentlichen Akteuren verwendet werden, zur Strukturierung von marktförmigen Austauschprozessen genutzt, auf welche die klassischen Bereiche des Privatrechts Anwendung finden. Die Engführung von Datenschutzrecht und Privatrecht ist dabei besonders getrieben durch die Nutzung von Daten als funktionales Geldäquivalent, bleibt jedoch an diesem Punkt nicht stehen.

In jüngerer Zeit wird vor allem im zivilrechtlichen Diskurs zunehmend von der Notwendigkeit der Ausformung eines Datenschuldrechts gesprochen.<sup>26</sup> Allerdings erweist sich dieser Begriff letztlich als zu eng, da die privatrechtlichen

<sup>24</sup> Siehe etwa *Zuiderveen Borgesius*, 13 IEEE Security & Privacy 2015, 103 (104f.); *Barocas/Nissenbaum*, 57(11) Communications of the ACM 2014, 31 (32); *Tene/Polonetsky*, 11 Northwestern Journal of Technology and Intellectual Property 2012, 239 (261f.); vgl. ferner die Nachweise in § 6, Fn. 195 ff.

<sup>25</sup> Dazu näher unten, § 6 C.

<sup>26</sup> Begriffsprägend *Schmidt-Kessel*, Daten als Gegenleistung in Verträgen über die Bereitstellung digitaler Inhalte, Folien zum Vortrag vom 3.5.2016, Folie 7, [https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016\\_digitalesVertragsrecht\\_Schmidt\\_Kessler.html](https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.html); bereits zuvor in der Sache *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (220 ff.); aufgegriffen bei *Wendehorst*, NJW 2016, 2609 (2610); *Sattler*, JZ 2017, 1036 (1036); *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (102 ff.); *Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder*, Bericht vom 15. Mai 2017, 2017, 16, 202 ff.; *Föblisch*, CR 2018, 583 (583); *Gsell*, ZUM 2018, 75 (80 Fn. 64); *Sattler*, in: Ochs et al. (Hrsg.), Die Zukunft der Datenökonomie, 2019, 1 (3 ff.); *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, 147; *Indenhucke/Britz*, BB 2019, 1091 (1091 ff.); *Staudenmayer*, NJW 2019, 2497 (2497); *Riechert*, DuD 2019, 353 (360).

Implikationen von Daten über die Wechselwirkungen des Datenschutzrechts mit dem Schuldrecht im engeren Sinne hinausgehen. Die zunehmende Integration digitaler Technologien in alle Lebensverhältnisse und Austauschprozesse macht daher die Entwicklung eines *Datenprivatrechts* notwendig, in dem auch das Datenschuldrecht als ein Spezialgebiet seinen Platz findet. Der Begriff des „Datenprivatrechts“ wurde bislang, soweit ersichtlich, nur im Kontext des internationalen Privatrechts verwandt (internationales Datenprivatrecht),<sup>27</sup> dort jedoch als Chiffre für Fragen des internationalen Privat- und Zuständigkeitsrechts des Datenschutzrechts.<sup>28</sup> Bei Lichte betrachtet reicht das Datenprivatrecht aber, wie auch die Untersuchungen zum IPR schon andeuten,<sup>29</sup> über die DS-GVO und weitere Datenschutzrechtsakte weit hinaus. Letztlich steht der Begriff für ein interdisziplinär informiertes Privatrecht des Umgangs mit Daten. Zum Aufbau einer solchen Querschnittsmaterie kann eine einzelne Untersuchung naturgemäß nur einen Baustein liefern. Ausgespart werden muss vorliegend etwa die besonders vor einigen Jahren aktiv geführte und nun noch einmal von der WIPO<sup>30</sup> aufgegriffene Debatte um ein „Datenrecht“ bzw. ein „Dateneigentum“.<sup>31</sup>

Die zentrale Zäsur innerhalb des Datenprivatrechts stellt vielmehr die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten dar: Mit ihr steht und fällt die Anwendbarkeit des (unionalen und nationalen) Datenschutzrechts. Wie im Folgenden noch genauer darzustellen ist,<sup>32</sup> interpretiert der EuGH den Begriff der personenbezogenen Daten denkbar weit. Dies impliziert, dass die Wechselwirkungen zwischen Datenschutzrecht und Privatrecht einen Kernbereich des Datenprivatrechts ausmachen, für datengeprägte Austauschprozesse außerhalb der Industrie 4.0 vielleicht gar den relevantesten. Dieser Schnittbereich lässt sich, infolge der schon durch den Anwendungsvorrang des Unionsrechts bedingten Schlüsselstellung des Datenschutzrechts, als *Datenschutzprivatrecht* beschreiben.<sup>33</sup> Dabei muss jedoch, wie sich zeigen wird, neben dem klassisch-regulatorischen Zugriff des Datenschutzrechts immer zugleich die Perspektive eines *Datenermöglichungsrechts* mitgedacht werden, welches die Nutzer in die Lage versetzt, mit ihren Daten, so weit als möglich, souverän zu verfahren und diese beispielsweise als funktionales Zahlungsäquivalent einzusetzen. Inwiefern solche autonomieförderli-

---

<sup>27</sup> Lüttringhaus, ZVglRWiss 117 (2018), 50; ihm begrifflich folgend Thon, RabelsZ 84 (2020), 24.

<sup>28</sup> Lüttringhaus, ZVglRWiss 117 (2018), 50 (52).

<sup>29</sup> Siehe etwa Lüttringhaus, ZVglRWiss 117 (2018), 50 (56 ff., 76 ff.).

<sup>30</sup> WIPO, Draft Issues Paper on Intellectual Property and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1, 2019, Issue 10.

<sup>31</sup> Siehe dazu etwa Zech, CR 2015, 137 (144 ff.); Fezer, MMR 2017, 3; Specht, GRUR Int. 2017, 1040; Deng, NJW 2018, 1371; Kübling/Sackmann, ZD 2020, 24; Pertot (Hrsg.), Rechte an Daten (im Erscheinen).

<sup>32</sup> Siehe unten, § 4 A.II.2.

<sup>33</sup> So bereits Hacker, ZfPW 2019, 148 (150, 195 f.).

chen Ermöglichungsstrukturen im Datenprivatrecht, einschließlich des unionalen Datenschutzrechts, bereits jetzt angelegt sind bzw. ausgebaut werden können, wird eine zentrale Fragestellung der Arbeit ausmachen.<sup>34</sup>

Inhaltlich beschäftigt sich das Datenschutzprivatrecht also mit den Wechselwirkungen des Datenschutzrechts mit einer Reihe von Gebieten des Privatrechts, im Rahmen des bürgerlichen Rechts vordringlich etwa mit der Rechtsgeschäftslehre und dem Schuldrecht, letztlich aber mit allen Büchern des BGB.<sup>35</sup> Außerhalb des BGB stehen die Interferenzen des Datenschutzrechts mit dem Antidiskriminierungsrecht,<sup>36</sup> dem Lauterkeitsrecht<sup>37</sup> und, bereits am weitesten durch das Schrifttum erfasst, dem Kartellrecht<sup>38</sup> im Fokus.<sup>39</sup> Nur

<sup>34</sup> Siehe insbesondere §§ 4 B., 5 B., 6 C.

<sup>35</sup> Siehe zum Verhältnis von Datenschutzrecht und Erbrecht im Kontext des digitalen Nachlasses etwa BGH NJW 2018, 3178 Rn. 64 ff.; repräsentativ aus dem Schrifttum *Budzikiewicz*, AcP 218 (2018), 558 (577 ff.); zum Familienrecht, speziell zur Einwilligung in die Verarbeitung personenbezogener Daten durch Betreuungsbehörden, AG Altötting, Verfügung vom 9.9.2019 – 401 XVII 0178/92, BeckRS 2019, 30935; ferner allgemein die Beiträge in *Pertot* (Hrsg.), Rechte an Daten (im Erscheinen).

<sup>36</sup> Siehe dazu bereits *Hacker*, 55 *Common Market Law Review* 2018, 1143 (1172 ff.); *Zehlike/Hacker/Wiedemann*, 34 *Data Mining and Knowledge Discovery* 2020, 163 (186 ff.); *Wachter*, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising, 35 *Berkeley Technology Law Journal* (im Erscheinen), <https://ssrn.com/abstract=3388639>, 17 ff.

<sup>37</sup> Siehe nur LG Stuttgart, ZD 2019, 366; *Uebele*, GRUR 2019, 694 (697 f.); *Köhler*, ZD 2019, 285 (285); *Obly*, GRUR 2019, 686 (688 ff.); *de Franceschi*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 113 (131 f.).

<sup>38</sup> Siehe dazu OLG Düsseldorf NZKart 2019, 495 (498): von Marktmacht unabhängiger Datenschutzverstoß als solcher für kartellrechtlichen Missbrauch marktbeherrschender Stellung nicht ausreichend; im internationalen Schrifttum zum EU-Recht überwiegt die Befürwortung der Berücksichtigung von Datenschutzbelangen in der kartellrechtlichen Analyse, siehe etwa *Costa-Cabral/Lynskey*, 54 *Common Market Law Review* 2017, 11 (besonders 33 ff., dort 35 zur Kausalität); *Graef/Clifford/Valcke*, 8 *International Data Privacy Law* 2018, 200 (210 f.); *Stucke*, 2 *Georgetown Law Technology Review* 2018, 275 (286–290); *Lianos*, *Polycentric Competition Law*, 71 *Current Legal Problems* 2018, 161 (185–189); *European Data Protection Supervisor*, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Preliminary Opinion, 2014, besonders 29–32; ders., On the coherent enforcement of fundamental rights in the age of big data, Opinion 8/2016, 2016, besonders 5–7; *Autorité de la Concurrence/Bundeskartellamt*, Competition Law and Data, Joint Report (10.5.2016), 25; ferner auch *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 522–527; *Kuner/Cate/Millard/Svantesson/Lynskey*, 4 *International Data Privacy Law* 2014, 247 (248); *Buchner*, WRP 2019, 1243 (1245); tendenziell auch *Kamann/Miller*, NZKart 2016, 405 (406); das deutsche Schrifttum sieht dies mehrheitlich kritisch, etwa *Körber*, NZKart 2016, 348 (351 ff.); *Franck*, ZWeR 2016, 137 (151 ff.) (mangels Kausalität der marktbeherrschenden Stellung für die Datenschutzverletzung); so auch *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (303 f.); *Körber*, NZKart 2019, 187 (192 f.); ferner *Colangelo/Maggiolino*, 42(3) *World Competition Law and Economics Review* 2019, 355; sowie die Nachweise unten in § 4, Fn. 550; insgesamt skeptisch jedoch hinsichtlich der Möglichkeit einer durch das Kartellrecht getragenen Regulierung digitaler Austauschprozesse *Grünberger*, AcP 218 (2018), 213 (245 f.).

<sup>39</sup> Auch darüber hinaus werden privatrechtliche Gebiete von der DS-GVO maßgeblich beeinflusst, siehe etwa zum Wechselspiel von DS-GVO und ZPO *Ory/Weth*, NJW 2018,

durch die Analyse dieser Querbeziehungen kann ein integriertes Marktdurchsetzungsrecht für die digitale Wirtschaft erarbeitet werden, das einerseits sachspezifische Risiken adressiert, andererseits aber auch die Bedingungen der Möglichkeit privatautonomer Gestaltung von Rechtsverhältnissen erhält bzw., wo notwendig, wiederherstellt.

Die vorliegende Untersuchung kann jedoch schon aus Gründen des Umfangs nur einen Ausschnitt dieses umfassenden Forschungsprojekts verwirklichen. Sie fokussiert sich daher innerhalb des Datenprivatrechts auf das Datenschutzprivatrecht im soeben beschriebenen Sinn. Dabei identifiziert sie drei spezifische regulatorische Herausforderungen, welche ein Daten(schutz)privatrecht nach hier vertretener Auffassung vorrangig meistern muss: die Multi-relationalität von Daten; ihre Ambivalenz hinsichtlich Nutzen und Risiken; sowie die Heterogenität von Datenschutzpräferenzen.<sup>40</sup> Sachrechtlich kapriziert sich die Untersuchung dabei auf die Wechselwirkungen zwischen dem Datenschutzrecht einerseits und Kerngebieten des Zivilrechts andererseits, insbesondere der Rechtsgeschäftslehre und dem Schuldrecht. Dieser spezifische Querschnittsbereich erscheint gerade für die Frage des Stellenwerts und der Funktionsbedingungen der Privatautonomie zentral. Zudem werden rein rechtstatsächlich weite Bereiche der digitalen Austauschprozesse gegenwärtig auf vertraglichem Wege, zumal durch AGB, zwischen den Parteien geregelt,<sup>41</sup> was über die Rechtsgrundlage zur Verarbeitung vertragserforderlicher personenbezogener Daten in Art. 6 Abs. 1 lit. b. DS-GVO auch unmittelbar datenschutzrechtliche Relevanz gewinnt. Schließlich zeigt auch die zur Zeit der Niederschrift dieser Untersuchung gerade verabschiedete DIDD-Richtlinie,<sup>42</sup> dass die Wechselwirkungen zwischen Datenschutzrecht, Vertragsrecht und Rechtsgeschäftslehre gewissermaßen den Nukleus des Datenprivatrechts ausmachen.<sup>43</sup> Kartell- und lauterkeitsrechtliche Berührungspunkte werden im

---

2829; *Wiebel/Eichfeld*, NJW 2019, 2734; zur Rechtsdurchsetzung etwa *Fries*, NJW 2016, 2860 (2861 ff., besonders 2865).

<sup>40</sup> Siehe unten, §3 A.–C.

<sup>41</sup> Siehe nur die Portale Terms of Service; Didn't Read (<http://tosdr.org/>), bei dem Online-Nutzungsbedingungen benotet werden, und TOSBack (<https://tosback.org/>), das Änderungen von Nutzungsbedingungen transparent macht. Alle in dieser Arbeit zitierten Webseiten wurden, sofern nichts anderes angegeben ist, zuletzt abgerufen am 30.4.2020.

<sup>42</sup> Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. 2019 L 136/1; dazu, seit dem Erlass der Richtlinie, *Mischau*, ZEuP 2020, 335; *Metzger*, JZ 2019, 577; *Sein/Spindler*, 15 European Review of Contract Law 2019, 257; *Sein/Spindler*, 15 European Review of Contract Law 2019, 365; *Spindler/Sein*, MMR 2019, 415; *Spindler/Sein*, MMR 2019, 488; *Wendland*, ZvglRWiss 2019, 191; *Staudenmayer*, NJW 2019, 2497; *Bach*, NJW 2019, 1705; *Schulze*, ZEuP 2019, 695; *Morais Carvalho*, EuCML 2019, 194; bereits zuvor etwa, aus dem breiten Schrifttum, *Auer*, ZfPW 2019, 130 (132 ff.); *Grünberger*, AcP 218 (2018), 213 (218 ff.); *Gsell*, ZUM 2018, 75; *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (289 ff.); *Graf von Westphalen*, BB 2016, 1411.

<sup>43</sup> Vgl. *Staudenmayer*, NJW 2019, 2497 (2497).



Rahmen dieser Untersuchung an geeigneten Stellen aufgezeigt,<sup>44</sup> ohne dass jedoch eine umfassende Untersuchung der Interdependenzen dieser Rechtsgebiete mit dem Datenschutzrecht geleistet werden könnte. Den Verbindungen von Antidiskriminierungsrecht und Datenschutzrecht schließlich ist der Verfasser bereits an anderer Stelle nachgegangen.<sup>45</sup> In all diesen unterschiedlichen Querschnittsmaterien zeigt sich insbesondere, dass einmal mehr das europäische Mehrebenensystem<sup>46</sup> – im hier relevanten Bereich bestehend aus mitgliedstaatlichem und unionalem,<sup>47</sup> dabei teils durch Richtlinien geprägtem, teils unmittelbar durch Verordnungen gesetztem, teils durch Öffnungsklauseln konturiertem Recht – die methodische Komplexität der rechtswissenschaftlichen Erfassung neuer Technologien nicht unerheblich erhöht.<sup>48</sup>

### C. Regulatorisches und ermöglichendes Privatrecht

Die systematische Erfassung des Datenprivatrechts muss sich nicht nur an der Dogmatik, sondern auch an den Funktionen des Privatrechts orientieren. Dieses wird bereits seit längerem,<sup>49</sup> besonders deutlich in der grundlegenden Untersuchung von *Hellgardt*,<sup>50</sup> als ein multifunktionales System betrachtet, das neben einem sachgerechten Interessenausgleich<sup>51</sup> (zumindest<sup>52</sup>) zwei weitere, einander partiell ausschließende Ziele verfolgt: einerseits die Ermöglichung der

<sup>44</sup> Siehe zum Kartellrecht etwa § 4 B.I.3.a)dd)(3)(b)(aa) zur Relevanz der Marktmacht des Anbieters bei der Bestimmung der Freiwilligkeit der datenschutzrechtlichen Einwilligung; Text bei § 4, Fn. 945 zur kartellrechtlichen Dimension von Zugangsrechten; zum Lauterkeitsrecht etwa Text bei § 5, Fn. 504f. zum Unterlassungsanspruch von Mitbewerbern bei Datenschutzrechtsverstößen.

<sup>45</sup> Siehe die Nachweise oben in Fn. 36.

<sup>46</sup> Zu Begriff und Inhalt ausführlich *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 115 ff.

<sup>47</sup> Die Ebene des internationalen Rechts (Völkerrecht, Einheitsrecht, *lex mercatoria*) wird hingegen in dieser Arbeit ausgeblendet; siehe zu dieser Ebene im Kontext des europäischen Privatrechts allgemein *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 126 f., 469 ff.

<sup>48</sup> Siehe dazu unten, § 5 A.

<sup>49</sup> Siehe bereits *Böhm*, ORDO 17 (1966), 75 (91 f.); *Steindorff*, in: Festschrift für Ludwig Raiser, 1974, 621 (625); *Zöllner*, AcP 188 (1988), 85 (98–100), wengleich mit kritischem Blick auf die regulatorische Seite des Privatrechts; zu einer funktionalen Vertragsperspektive grundlegend *Raiser*, in: von Caemmerer et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben, 1960, 101 (109 ff.); siehe auch den Überblick bei *Grundmann*, in: Grundmann/Micklitz/Renner (Hrsg.), Privatrechtstheorie, Band I, 2015, 875 (877 ff.).

<sup>50</sup> *Hellgardt*, Regulierung und Privatrecht, 2016, 47 ff., besonders 58 f., der beide Funktionen auf das Recht als solches, über das Privatrecht hinaus, ausdehnt (ebd., 50 f., 58).

<sup>51</sup> Siehe repräsentativ *Hellgardt*, Regulierung und Privatrecht, 2016, 59 ff.; *Grundmann*, in: Festschrift Canaris, 2017, 907 (910 ff., 942); vgl. auch *Böhm*, ORDO 17 (1966), 75 (140 ff.); im Kontext des privaten Datenrechts auch *Denga*, NJW 2018, 1371 (1373 ff.).

<sup>52</sup> Zu weiteren Funktionen, *Hellgardt*, Regulierung und Privatrecht, 2016, 62 ff. (Organisations- und Begrenzungsfunktion); *Körber*, Grundfreiheiten und Privatrecht, 2004, 52 ff. (Integrationsfunktion im Binnenmarkt).

Ausübung von Privatautonomie (ermöglichendes Privatrecht)<sup>53</sup> und andererseits die Einhegung spezifischer Risiken (regulatorisches Privatrecht),<sup>54</sup> wobei sich letztere zumeist, wenngleich nicht notwendig,<sup>55</sup> als Folge eines Marktversagens darstellen.<sup>56</sup>

Regulierung, verstanden als bewusste, rechtsförmige, staatliche Beeinflussung, die einen über den Einzelfall hinausgehenden Ordnungszweck verfolgt,<sup>57</sup> ist schon begrifflich auf Ordnungsstrukturen bezogen.<sup>58</sup> In privatrechtlichen

<sup>53</sup> Siehe nur *Böhm*, ORDO 17 (1966), 75 (91); *Grundmann*, Europäisches Schuldvertragsrecht, 1999, 1. Teil, § 2 Rn. 52; *Collins*, Regulating Contracts, 1999, 7f.; *Körper*, Grundfreiheiten und Privatrecht, 2004, 41 ff.; *Grundmann*, 6 European Review of Private Law 2010, 1055 (1063–1066); *Wagner*, in: *Blaurock/Hager*, Obligationenrecht im 21. Jahrhundert, 2010, 13 (14f.); *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 36–38; diese Ermöglichungsfunktion wird auch als Infrastrukturfunktion des (Privat-)Rechts bezeichnet, siehe *Windbichler*, AcP 198 (1998), 261 (271); *Bachmann*, Private Ordnung, 2006, 73–76; *Ackermann*, Der Schutz des negativen Interesses, 2007, 136; *Möslein*, Dispositives Recht, 2011, 380 („staatliche Infrastrukturverantwortung“); *Hellgardt*, Regulierung und Privatrecht, 2016, 56–59; vgl. für das Gesellschaftsrecht auch *Fischel/Easterbrook*, The Economic Structure of Corporate Law, 1996, 34.

<sup>54</sup> Siehe dazu umfassend *Collins*, Regulating Contracts, 1999, 8 f. und 31 ff. (bezogen auf das Vertragsrecht); mit Blick auf das Privatrecht insgesamt *Hellgardt*, Regulierung und Privatrecht, 2016, 46 ff.; ferner *Windbichler*, AcP 198 (1998), 261 (272); *Körper*, Grundfreiheiten und Privatrecht, 2004, 47 ff.; *Wagner*, AcP 206 (2006), 352 (422 ff.) (Steuerungsfunktion); *Micklitz*, GPR 2009, 254 (255 ff.) (Europäisches Vertragsrecht als „Regulierungsprivatrecht“); *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 38–44; *Grundmann*, in: *Festschrift Canaris*, 2017, 907 (910); *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (256 f.); *Grünberger*, AcP 218 (2018), 213 (241); siehe auch die verwandte Unterscheidung zwischen marktkonstitutivem und markt kompensatorischem Vertragsrecht bei *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 65 ff.). Unter denjenigen, welche die Regulierungsfunktion des Privatrechts anerkennen, ist freilich umstritten, ob sich diese auf den Erhalt bzw. die Wiederherstellung der Ermöglichungsfunktion beschränken muss (so etwa *Zöllner*, AcP 188 [1988], 85 [98 f.]; vgl. auch *Bydliński*, AcP 204 [2004], 309 (344 f.) zum Strafschadensersatz) oder ob auch darüber hinausgehende Ziele verfolgt werden können (so *Collins*, Regulating Contracts, 1999, 8; *Wagner*, AcP 206 [2006], 352 [432 ff.]; *Micklitz*, GPR 2009, 254 [257]; *Collins*, 22 EBLR 2011, 425, 426; *Hellgardt*, Regulierung und Privatrecht, 2016, 81; *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 41 ff.; *Hacker*, Verhaltensökonomik und Normativität, 2017, § 6 und § 9).

<sup>55</sup> Siehe nur *Collins*, Regulating Contracts, 1999, 8.

<sup>56</sup> *Grundmann*, in: *Grundmann* (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, 1 (29); siehe auch *Collins*, Regulating Contracts, 1999, 7.

<sup>57</sup> Vgl. *Eifert*, in: *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle* (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Aufl. 2012, 1319, besonders Rn. 5; dort auch zum uneinheitlichen Begriff der Regulierung (ebd. Rn. 1 ff.); dazu auch, rechtsvergleichend, *Grundmann*, in: *Festschrift Canaris*, 2017, 907 (909 f.); *Hellgardt*, Regulierung und Privatrecht, 2016, 16 ff., besonders 50 ff., der zudem die Verfolgung von Zielen des Allgemeinwohls als notwendige Begriffsbedingung postuliert (ebd., 53–55, 81). Im hier betrachteten Schnittbereich von Datenschutz- und Privatrecht macht die (nicht unumstrittene, siehe nur *Collins*, Regulating Contracts, 1999, 7) Hinzunahme dieser Bedingung jedoch keinen Unterschied, da regelmäßig staatliche Eingriffe (zumindest auch) die Verwirklichung von Markt- oder Datenschutz zum Ziel haben; siehe im Einzelnen unten, § 4 C. und § 5 C.

<sup>58</sup> Vgl. auch den Überblick über Ordnungsdenken und die ordoliberalen Schule bei

Kontexten interveniert Regulierung typischerweise durch die Verfolgung jeweils zu rechtfertigender Ordnungszwecke in den Marktmechanismus und begrenzt den Spielraum der Akteure.<sup>59</sup> Damit fungiert diese regulatorische Ebene als ein Rahmen für die Ausübung von Privatautonomie.<sup>60</sup> Demgegenüber lassen sich solche Normen identifizieren, die primär, zum Teil auch durch zwingendes Recht, eine Erweiterung dieses Spielraums bezwecken. Sie halten rechtliche Konstrukte bereit, welche privatautonome Gestaltung unterstützen oder überhaupt erst ermöglichen.<sup>61</sup> Beispiele für derartige Ermöglichungsstrukturen bieten die Anerkennung von (natürlichen oder juristischen) Personen als Rechtssubjekte,<sup>62</sup> rechtliche (z. B. vertragliche) Typisierungen<sup>63</sup> oder die Verfügbarmachung von staatlichen Rechtsdurchsetzungsmechanismen.<sup>64</sup>

Dabei ist zu konzedieren, dass gerade im Vertragsrecht viele Normen sowohl regulatorischen als auch ermöglichenden Charakter haben,<sup>65</sup> da sie einerseits bestimmte, (auch) der Allgemeinheit dienende Schutzzwecke verfolgen,

---

*Grundmann*, in: Grundmann/Micklitz/Renner (Hrsg.), *Privatrechtstheorie*, Band I, 2015, 405 (408 ff.); *Vanberg*, in: Newman (Hrsg.), *The New Palgrave Dictionary of Law and Economics*, Band 2, 1998, 172; zu Ordnungsstrukturen im Privatrecht auch *Mestmäcker*, JZ 1964, 441 (443 ff.); grundlegend *Böhm*, ORDO 17 (1966), 75 (85 ff., 99 ff.).

<sup>59</sup> *Hellgardt*, Regulierung und Privatrecht, 2016, 59; vgl. auch *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), *Grundlagen des Verwaltungsrechts – Band I*, 2. Auf. 2012, 1319 Rn. 3; *Eisner/Worsham/Ringquist*, *Contemporary Regulatory Policy*, 2000, 6 ff.; für das Datenschutzrecht auch *Buchner*, *Informationelle Selbstbestimmung im Privatrecht*, 2006, 62.

<sup>60</sup> *Kilian*, in: Grundmann (Hrsg.), *Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts*, 2000, 427 (431); *Grundmann*, in: *Festschrift Canaris*, 2017, 907 (911).

<sup>61</sup> Siehe die Nachweise oben in Fn. 53.

<sup>62</sup> *Körber*, *Grundfreiheiten und Privatrecht*, 2004, 41 f.; *Unberath*, *Die Vertragsverletzung*, 2007, 71 ff.; *Starke*, *EU-Grundrechte und Vertragsrecht*, 2016, 36.

<sup>63</sup> *Körber*, *Grundfreiheiten und Privatrecht*, 2004, 42; *Hellgardt*, *Regulierung und Privatrecht*, 2016, 72.

<sup>64</sup> *Körber*, *Grundfreiheiten und Privatrecht*, 2004, 44; *Ackermann*, *Der Schutz des negativen Interesses*, 2007, 135 f.; *Starke*, *EU-Grundrechte und Vertragsrecht*, 2016, 37; *Hacker*, *Verhaltensökonomik und Normativität*, 2017, 238; vgl. auch *Raiser*, in: von Caemmerer et al. (Hrsg.), *Hundert Jahre deutsches Rechtsleben*, 1960, 101 (115).

<sup>65</sup> *Körber*, *Grundfreiheiten und Privatrecht*, 2004, 41; *Starke*, *EU-Grundrechte und Vertragsrecht*, 2016, 36; vgl. auch *Fornasier*, *Freier Markt und zwingendes Vertragsrecht*, 2013, 66 (Hybridqualität von Normen mit sowohl marktkonstitutiver als auch markt kompensatorischer Funktion, etwa § 138 BGB). Ob man Ermöglichung bzw. Erhalt und Wiederherstellung der Möglichkeit zur effektiven Wahrnehmung privater Gestaltungsmacht durch privatautonome Regelsetzung auch als Teil der Regulierung sieht, weil auch hier zielgerichtet Verhalten und Marktstruktur beeinflusst werden, ist eine rein begriffliche Frage, von der hier nichts weiter abhängt (ablehnend etwa *Hellgardt*, *Regulierung und Privatrecht*, 2016, 71 f.; *Ackermann*, *Der Schutz des negativen Interesses*, 2007, 136 [kein Eingriffscharakter]; bejahend *Grundmann*, in: *Festschrift Canaris*, 2017, 907 [911]; wohl auch schon *Grundmann*, 6 *European Review of Private Law* 2010, 1055 [1064 f.]). Für die Zwecke dieser Arbeit werden derartige Normen in terminologischer Hinsicht als Hybrid von Ermöglichungs- und Regulierungsfunktion betrachtet. Analytisch bleibt nichtsdestoweniger die Differenz zwischen Ermöglichung einerseits und restringierend ordnender Regulierung andererseits zentral.

## Sachregister

- ad exchanges* 16, 52, 56, 112, 128, 144f.,  
279, 570, 633  
Adresshandel 415  
*agreement technologies* 638  
allgemeines Persönlichkeitsrecht 20, 214,  
519f., 525–527, 529–533, 537  
Anfechtung 364–370, 539  
Anonymisierung 106, 109, 157, 276  
Antidiskriminierungsrecht 6, 8, 151, 315  
Anti-Tracking-Tools 556, 559, 565, 576,  
644, 655  
Anwendungsbereich des Unionsrechts  
120, 122–127  
Anwendungsvorrang 5, 92, 147, 227,  
314f., 317, 321, 324–326, 330, 332–334,  
341–343, 357, 369f., 394, 413, 416f.,  
428, 477, 482, 493, 496–499, 502, 504f.,  
510, 512, 514, 521, 532, 538f., 669  
Äquivalenzkontrolle 479f., 483–485,  
488, 490f., 493, 495f.  
Arglistige Täuschung 367  
Automatisierung 36, 39, 57, 605  
autonome Fahrzeuge 44, 80, 388, 391,  
394, 642  
*Aziz-Test* 448f., 451–453, 456–458, 474–  
476, 485, 487, 490, 541, 661, 670
- beachtlicher Motivirrtum 369  
Bereicherungsrecht 407, 514  
Blanketterklärung 612  
Blockchain 94f., 100f., 557  
*bluetooth beacons* 28, 79
- Cookies 26, 238  
Co-Regulierung 18, 300–302, 309  
*culpa in contrahendo* 467, 503, 514, 536
- data on top-Modell 202, 283, 297, 347,  
435
- data protection by default* 289, 291,  
295f., 592  
Daten als funktionales Geldäquivalent 2,  
4, 16, 49  
datenbasierte *laesio enormis* 476, 494,  
541, 670  
Datenermöglichungsrecht 5, 15, 159, 255,  
260, 547, 593, 621, 655, 669  
Datenexzesskontrolle 486, 489, 491, 494,  
541, 648  
Datenhandel 52, 416, 540, 670  
Datenminimierung 156–159, 288, 294,  
297, 444, 455, 479, 599  
Datenpreis 68, 272, 284, 428, 434f., 437f.,  
441, 536  
Datenschutzassistenten 21, 552, 597f.,  
601, 603–606, 608–611, 613, 615f.,  
619f., 638, 643, 649, 654, 656, 663, 665,  
667, 671  
Datenschutz-Dashboard 594, 619  
Datenschutz durch Technikgestaltung  
18, 219, 289, 293, 307, 311, 555, 561,  
608, 619, 653  
Datenschutz durch Voreinstellungen 18,  
150, 219, 289, 295, 307, 311, 664  
Datenschutzprivatrecht 5–7, 154, 328,  
351  
datenschutzrechtliche Verantwortlich-  
keit 129  
Datenschutzrechtsakzessorietät (der  
Wirksamkeit des Vertrags) 399  
Datenüberlassung als Gegenleistung 345  
*debiasing* 591f., 619, 650, 664  
DIDD-Richtlinie 7, 99, 163, 199f., 211,  
228, 264, 266, 268f., 315, 317, 329, 333,  
341, 371, 377, 384, 394, 403, 477  
*differential privacy* 110  
Dilemma individueller Kontrolle 310,  
656, 666, 671

- Diskriminierung 75, 116, 153, 237, 277, 305, 532, 665
- dolo agit*-Einrede 215f., 219, 222f., 225, 347, 401–403, 405f., 415, 500
- do not track* 253, 559, 613–616
- Doppelwirkung im Recht 366
- Drittanbietercookies 27, 79, 116, 135, 283, 299, 426, 560
- Drittchadensliquidation 395
- edge computing* 40, 599
- Einwilligung als Gegenleistung 345
- Einwilligungsbewusstsein 358
- Einwilligungsfähigkeit 230f., 233–235, 348, 356, 370, 409, 539
- Entäußerungstheorie 361, 370, 539
- ePrivacy-VO 28, 170, 238, 245, 248–253, 256f.
- Erklärungsbewusstsein 357–359, 370, 384–387, 389f., 396
- Erklärungsirrtum 367
- Facebook Fanpages 129, 132f., 135–137
- Fairnessgebot (datenschutzrechtliches) 151–153, 339
- fingerprinting* 26, 28, 80, 116, 238f., 250, 254, 286, 299, 560f.
- first-party tracking* 26, 79, 252
- framing* 63, 591
- gemeinsame datenschutzrechtliche Verantwortlichkeit 130, 133, 179
- Geräte-Identifizier 26, 238–241, 245, 254, 259, 281, 298f., 616
- geschäftsähnliche Handlung 163, 349f., 369, 397, 429, 539, 613, 670
- Geschäftsgeheimnis 573
- Geschäftsgrundlage 199, 225–227, 229, 406, 409–411, 413, 417, 465, 492
- grenzüberschreitendes Element 120f., 123
- Grundsätze der Datenverarbeitung 128f., 148–150, 159, 278, 290f., 293, 443f., 475, 477, 482
- Grundsatz von Treu und Glauben 152f., 207, 449, 473, 480, 495, 497–502, 531, 541f., 661
- Icons 91, 176, 179, 585f., 589, 591, 618, 633
- Identity-Management-Systeme 556, 558f., 655
- Informationsasymmetrie 59f., 70, 76, 82, 138, 141, 174, 176, 292, 361, 375f., 389, 396, 618, 663
- Informationspflichten 11, 129, 152, 154f., 160, 174, 179, 244, 246, 257, 259–261, 310, 363, 366, 388, 427f., 474, 510, 541, 543, 634
- Inhaltsirrtum 367
- Internet of Everything 1–4, 15f., 21, 38, 42–45, 48, 194, 255, 284, 665, 669, 671
- inverse predatory pricing approach* 647, 668
- Just-in-time-Hinweise 587f., 618, 626
- Kampfpreisunterbietung 647
- konditionale Verknüpfung 198, 225, 228, 234f., 396, 431, 540
- Konditionenmissbrauch 449
- Kopplungsverbot 181, 253, 272, 279, 399, 457, 493
- künstliche Intelligenz 1, 16, 29f., 37, 43f., 209, 669
- Lesbarkeit 60, 62, 256, 579f., 633f.
- Marktortprinzip 94, 98, 101f., 150
- Marktversagen 15, 17–19, 59f., 62, 64, 67, 70, 81f., 176, 209, 258, 291, 311, 361, 363, 401, 417, 421, 427, 437, 439, 441, 449, 484, 486, 491, 494, 547, 564, 575, 578, 602, 605, 618, 624, 628, 634, 650, 654, 661, 663f.
- Maschinendaten 117
- Mastereinwilligung 620
- Mehrebenen-Datenschutzklärungen 581, 584, 589, 618
- mehrseitiger Vertrag 374f., 396, 426, 540
- Minderjährige 230–235, 238, 286, 320, 348, 356, 384, 391, 457
- neuronale Netze 34
- Niederlassungsprinzip 94
- Nutzungsvertrag (hinsichtlich IoT-Geräten) 162, 372, 381, 383, 385, 396

- One-Pager 584, 589, 618f., 624, 634
- Paradox der Privatheit 59, 550, 564, 576, 628
- penalty default* 292, 592
- Personenbezug 103f., 106, 108, 113, 117, 128, 241, 391
- Preisangabenverordnung 428
- Preishauptabrede 432, 435f.
- Preisnebenabrede 432, 435, 438
- privacy by design* 158, 271, 289, 293, 296, 320, 554f., 576, 619
- privacy-enhancing technologies* 20, 554f., 563f., 566, 593, 596, 655
- privacy nudges* 578, 590, 592, 619
- privacy nutrition label* 582, 584
- privacy paradox*. Siehe Paradox der Privatheit
- privacy score* 21, 69, 621f., 627f., 630–632, 634, 650, 652–654, 656, 663f., 668
- qui habet commoda ferre debet onera* 130, 452, 491, 609
- Rabattmodell 201, 435, 487
- Recht auf informationelle Selbstbestimmung 92, 128, 206, 282, 517f., 520–527, 537, 562, 564, 651
- Recht auf Vergessen 92, 194, 319, 340f., 445, 517, 520–523, 525–528
- Rechtsgeschäftslehre 6f., 12, 19, 313f., 343f., 348, 351f., 356f., 359, 369–371, 389, 459, 538–540, 656, 667, 670
- Rechtsmissbrauch 494, 496, 498, 502, 542
- Registrierungsdaten 25, 218f., 222
- regulatory arbitrage* 98
- Re-Identifizierung 64, 106, 110–113
- reinforcement learning* 31, 33f.
- Risikospezifizität 19, 319, 324f., 332, 341, 343, 368, 370, 478–481, 506, 529, 538f., 669
- Sachdaten 104
- Sachintegration 147, 333, 342f., 419–421, 538, 669
- schwarze Liste 285, 459, 645
- Scoring 66, 72, 92, 263
- secondary use* (von Daten) 155, 173, 287, 633
- Selbstdatenschutz 555f., 576, 651
- sensitive Daten 236f., 287, 320, 383, 562
- Separierungsgebot 205f., 457
- single click privacy* 595, 600, 640
- singling out* 105, 116
- Smart City 43, 73, 171, 306, 388, 391, 394, 396, 653
- Smart Home 40, 42, 44, 57, 117, 171, 390, 393f., 396, 600, 604, 617, 630
- Social Plug-Ins 27, 60, 79, 103, 114, 116, 129, 133, 136, 144, 146, 171, 283, 639
- Sonderrechtsverhältnis 510, 513f., 542
- Sozialkreditsystem 3, 43
- Stellvertretung 313, 348, 356f., 362f., 370, 377, 379, 426, 539, 612f., 662
- Suchmaschinen 96, 458, 596, 601, 640f., 653f.
- supervised learning* 31, 34, 567
- Synallagma 197f., 219, 225, 229, 431, 466, 564
- technologiebasierte Ansätze (hinsichtlich der Einwilligung) 21, 578, 605, 618f., 624, 656, 667
- technologische Einwilligung 21, 255, 257, 260, 597, 618, 667, 671
- territoriale Anwendbarkeit der DS-GVO 93f.
- third-party tracking* 16f., 26, 56, 79, 114, 133, 143, 171, 178, 238, 250f., 259, 264, 273, 298–300, 306, 312, 385, 391, 399, 539, 571, 588, 590, 649, 669
- tracking walls* 202, 245, 248, 251, 253f., 259, 380, 383, 565, 625, 637, 646
- Trainingsdaten 31, 36, 43, 51, 93, 106, 110, 118, 128, 566, 569, 574
- transparenzbasierte Ansätze (hinsichtlich der Einwilligung) 551, 589, 593, 602, 624, 656, 663, 665
- Transparenzgebot 152, 206, 424, 427, 429, 471
- Überraschungseffekt 276, 282, 286, 425f., 430, 474
- UGP-Richtlinie 151, 336, 482
- Unmissverständlichkeit (der Einwilligung) 160, 165–173, 180f., 203, 206, 243, 247f., 257f., 269, 272, 312, 358, 389f., 396, 465, 540, 571, 662

- Unmöglichkeit 142 f., 148, 406–408, 412, 536  
*unsupervised learning* 31, 33
- Verbotsgesetz 397, 400–402, 533  
 verhaltensbasierte Ansätze (hinsichtlich der Einwilligung). *Siehe privacy nudges*
- Verhaltensökonomik 590  
 Verkehrsschutzinteresse 370, 389  
 Verschlüsselung 208, 287, 556–558, 565, 633
- Vertrag mit Schutzwirkung zugunsten Dritter 19, 392, 394, 396, 662  
 Vollmachtsampel 612
- Warenkauf-Richtlinie 163, 317, 371, 377, 394 f., 477  
 Warnhinweise 589, 618  
 Web 2.0 129  
 weite Leistungspflicht 313, 425, 440, 457, 459, 468, 473, 475, 541  
 Whistleblowing 573  
 Widerrechtliche Drohung 364  
 Widerruf (der Einwilligung) 206, 279, 346, 355, 360, 364, 374, 409, 454, 456, 649
- Zielkompatibilität 324 f., 343, 370, 478, 481, 529, 538 f.  
 Zweckbindung 155, 287 f., 455  
 zweistufige Prüfung 323, 343, 355, 368, 395, 478, 481 f., 506, 539