

MATTHIAS LEISTNER
LUCIE ANTOINE
THOMAS SAGSTETTER

Big Data

*Geistiges Eigentum
und Wettbewerbsrecht*

Mohr Siebeck

Geistiges Eigentum und Wettbewerbsrecht

herausgegeben von

Peter Heermann, Diethelm Klippel,
Ansgar Ohly und Olaf Sosnitzer

162



Matthias Leistner, Lucie Antoine
und Thomas Sagstetter

Big Data

Rahmenbedingungen im europäischen
Datenschutz- und Immaterialgüterrecht und
übergreifende Reformperspektive

Mohr Siebeck

Matthias Leistner ist Inhaber des Lehrstuhls für Bürgerliches Recht und Recht des Geistigen Eigentums mit Informations- und IT-Recht (GRUR-Lehrstuhl) an der LMU München.

Lucie Antoine ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Bürgerliches Recht und Recht des Geistigen Eigentums mit Informationsrecht und IT-Recht (GRUR-Lehrstuhl) an der LMU München.

Thomas Sagstetter ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht und Recht des Geistigen Eigentums mit Informationsrecht und IT-Recht (GRUR-Lehrstuhl) an der LMU München.

ISBN 978-3-16-160145-3 / eISBN 978-3-16-160198-9

DOI 10.1628/978-3-16-160198-9

ISSN 1860-7306 / eISSN 2569-3956 (Geistiges Eigentum und Wettbewerbsrecht)

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

© 2021 Mohr Siebeck Tübingen. 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 Gulde Druck in Tübingen aus der Times gesetzt, auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Printed in Germany.

Vorwort

Die regulatorischen Herausforderungen der Datenökonomie sind in aller Munde. Dabei sind voreilige Forderungen nach der Schaffung neuer Exklusivrechte an Daten („Dateneigentum“) zwischenzeitlich zu Recht verhallt. Die aktuelle Diskussion wird eher vom Aspekt des Datenzugangs und insoweit von zunehmend konkreteren, präziseren Forschungsarbeiten und rechtspolitischen Entwicklungen bestimmt.

Hier reiht sich die vorliegende Studie ein, die aus immaterialgüter- und datenschutzrechtlicher Perspektive einen Beitrag zur Konkretisierung und Präzisierung der Diskussion liefern will. Einerseits wird Handwerksarbeit geleistet und der Stand der *lex lata* sowie aktueller Reformprojekte umfassend aufbereitet. Andererseits werden auf dieser Basis weitere Reformperspektiven aufgezeigt, die von den Leitgedanken vielfältiger Innovation durch wirksamen Wettbewerb sowie materieller Privatautonomie (einschließlich des Schutzes der Privatsphäre) auf der Basis der einschlägigen Grundrechtspositionen bestimmt sind. Ein besonderes Anliegen war es uns, den aus unserer Sicht für den immaterialgüterrechtlichen Rahmen der Datenökonomie zentral wesentlichen Geschäftsgeheimnisschutz mit einzubeziehen; entsprechend werden das GeschGehG und die EU-Geschäftsgeheimnis-Richtlinie in ihren für Daten als Schutzgegenstand wesentlichen Elementen ausführlich mit behandelt. Ebenso wichtig war es uns, den Einfluss der Datenschutzgrundverordnung auf die Entwicklung eines freien, unverzerrten und innovativen Wettbewerbs in den europäischen Datenmärkten praxisorientiert und differenziert zu diskutieren. Auch konnten wir zuletzt noch die aktuellen Vorschläge der Kommission für den Data Governance Act, den Digital Markets Act und den Digital Services Act mit einbeziehen.

Die Studie ist ein echtes Lehrstuhlprojekt und Gemeinschaftswerk. Auf der Grundlage einzelner Vorarbeiten haben die Autoren die einzelnen Teile unter der Federführung von *Leistner* gemeinsam bearbeitet, wobei *Antoine* schwerpunktmäßig den Teil zum Datenschutzrecht entworfen hat, *Sagstetter* schwerpunktmäßig den Teil zum Geschäftsgeheimnisschutz (und auch Abschnitte zum sui generis-Recht und zu den Grundlagen) und *Leistner* alle verbleibenden Teile, wobei ihm seine Mitarbeiter wiederum ihrerseits tatkräftig geholfen haben.

Zahlreiche Anregungen und auch Kritik, die uns in einzelnen Bereichen geholfen hat, die Gedanken schärfer zu konturieren, verdanken wir der kontinuierlichen Diskussion mit KollegInnen in Wissenschaft, Politik und Praxis. So zahlreich waren die Diskussionen in den vergangenen Jahren, so intensiv und ertragreich der Austausch, dass wir nicht einmal annähernd allen gebührend danken können. Immer wieder überaus fruchtbringend waren etwa der Dialog mit *Josef Drexl, Reto Hilty* und der gesamten „Datengruppe“ des Max-Planck-Instituts für Innovation und Wettbewerb in München sowie der kontinuierliche inspirierende Austausch zu einzelnen Themen mit *Tanya Aplin, Jeanne Fromer, Jane Ginsburg, Pamela Samuelson, Heike Schweitzer, Thomas Ackermann, Barton Beebe, Lionel Bently, Henning Große Ruse-Khan, Bernt Hugenholtz, Wolfgang Kerber, Kung-Chung Liu, Axel Metzger, Ansgar Ohly, Rupprecht Podszun, Jule Sigall, Gerald Spindler, Christopher Sprigman, Yoshiuki Tamura, Tatsuhiko Ueno, Jacob Victor, Michael Weinberg, Peter Yu* und *Herbert Zech*. Auch allen anderen KollegInnen und Studierenden, mit denen wir uns in den letzten Jahren in ganz unterschiedlichen nationalen und internationalen Foren zu Einzelaspekten ausgetauscht haben, sei von Herzen für diese faszinierenden, zunehmend immer genaueren, tiefer gehenden Diskussionen zur Regulierung der Datenökonomie gedankt.

Großer Dank gilt schließlich allen wissenschaftlichen und studentischen MitarbeiterInnen des Lehrstuhls für Bürgerliches Recht und Recht des Geistigen Eigentums mit Informationsrecht und IT-Recht (GRUR-Lehrstuhl) an der LMU. Ohne die lebhafteste, auch kontroverse, dabei stets anregende und freundschaftliche Diskussionskultur am Lehrstuhl (und darüber hinaus an der Juristischen Fakultät der LMU und am Münchener Max-Planck-Institut) und ohne die einsatzfreudige Mithilfe der LehrstuhlmitarbeiterInnen in Recherche- und Redaktionsangelegenheiten wäre dieses Buch nicht in seiner jetzigen Form zustande gekommen.

Abschließend sei den Herausgebern der Schriftenreihe „Geistiges Eigentum und Wettbewerbsrecht“ für die Aufnahme in die Reihe und allen MitarbeiterInnen des Mohr Siebeck-Verlags für die sorgsame verlegerische Betreuung unseres Werks gedankt. Es ist für uns eine bewusste Entscheidung und besondere Freude gewesen, das Buch in einer so gediegenen, genuin wissenschaftlich geprägten Reihe zu veröffentlichen.

München, Januar 2021

Matthias Leistner
Lucie Antoine
Thomas Sagstetter

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	XIII
A. Einführung	1
B. Grundlagen	5
I. Strukturwandel durch big data und AI	5
1. Big data	5
2. Soziale und ökonomische Funktion entscheidend für die rechtliche Strukturierung	6
3. Datenzugang und Datenqualität als Bottleneck	7
4. Angestammte und neuartige Geschäftsmodelle auf unterschiedlichen Marktebenen und mit marktübergreifender Relevanz	9
5. Allgemeingültige Definition von big data und AI weder möglich noch notwendig	11
II. Die immaterialgüter- und datenschutzrechtliche Perspektive: Drei Phasen im Rahmen typischer big data-Sachverhalte	14
1. Ausgangspunkt	14
2. Potenziell relevante materielle und immaterielle Rechtsobjekte in typischen big data-Prozessen	16
III. Identifizierbare Probleme der Datenökonomie und mögliche Lösungsansätze	22
1. Verlagerung und Spezifizierung der Diskussion um die Regulierung der Datenökonomie in den letzten Jahren	22
2. Grundlegende Zielsetzungen	25
3. Konkrete Probleme und immaterialgüterrechtliche Forschungsherausforderungen	30
4. Bedeutung der immaterialgüterrechtlichen Perspektive: „Hin- und Herwandern“ des Blicks	37

C. Der urheberrechtliche Rahmen der Datenwirtschaft de lege lata und de lege ferenda	41
I. Überblick	41
II. Urheberrechtlicher Schutz für kreative und investitorische Leistungen in der Datenwirtschaft	42
1. Urheberrecht und Leistungsschutz an Datenbanken	42
2. Urheberrechtlicher Computerprogrammschutz	115
III. Bereichsübergreifende Anpassung der allgemeinen urheberrechtlichen Schrankenregelungen an die Belange und Besonderheiten der Datenwirtschaft, insbesondere Text- und Data-Mining	121
1. Die neuen Text- und Data-Mining-Schranken der DSM-RL und bestehender weiterer Reformbedarf	121
2. Unzureichende Absicherungen gegen die Umgehung von Ausnahmen und Schranken in der InfoSoc-RL	125
3. Zusammenfassung und Reformbedarf	126
D. Der patentrechtliche Rahmen der Datenwirtschaft de lege lata und de lege ferenda	127
I. Zusätzliche Anreize für Schaffung und Offenlegung wertvoller Datensätze	128
II. Datenformate, Schnittstellen und Rolle des Patentrechts	130
III. Zugang zu Patentlizenzen im Bereich technischer Standards (standardessentielle Patente)	132
IV. Zusammenfassung und Reformbedarf	135
E. Die Relevanz der Trade Secrets-RL für die europäische Datenwirtschaft de lege lata und de lege ferenda	137
I. Schutzgegenstand	138
1. Weite Definition des Geschäftsgeheimnisses	138
2. Anknüpfungspunkte in typischen big data- und Industrie 4.0-Sachverhalten	141
3. Zusammenfassung	155
II. Schutzsubjekt: Inhaberschaft des Geschäftsgeheimnisses	156
1. Ausgangspunkt: Vage Legaldefinition	156
2. Lösungsvorschläge zur rechtssicheren Konkretisierung des Rechtsinhabers	157

III.	Schutzwirkung	163
	1. Grundsatz der Informations(zugangs)freiheit: Rechtmäßiger Erwerb, rechtmäßige Nutzung und Offenlegung	163
	2. Schutz vor bestimmten Verletzungshandlungen	168
IV.	Ausnahmen	177
	1. Abwägung mit dem Recht der freien Meinungsäußerung und der Informationsfreiheit	177
	2. Whistleblowing-Ausnahme	178
	3. Sonstige legitime Interessen	181
V.	Flexible Durchsetzungsvorschriften	182
VI.	Zusammenfassung und Reformbedarf	184
F. Datenschutz und DSGVO		191
I.	Ausgangspunkt: Freier Datenverkehr vs. Schutz des Einzelnen	193
	1. Regelungsziele der Datenschutzgrundverordnung	194
	2. Datenschutzrecht als Ausschließlichkeitsrecht für personenbezogene Daten?	197
II.	Spannungsverhältnis zwischen big data und Datenschutz	199
	1. Veränderte Verarbeitungsprozesse durch big data	199
	2. Datenschutzrechtliche Interessenlage bei big data	201
III.	Anwendungsbereich der DSGVO in big data-Sachverhalten	205
	1. Gegenstand: Verarbeitung personenbezogener Daten	205
	2. Besondere Arten personenbezogener Daten	209
	3. Anonymisierte Daten	214
IV.	Grenzüberschreitender Datenverkehr	227
	1. Territorialer Anwendungsbereich der DSGVO	227
	2. Voraussetzungen der DSGVO für den Datentransfer in Drittstaaten	230
V.	An der Datenverarbeitung Beteiligte: Verantwortliche – Auftragsverarbeiter – Betroffene	239
	1. Verantwortlicher vs. Betroffener	239
	2. Gemeinsame Verantwortlichkeit (Joint Controllership)	240
VI.	Grundvoraussetzung: Rechtmäßigkeit der Datenverarbeitung	247
	1. Erforderlichkeit der Festlegung einer spezifischen Verarbeitungsgrundlage	247
	2. Einwilligung des Betroffenen	248
	3. Berechtigte Interessen des Verantwortlichen	275
	4. Möglichkeiten der Zweckänderung einer Datenverarbeitung	282
	5. Zusammenfassung und Reformbedarf	291

VII.	Betroffenenrechte	294
	1. Allgemeine Vorgaben für die Betroffenenrechte	295
	2. Betroffenenrechte – entgrenzte Pflichten oder Verhältnismäßigkeit?	295
	3. Auskunftsrecht	296
	4. Recht auf Löschung („Recht auf Vergessenwerden“)	307
	5. Recht auf Berichtigung	315
	6. Datenportabilität gemäß Art. 20 DSGVO	315
	7. Zusammenfassung und Reformbedarf	351
VIII.	Risikobasierter Ansatz der DSGVO – Chance oder Bürde für big data?	353
	1. Allgemeine Pflicht zur Datenschutzfolgenabschätzung?	354
	2. Privacy by design und privacy by default – Umsetzbarkeit bei big data?	358
	3. Technische und organisatorische Maßnahmen als Mittel der Risikominimierung?	362
	4. Berücksichtigung der Unternehmensgröße?	363
	5. Zusammenfassung und Reformbedarf	364
IX.	DSGVO und „Künstliche Intelligenz“: Verbot der automatisierten Einzelentscheidung	364
	1. Voraussetzung: Ausschließlich auf automatisierter Datenverarbeitung beruhende Entscheidung	365
	2. Unmittelbare rechtliche Wirkung oder vergleichbare erhebliche Beeinträchtigung	366
	3. Erlaubnistatbestände des Art. 22 Abs. 2 DSGVO	369
	4. Umfang der Informations- und Auskunftspflichten bei automatisierten Einzelentscheidungen	370
	5. Zusammenfassung und Reformbedarf	375
X.	Datenschutzverstöße: Remedies – Enforcement – Accountability	379
	1. Grundproblem 1: Zentralisierte Verantwortlichkeit bei dezentralisierter Verarbeitung	380
	2. Grundproblem 2: Inkohärente Bewertung durch mitgliedstaatliche Datenschutzbehörden	381
	3. Anspruch auf Schadensersatz bei Datenschutzverstößen	381
	4. Bußgelder und sonstige Sanktionen für Datenschutzverstöße	383
	5. Privatrechtliche Durchsetzung der DSGVO?	384
XI.	Bereichsspezifische Sonderregeln des Datenschutzrechts, insbesondere ePrivacy-RL	389
XII.	Ausblick: Funktionale Schwächen der angestammten Datenschutzkonzeption und mögliche alternative Lösungsansätze	391

1. Überlegungen zu weitergehenden Rechten zum Schutz der Privatsphäre?	391
2. Vertragsrecht als Lösung	394
XIII. Zusammenfassung und Reformbedarf	401

G. Reformperspektive: Immaterialgüter- und datenschutzrechtliche Probleme, Trends und Building Blocks für die Datenökonomie 409

I. Möglicher Überschutz und Transaktionskosten	409
1. Anreizgedanke für Datenproduktion und effiziente Datendissemination als inhärente Grenze des Schutzgegenstands	409
2. Funktionale Grenzen zentralisierter Ausschließlichkeitsrechte in big data-Szenarien und besondere Bedeutung des Vertragsrechts	411
3. Schutzrechtsüberschneidung als Problem für Datenzugang . . .	414
4. Trend de lege ferenda: Sinkende Schutzfristen und langfristig wachsende Bedeutung von Registerrechten	417
II. Flexible Hybride zwischen Ausschließlichkeitsrecht und verhaltensbezogener Regelung: Begrenzte Drittwirkung vertraglicher Vereinbarungen als Paradigma für die Datenökonomie?	420
1. Kommerzialisierung von Daten und der immaterialgüterrechtliche und datenschutzrechtliche Rahmen . .	420
2. Qualifizierte Drittwirkung vertraglicher Vereinbarungen in Anlehnung an den Geschäftsgeheimnisschutz?	422
3. Mögliche lauterkeitsrechtliche Ansätze de lege lata und de lege ferenda?	426
III. Neue Zugangsrechte in der Datenökonomie, Datenportabilität und die Schnittstelle zum Immaterialgüter- und Datenschutzrecht . . .	428
1. Verlagerung der Diskussion in Richtung (bereichsspezifischer) Zugangsrechte	428
2. Die Unterscheidung von Zugangsrechten und Nutzungsmöglichkeiten und -rechten	429
3. Relevante Szenarien für Zugangsrechte und die Schnittstelle zum Immaterialgüterrecht hinsichtlich der Nutzungsregelung . .	435
4. Portabilität und Interoperabilität	457

Literaturverzeichnis	461
Sachregister	495

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
A. Einführung	1
B. Grundlagen	5
I. Strukturwandel durch big data und AI	5
1. Big data	5
2. Soziale und ökonomische Funktion entscheidend für die rechtliche Strukturierung	6
3. Datenzugang und Datenqualität als Bottleneck	7
4. Angestammte und neuartige Geschäftsmodelle auf unterschiedlichen Marktebenen und mit marktübergreifender Relevanz	9
5. Allgemeingültige Definition von big data und AI weder möglich noch notwendig	11
II. Die immaterialgüter- und datenschutzrechtliche Perspektive: Drei Phasen im Rahmen typischer big data-Sachverhalte	14
1. Ausgangspunkt	14
2. Potenziell relevante materielle und immaterielle Rechtsobjekte in typischen big data-Prozessen	16
a) Erste Phase: Datenbeschaffung (gegebenenfalls inkl. Datenvalidierung)	17
b) Zweite Phase: Datenanalyse (gegebenenfalls inkl. Datenvalidierung)	19
c) Dritte Phase: Umgang mit den Ergebnissen der Analyse (inkl. Präsentation)	21
III. Identifizierbare Probleme der Datenökonomie und mögliche Lösungsansätze	22
1. Verlagerung und Spezifizierung der Diskussion um die Regulierung der Datenökonomie in den letzten Jahren	22

2. Grundlegende Zielsetzungen	25
a) Wirksamer Wettbewerb und Wahrung von Privatautonomie	26
b) Innovationsförderung	27
c) Wahrung grundrechtlich besonders geschützter Rechtspositionen	28
d) Wahrung öffentlicher Interessen	29
3. Konkrete Probleme und immaterialgüterrechtliche Forschungsherausforderungen	30
a) Möglicher Überschutz und Transaktionskosten	31
b) Mögliche Schwächen des derzeitigen rechtlichen und technischen Rahmens für den Zugang zu und die Teilung von Daten	32
aa) Institutionen für wettbewerbsbasierte Datenverbreitung und -nutzung	32
bb) Technische und organisatorische Standards für die Datenverarbeitung und Schnittstelle für Datenaustausch (Infrastrukturebene)	33
c) Neue bereichsspezifische Zugangsrechte in der Datenökonomie und Datenportabilität	35
4. Bedeutung der immaterialgüterrechtlichen Perspektive: „Hin- und Herwandern“ des Blicks	37
 C. Der urheberrechtliche Rahmen der Datenwirtschaft de lege lata und de lege ferenda	41
I. Überblick	41
II. Urheberrechtlicher Schutz für kreative und investitorische Leistungen in der Datenwirtschaft	42
1. Urheberrecht und Leistungsschutz an Datenbanken	42
a) Allgemeine Voraussetzungen	42
b) Urheberrechtlicher Datenbankwerkschutz	46
aa) Besondere Schutzvoraussetzung: Eigene geistige Schöpfung	46
bb) Schutzzumfang und Schranken	52
(1) Datenbankstruktur als Schutzgegenstand: Begrenzung auf strukturelevante Nutzungen	52
(2) Technisch notwendige Vervielfältigung der Datenbankstruktur als Voraussetzung der Datennutzung	53
(3) Nutzung der Datenbankstruktur und resultierende Probleme für die Datenwirtschaft	54

(a) Problem: Urheberpersönlichkeitsrechte, insbesondere Entstellungsschutz sowie Änderungsverbot	55
(b) Problem: Datenbankstruktur als Industriestandard und Reformbedarf auf der Ebene des Schutzgegenstands?	56
(c) Problem: Herstellung von Interoperabilität und Datenportabilität und Reformbedarf im Bereich der Schranken	58
cc) Zusammenfassung und Reformbedarf	59
c) Datenbankschutz sui generis	62
aa) Besondere Schutzvoraussetzung: Wesentliche Investition	62
(1) Wesentlichkeitskriterium als de minimis-Schwelle	62
(2) Investitionen in das „Beschaffen“ der Datenbankinhalte	64
(a) Restriktive Interpretation der Kommission und der überwiegenden Literatur	64
(b) Gebotene teleologische Interpretation der Abgrenzungskriterien „Beschaffen“ vs. „Erzeugen“ (teleologischer BHB/Hill-Test)	65
(c) Typische Szenarien in der Datenwirtschaft	68
(aa) Zurverfügungstellung von Daten insbesondere durch Nutzer von Dienstleistungen (<i>volunteered data</i>)	68
(bb) Betriebsdaten im engeren Sinne und Datenerhebung bei Gelegenheit des Betriebs einer Maschine im weiteren Sinne (<i>observed data</i>)	69
(cc) Derivative Daten (<i>inferred data</i>)	72
(dd) Metadaten	74
(ee) Alternative Gestaltungsmodelle	75
(3) Weitere Anknüpfungspunkte für berücksichtigungsfähige Investitionen in typischen big data-Sachverhalten	76
(4) Ausschluss typischer big data-Datenbanken nach der spin off-Theorie?	78
(5) Zusammenfassung und Reformbedarf	80
bb) Ausschließlichkeitsrechte des Datenbankherstellers	82
(1) Weite Auslegung der „Entnahme“ oder „Weiterverwendung“	82

(2) Begrenzung des Schutzgegenstands auf wesentliche Teile einer Datenbank	84
cc) Inhaberschaft des sui generis-Rechts	85
(1) Ausgangspunkt: Der Begriff des Datenbankherstellers und die vage Konkretisierung in Erwägungsgrund 41 S. 2 Datenbank-RL	85
(2) Resultierender Reformbedarf: Primat des Vertragsrechts	88
dd) Schranken (Ausnahmen) des Datenbankherstellerrechts	91
(1) Fehlende Kohärenz mit dem allgemeinen Urheberrecht	92
(2) Fehlende systematische Kohärenz mit dem Datenbankurheberrecht und Sonderproblem bei public sector information (PSI)	93
(3) Zusammenfassung und Reformbedarf	95
ee) Schutzdauer	96
(1) Angemessenheit der fünfzehnjährigen Schutzfrist	96
(2) Begründung einer eigenen Schutzdauer für Neuinvestitionen	96
(a) Ausgangspunkt und Begriff der Neuinvestitionen	96
(b) Schutzzumfang des sui generis-Rechts an der „veränderten“ Datenbank	97
(3) Verbleibende Probleme und Lösungsmöglichkeiten de lege ferenda	98
(a) Ewigkeitsschutz bei dauernd aktualisierten Datenbanken	98
(b) Nachweis- bzw. Nutzungsschwierigkeiten bei Teiländerungen	98
ff) Umwandlung des sui generis-Schutzrechts in ein Registerrecht	100
(1) Vorschläge zur Umwandlung in ein Registerrecht und kritische Bewertung	100
(2) Möglichkeiten der praktischen Umsetzung	104
(a) Beschreibung und Glaubhaftmachung des Datenbankinhalts	104
(b) Hinterlegung des gesamten Datenbankinhalts	105
(c) Hinterlegung des Hashwerts (kryptographischer Zeitstempeldienst)	106
(d) Vorzugswürdige praktische Umsetzung und Grenzen	108
gg) Verhältnis zu lauterkeitsrechtlichem Leistungsschutz in den Mitgliedstaaten	110

hh) Verallgemeinerung: Abgrenzung zu anderen Rechtsinstrumenten	112
ii) Zusammenfassung und Reformbedarf	112
2. Urheberrechtlicher Computerprogrammenschutz	115
a) Schutzvoraussetzungen und Schutzgegenstand	115
b) Schutzzumfang: Persönlichkeitsrechte und Verwertungsrechte	118
c) Schranken (Ausnahmen) vom urheberrechtlichen Schutz für Computerprogramme	119
III. Bereichsübergreifende Anpassung der allgemeinen urheberrechtlichen Schrankenregelungen an die Belange und Besonderheiten der Datenwirtschaft, insbesondere Text- und Data-Mining	121
1. Die neuen Text- und Data-Mining-Schranken der DSM-RL und bestehender weiterer Reformbedarf	121
2. Unzureichende Absicherungen gegen die Umgehung von Ausnahmen und Schranken in der InfoSoc-RL	125
a) Umgehung durch technische Schutzmaßnahmen (TPM)	125
b) Umgehung der Ausnahmen durch privatautonome Gestaltungen	125
3. Zusammenfassung und Reformbedarf	126
 D. Der patentrechtliche Rahmen der Datenwirtschaft de lege lata und de lege ferenda	 127
I. Zusätzliche Anreize für Schaffung und Offenlegung wertvoller Datensätze	128
II. Datenformate, Schnittstellen und Rolle des Patentrechts	130
III. Zugang zu Patentlizenzen im Bereich technischer Standards (standardessentielle Patente)	132
IV. Zusammenfassung und Reformbedarf	135
 E. Die Relevanz der Trade Secrets-RL für die europäische Datenwirtschaft de lege lata und de lege ferenda	 137
I. Schutzgegenstand	138
1. Weite Definition des Geschäftsgeheimnisses	138
2. Anknüpfungspunkte in typischen big data- und Industrie 4.0-Sachverhalten	141
a) Einzeldatum	142
b) Datensets	144

aa)	Kommerzieller Wert	144
bb)	Ausschluss belangloser Informationen	145
cc)	Geheimer Charakter	146
dd)	Angemessene Geheimhaltungsmaßnahmen	149
ee)	Zusammenfassung	151
c)	Algorithmen	151
d)	Neuronale Netze und separat gespeicherte Gewichtungsmatrizen	153
e)	Private Blockchains	153
f)	Software-Implementierungen	153
g)	„Negative Informationen“	154
3.	Zusammenfassung	155
II.	Schutzsubjekt: Inhaberschaft des Geschäftsgeheimnisses	156
1.	Ausgangspunkt: Vage Legaldefinition	156
2.	Lösungsvorschläge zur rechtssicheren Konkretisierung des Rechtsinhabers	157
a)	Rechtssicherheit durch privat- und parteiautonome Regelungen	157
b)	Fakultative Registrierung im „Geheimnisschutzregister“	159
III.	Schutzwirkung	163
1.	Grundsatz der Informations(zugangs)freiheit: Rechtmäßiger Erwerb, rechtmäßige Nutzung und Offenlegung	163
2.	Schutz vor bestimmten Verletzungshandlungen	168
a)	Rechtswidriger Erwerb	169
b)	Rechtswidrige Nutzung oder Offenlegung	170
c)	Erwerb, Nutzung und Offenlegung durch Dritte – Begrenzte Drittwirkung	174
d)	Rechtsverletzende Produkte	176
IV.	Ausnahmen	177
1.	Abwägung mit dem Recht der freien Meinungsäußerung und der Informationsfreiheit	177
2.	Whistleblowing-Ausnahme	178
3.	Sonstige legitime Interessen	181
V.	Flexible Durchsetzungsvorschriften	182
VI.	Zusammenfassung und Reformbedarf	184
F.	Datenschutz und DSGVO	191
I.	Ausgangspunkt: Freier Datenverkehr vs. Schutz des Einzelnen	193
1.	Regelungsziele der Datenschutzgrundverordnung	194
a)	Schutz personenbezogener Daten	194

	b) Gewährleistung freien Datenverkehrs	195
	2. Datenschutzrecht als Ausschließlichkeitsrecht für personenbezogene Daten?	197
II.	Spannungsverhältnis zwischen big data und Datenschutz	199
	1. Veränderte Verarbeitungsprozesse durch big data	199
	2. Datenschutzrechtliche Interessenlage bei big data	201
	a) Interessen der Wettbewerber auf Datenmärkten	201
	b) Interessen der Marktgegenseite (Kunden und Verbraucher)	203
	c) Interessen der Öffentlichkeit bzw. Allgemeinheit	204
III.	Anwendungsbereich der DSGVO in big data-Sachverhalten	205
	1. Gegenstand: Verarbeitung personenbezogener Daten	205
	a) Begriff der personenbezogenen Daten	205
	b) Pseudonymisierung und Verschlüsselung	208
	2. Besondere Arten personenbezogener Daten	209
	a) Grundsatz des Verarbeitungsverbots	210
	b) Einwilligung in die Verarbeitung besonderer Arten personenbezogener Daten	211
	c) Ausnahme vom Verarbeitungsverbot: Öffentlich zugänglich gemachte Daten	213
	3. Anonymisierte Daten	214
	a) Vorgaben der DSGVO zur Anonymisierung	215
	b) Probleme der Anonymisierung bei big data	216
	aa) Gefahr der Re-Identifizierung	216
	bb) Folgen nachträglicher Identifizierung bzw. unzureichender Anonymisierung	217
	c) Probleme rein technischer Anonymisierungsverfahren	218
	d) Weitergehende technische und organisatorische Maßnahmen – best practices und Standards	219
	e) Rechts- und Interessenausgleich: Widerlegliche Vermutung der Anonymisierung	219
	aa) Vergleichbare Ansätze weltweit	220
	bb) Umsetzung in der EU	222
	cc) Interimslösungen für Anonymisierung	224
	f) Art. 11 DSGVO als Ansatzpunkt?	224
	g) Ausnahmetatbestand für vorübergehende Datenspeicherung zu Anonymisierungszwecken?	225
	h) Zusammenfassung und Reformbedarf	225
IV.	Grenzüberschreitender Datenverkehr	227
	1. Territorialer Anwendungsbereich der DSGVO	227

a)	Weitreichende Geltung der DSGVO für Stellen außerhalb der EU	227
b)	Einschränkung der Reichweite auf Ebene der Betroffenenrechte	228
2.	Voraussetzungen der DSGVO für den Datentransfer in Drittstaaten	230
a)	Angemessenheitsbeschluss	231
b)	Geeignete Garantien	232
aa)	Standardvertragsklauseln (SCC)	233
bb)	Binding Corporate Rules (BCR)	235
cc)	Codes of conduct	235
dd)	Zertifizierung	236
c)	Ausnahmetatbestände des Art. 49 DSGVO:	
	Beschränkte Reichweite	237
aa)	Ausdrückliche Einwilligung in den Datentransfer	237
bb)	Zur Vertragserfüllung erforderlicher Datentransfer und zwingendes berechtigtes Interesse	238
d)	Bewertung und Folgerungen	239
V.	An der Datenverarbeitung Beteiligte:	
	Verantwortliche – Auftragsverarbeiter – Betroffene	239
1.	Verantwortlicher vs. Betroffener	239
2.	Gemeinsame Verantwortlichkeit (Joint Controllership)	240
a)	Voraussetzungen der gemeinsamen Verantwortlichkeit	242
b)	Folge der gemeinsamen Verantwortlichkeit: Klar abgegrenzte Verantwortungsbereiche?	243
c)	Abgrenzung der gemeinsamen Verantwortlichkeit von der Auftragsverarbeitung	245
d)	Weitere Konstellationen	246
VI.	Grundvoraussetzung: Rechtmäßigkeit der Datenverarbeitung	247
1.	Erforderlichkeit der Festlegung einer spezifischen Verarbeitungsgrundlage	247
2.	Einwilligung des Betroffenen	248
a)	Bedeutung der Einwilligung	248
b)	Grundproblem: Einwilligung bei multipolaren Strukturen	250
c)	Voraussetzungen einer wirksamen Einwilligung im Datenschutzrecht	252
aa)	Freiwilligkeit der Einwilligung	252
(1)	Unterschiedliche Auslegung der Freiwilligkeit in den Mitgliedstaaten	252

(2) Spannungsverhältnis zwischen Freiwilligkeit der Einwilligung und Vertragsrecht: „Dienste gegen Daten“	253
(a) Hintergrund	253
(b) Freiwilligkeit der Einwilligung bei „Diensten gegen Daten“?	256
(c) Andere Verarbeitungsgrundlagen für Fälle von „Diensten gegen Daten“?	258
(d) Bewertung und Folgerungen	260
bb) Bestimmtheit der Einwilligung	260
cc) Informierte Einwilligung	261
dd) Unmissverständlichkeit der Einwilligung	263
ee) Abgrenzung der Einwilligung von erforderlicher Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DSGVO	264
ff) Bewertung und Folgerungen	267
d) AGB-rechtliche Kontrolle der Einwilligungserklärung	268
e) Widerruf der Einwilligung	269
f) Zusammenfassung und Reformbedarf	273
3. Berechtigte Interessen des Verantwortlichen	275
a) Bedeutung der Interessenabwägung	275
b) Struktur der Interessenabwägung	276
c) Interessenabwägung im engeren Sinne	277
aa) Interessen des Verantwortlichen	277
bb) Interessen des Betroffenen	278
d) Widerspruchsrecht des Betroffenen	279
e) Bewertung und Folgerungen	280
4. Möglichkeiten der Zweckänderung einer Datenverarbeitung	282
a) Exkurs: Spannungsverhältnis zwischen Grundsätzen des Datenschutzes und big data	282
b) Zweckbindung vs. Zweckänderung	283
aa) Einwilligung in die Zweckänderung der Datenverarbeitung	285
bb) Erlaubte Zweckänderung bei Kompatibilität der Verarbeitungszwecke	285
cc) Privilegierung der Zweckänderung bei Forschungszwecken bzw. statistischen Zwecken	287
c) Bewertung und Folgerungen	290
5. Zusammenfassung und Reformbedarf	291
VII. Betroffenenrechte	294
1. Allgemeine Vorgaben für die Betroffenenrechte	295

2. Betroffenenrechte – entgrenzte Pflichten oder Verhältnismäßigkeit?	295
3. Auskunftsrecht	296
a) Reichweite des Auskunftsrechts	296
aa) Nur Auskunft oder Recht auf Kopie?	296
bb) Erforderlicher Umfang der Auskunft	299
cc) Sonderfall: Auskunft bei automatisierten Entscheidungen, insbesondere Scoring	300
b) Einschränkungen des Auskunftsrechts bei Datenverarbeitung zu Forschungszwecken	301
c) Einschränkung des Auskunftsrechts durch Interessenabwägung	301
aa) Geschäftsgeheimnisschutz vs. Auskunftsinteresse des Berechtigten	302
bb) Rechte des geistigen Eigentums vs. Auskunftsinteresse des Berechtigten	304
cc) Auskunftsinteresse bei Daten Dritter?	304
dd) Auskunftsinteresse bei nicht identifizierbaren Betroffenen?	305
ee) Folgen für Auskunftserteilung	305
d) Bewertung und Folgerungen	306
4. Recht auf Löschung („Recht auf Vergessenwerden“)	307
a) Recht auf Löschung – Pflicht zur Löschung	307
b) Technische Alternativen zur Löschung?	308
c) Einschränkungen der Löschpflicht des Verantwortlichen	310
d) Sonderfall: Recht auf Löschung bzw. Vergessenwerden bei Suchmaschinen	311
e) Löschpflichten und „künstliche Intelligenz“	313
5. Recht auf Berichtigung	315
6. Datenportabilität gemäß Art. 20 DSGVO	315
a) Vom Portabilitätsrecht betroffene Datenverarbeitungen	315
b) Sinn und Zweck des Portabilitätsrechts	316
c) Gegenstand des Portabilitätsrechts: Bereitgestellte Daten	318
d) Form der zu portierenden Daten	320
aa) Strukturiertes, gängiges und maschinenlesbares Format	320
bb) Spezialfall: Datenübermittlung an andere Anbieter	321
e) Technische Umsetzungsansätze für das Portabilitätsrecht	322
f) Bestehende Ansätze für die praktische Umsetzung des Portabilitätsrechts	324
aa) Mittel zur effektiven Durchsetzung des Portabilitätsrechts	325
(1) Art. 20 DSGVO als Marktverhaltensregelung	325
(2) Übertragbarkeit des Portabilitätsrechts	326

bb) Übertragungs- und Exporttools	327
cc) Personal Information Management-Systeme und user centric approach	327
dd) Single sign on-Dienste	330
ee) Branchenspezifische Lösungen und Datentreuhändermodelle	331
ff) Datenverwertungsgesellschaften und gerätebasierte Datenverwaltung	332
gg) Bewertung und Folgerungen: Bedeutung von Datenintermediären	333
g) Einschränkung des Portabilitätsrechts durch Interessenabwägung	333
aa) Herausgabe von Daten Dritter?	333
bb) Geschäftsgeheimnisschutz vs. Interesse des Betroffenen	335
cc) Rechte des geistigen Eigentums vs. Interesse des Betroffenen	336
dd) Nutzungszweck als Abgrenzungskriterium für die herauszugebenden Daten?	338
ee) Weitere Einschränkungen des Portabilitätsrechts?	339
h) Datenportabilität gemäß Art. 16 Abs. 4 Digitale Inhalte-RL	339
i) Verallgemeinerungsfähigkeit des Rechts auf Datenportabilität?	342
j) Bewertung und Folgerungen	347
7. Zusammenfassung und Reformbedarf	351
VIII. Risikobasierter Ansatz der DSGVO – Chance oder Bürde für big data?	353
1. Allgemeine Pflicht zur Datenschutzfolgenabschätzung?	354
a) Erforderlichkeit einer Datenschutzfolgenabschätzung	354
b) Kriterien für die Risikobewertung	355
c) Leitlinien der Datenschutzbehörden	356
d) Problem: Zentralisierte Risikobewertung bei dezentralisierter Datenverarbeitung	357
e) Bewertung und Folgerungen	358
2. Privacy by design und privacy by default – Umsetzbarkeit bei big data?	358
3. Technische und organisatorische Maßnahmen als Mittel der Risikominimierung?	362
4. Berücksichtigung der Unternehmensgröße?	363
5. Zusammenfassung und Reformbedarf	364
IX. DSGVO und „Künstliche Intelligenz“: Verbot der automatisierten Einzelentscheidung	364

1. Voraussetzung: Ausschließlich auf automatisierter Datenverarbeitung beruhende Entscheidung	365
2. Unmittelbare rechtliche Wirkung oder vergleichbare erhebliche Beeinträchtigung	366
a) Allgemeine Anforderungen an rechtliche Wirkung und erhebliche Beeinträchtigung	366
b) Einzelfälle rechtlicher Wirkung und erheblicher Beeinträchtigung	367
3. Erlaubnistatbestände des Art. 22 Abs. 2 DSGVO	369
4. Umfang der Informations- und Auskunftspflichten bei automatisierten Einzelentscheidungen	370
a) Offenlegung von Algorithmen und Formeln?	370
b) Offenlegung konkret getroffener Einzelentscheidung?	372
c) Erforderlichkeit geeigneter Maßnahmen und Garantien	373
5. Zusammenfassung und Reformbedarf	375
a) Verbot automatisierter Einzelentscheidungen im System der DSGVO	375
b) Keine datenschutzrechtlichen Offenlegungspflichten	376
c) Algorithmenregulierung: Kein primärer Gegenstand des Datenschutzrechts	376
X. Datenschutzverstöße: Remedies – Enforcement – Accountability	379
1. Grundproblem 1: Zentralisierte Verantwortlichkeit bei dezentralisierter Verarbeitung	380
2. Grundproblem 2: Inkohärente Bewertung durch mitgliedstaatliche Datenschutzbehörden	381
3. Anspruch auf Schadensersatz bei Datenschutzverstößen	381
4. Bußgelder und sonstige Sanktionen für Datenschutzverstöße	383
5. Privatrechtliche Durchsetzung der DSGVO?	384
a) Durchsetzung im Wege des Rechts des unlauteren Wettbewerbs?	384
b) Durchsetzung im Wege des Kartellrechts?	386
XI. Bereichsspezifische Sonderregeln des Datenschutzrechts, insbesondere ePrivacy-RL	389
XII. Ausblick: Funktionale Schwächen der angestammten Datenschutzkonzeption und mögliche alternative Lösungsansätze	391
1. Überlegungen zu weitergehenden Rechten zum Schutz der Privatsphäre?	391
2. Vertragsrecht als Lösung	394
a) Bedeutung des AGB-Rechts	394
b) Transparenz als allgemeiner Wertungsmaßstab	394

c) Wechselspiel zwischen datenschutzrechtlichen Vorgaben und Vertragsbedingungen	395
d) Standardverträge und Selbstverpflichtung	395
e) Weitergehender Lösungsansatz: Personal information management-Systeme und datenschutzrechtliches Lizenzvertragsrecht	397
XIII. Zusammenfassung und Reformbedarf	401

G. Reformperspektive: Immaterialgüter- und datenschutzrechtliche Probleme, Trends und Building Blocks für die Datenökonomie 409

I. Möglicher Überschutz und Transaktionskosten	409
1. Anreizgedanke für Datenproduktion und effiziente Datendissemination als inhärente Grenze des Schutzgegenstands	409
2. Funktionale Grenzen zentralisierter Ausschließlichkeitsrechte in big data-Szenarien und besondere Bedeutung des Vertragsrechts	411
3. Schutzrechtsüberschneidung als Problem für Datenzugang . . .	414
4. Trend de lege ferenda: Sinkende Schutzfristen und langfristig wachsende Bedeutung von Registerrechten	417
II. Flexible Hybride zwischen Ausschließlichkeitsrecht und verhaltensbezogener Regelung: Begrenzte Drittwirkung vertraglicher Vereinbarungen als Paradigma für die Datenökonomie?	420
1. Kommerzialisierung von Daten und der immaterialgüterrechtliche und datenschutzrechtliche Rahmen . .	420
2. Qualifizierte Drittwirkung vertraglicher Vereinbarungen in Anlehnung an den Geschäftsgeheimnisschutz?	422
a) Grenzen des bestehenden Geschäftsgeheimnisschutzes und Vorschläge bzw. Modelle für eine Ausdehnung des Prinzips begrenzter Drittwirkung	422
b) Bestehendes zivilrechtliches Instrumentarium (insbesondere § 241 Abs. 2 BGB)	423
3. Mögliche lauterkeitsrechtliche Ansätze de lege lata und de lege ferenda?	426
III. Neue Zugangsrechte in der Datenökonomie, Datenportabilität und die Schnittstelle zum Immaterialgüter- und Datenschutzrecht . . .	428
1. Verlagerung der Diskussion in Richtung (bereichsspezifischer) Zugangsrechte	428
2. Die Unterscheidung von Zugangsrechten und Nutzungsmöglichkeiten und -rechten	429

a) Grundsatzüberlegung: Nur indirekte Relevanz des Immaterialgüterrechts bezüglich Zugangsregimes	429
b) Besonderheiten bei Geschäftsgeheimnissen und Bedeutung des bestehenden kartellrechtlichen Rahmens	431
c) Verbleibende Bedeutung des Immaterialgüterrechts als Leitbild für Ausgestaltung nachfolgender Nutzungsmöglichkeiten	435
3. Relevante Szenarien für Zugangsrechte und die Schnittstelle zum Immaterialgüterrecht hinsichtlich der Nutzungsregelung	435
a) Relevante Szenarien für Zugangs- und Nutzungsregimes	435
b) Schnittstelle zum Immaterialgüterrecht, insbesondere Datenbankschutzrecht sui generis	438
aa) Berücksichtigung auf der Ebene von Schutzvoraussetzungen und Schutzgegenstand	438
bb) Fallgruppen spezifischer Zugangsinteressen trotz grundsätzlich bestehenden immaterialgüterrechtlichen Schutzbedarfs	439
(1) Zugangs- und Portabilitätsrechte betreffend individual level use data für „berechtigte Nutzer“ von smart devices	440
(a) Regelung der Mindestrechte des „rechtmäßigen Nutzers“ im digitalen Urheberrecht als bestehende funktionale Entsprechung	440
(b) Folgerung hinsichtlich der Portabilität auf der Nutzungsebene: In der Regel keine zusätzliche Vergütung bei individual level data berechtigter Nutzer	443
(c) Zwingende sektorspezifische Zugangs- und Portabilitätsrechte für berechtigte Nutzer?	444
(d) Zusammenfassung und Reformbedarf in der Datenbank-RL	446
(2) Zugangs- und Nutzungsrechte betreffend komplette Datenstrukturen oder Datensets für Wettbewerber (aggregated data)	448
(a) Grundsätzlich mit verhandelter Vergütung (Zwangslizenz, liability rule)	448
(b) Zwangslizenzen auf kartellrechtlicher Grundlage	449
(c) Neue Zwangslizenzregelung für sui generis-geschützte sole source Datenbanken in der Datenbank-RL	451

(d) Nutzungsumfang und FRAND-Vergütung	453
(e) Gegenlizenzen (Kreuzlizenzen)	454
(f) Zugangsansprüche bei geheimen Informationen . .	455
4. Portabilität und Interoperabilität	457
Literaturverzeichnis	461
Sachregister	495

A. Einführung

Der angemessene und sichere *Zugang zu Daten* in hinreichender *Qualität* steht im Mittelpunkt der von Daten vorangetriebenen Innovation. Zugleich wirft der digitale Strukturwandel in Gestalt von big data diverse ethisch-philosophische, sozialwissenschaftliche, ökonomische, politische und rechtliche Fragen auf.

Die zugrundeliegenden Zielsetzungen sind zum Teil *komplementär*. So entspricht es dem heutigen Stand der Forschung, dass die Zielsetzung *freier Datenmärkte mit funktionierendem Wettbewerb* zur Zielsetzung der *Innovationsförderung*, idealerweise in einem *Komplementaritätsverhältnis* steht.¹ Hier sind mit Blick auf die Datenökonomie in erster Linie *funktionale Rahmenbedingungen* zu schaffen, die dieses Komplementaritätsverhältnis angemessen ausgestalten. Diese Aufgabe ist insbesondere für das Immaterialgüterrecht nicht neu – es geht also eher um eine *Anpassung des rechtlichen Rahmens* an neue, so bisher nicht dagewesene regulatorische Herausforderungen der Datenökonomie. Das betrifft insbesondere die Sicherstellung eines angemessenen *Zugangs zu notwendigen Daten* bei gleichzeitig hinreichender Wahrung tatsächlich notwendiger *Anreize*, um Innovation optimal zu ermöglichen, insbesondere aber auch um der Ausprägung marktübergreifender Machtpositionen vorzubeugen oder jedenfalls deren Missbrauch zu unterbinden.²

Darüber hinaus sind zweifellos auch regelrecht *divergierende Rechte und Interessen* zu angemessenem, verhältnismäßigem Ausgleich zu bringen. Das heißt, es ist anzuerkennen, dass bestimmte weitere verfassungsrechtlich abgesicherte, ethische und politische Zielsetzungen in einem Spannungsverhältnis zu Wettbewerbsfreiheit und angemessenen Innovationsanreizen stehen können. So hat ein

¹ Die Zielsetzung der *Innovationsförderung* kann es auch erforderlich machen, bestimmte Marktchancen mit Ausschließlichkeitscharakter (ausschließliche Rechte) oder auch in Form bestimmter Abwehrrechte (bloße rechtlich abgesicherte Freiheiten) einzelnen Marktteilnehmern zuzuweisen.

² An dieser Stelle ist naturgemäß ganz zentral auch das Kartellrecht angesprochen. Angesichts des in diesem Bereich auf deutscher und europäischer Ebene vergleichsweise schon überaus fortgeschrittenen Forschungsstandes wird das Kartellrecht in dieser Untersuchung als eigenständiger Gegenstand allerdings ausgespart, dennoch informiert die diesbezügliche Forschung natürlich ganz konkret auch viele der hier angestellten Überlegungen und entwickelten Vorschläge insbesondere im Immaterialgüterrecht, vgl. unten S. 35.

falsch verstandener *Datenschutz* durchaus das Potential, die von Daten vorangetriebene Innovation nachhaltig zu hemmen. Einerseits muss es hier wiederum darum gehen, die diesbezüglich dennoch vorhandenen Potentiale für mögliche *Konvergenzen* dieser Zielsetzungen durch entsprechend funktional ausgestaltete institutionelle Rahmenbedingungen zunächst einmal auszuschöpfen. Zum Beispiel kann ein angemessen und praxistauglich ausgestalteter Schutz persönlicher Daten zweifellos das Vertrauen der Datensubjekte in den rechtlichen Rahmen stärken und damit zur Bereitschaft beitragen, persönliche Daten für bestimmte Innovationszwecke überhaupt erst zur Verfügung zu stellen. Andererseits ist aber zugleich auch anzuerkennen, dass bestimmte verfassungsrechtlich abgesicherte Rechtspositionen gegebenenfalls auch dazu führen können, dass nicht allein ein *Maximum* an datengetriebener, effizienter Innovation anzustreben ist, sondern vielmehr ein *Optimum* angemessenen Ausgleichs zwischen den unterschiedlichen involvierten Rechten, Interessen und Werten im Sinne praktischer Konkordanz. Hier sind zugleich ersichtlich auch zahlreiche *weitere private und öffentliche Interessen* betroffen, wie etwa der Schutz vor *Diskriminierung*, *Informationsfreiheit* als Funktionsvoraussetzung demokratischer Willensbildungsprozesse, *Fairness* und *Vertrauen*.

Angesichts dieser komplexen Gemengelage herrscht über die richtigen regulatorischen Rahmenbedingungen derzeit in weiten Bereichen noch *Unsicherheit*. Diese beruht teilweise auf *fehlenden Informationen* über die Funktionsbedingungen neuer datengetriebener Innovationsräume und Geschäftsmodelle. Teilweise sind auch schlichtweg die *politischen Wertentscheidungen* noch nicht getroffen, die notwendig sind, um divergierende Rechte und Interessen in einen angemessenen Ausgleich zu bringen und dabei zugleich hinreichende *Handlungsspielräume* für Wettbewerb und Innovation zu sichern, die dann ihrerseits garantieren, dass die resultierenden Zielsetzungen auch effizient erreicht werden können. Hinzu kommt die Tatsache, dass sich die aufgeworfenen Rechtsfragen naturgemäß nicht *abstrakt allgemeingültig*, sondern vielmehr nur *konkret bereichsspezifisch* beantworten lassen werden.

Die derzeit demnach teilweise bestehende *Unsicherheit* über Chancen und Risiken der Datenökonomie und ihre zutreffende *bereichsspezifische Regulierung* ist kein rechtspolitisches Zukunftsproblem. Vielmehr spiegelt sie sich bereits konkret in erheblicher *Rechtsunsicherheit* auf Grundlage der *lex lata* überall dort, wo europäische Regelungsinstrumente auf dem Wege von unbestimmten Rechtsbegriffen und Generalklauseln der Rechtsprechung erhebliche Spielräume zur Rechtskonkretisierung und -fortentwicklung einräumen. Das betrifft insbesondere, aber nicht nur den datenschutzrechtlichen Rahmen für big data in Europa. Die Eigenheiten der Rechtsauslegung und Rechtsfortbildung im europäischen Mehrebenensystem führen dabei dazu, dass eine verlässliche Klärung der wesentlichen-

ten offenen Fragen unter diesen Bedingungen erhebliche Zeit beansprucht und häufig zudem – auf europäischer Ebene – eher lediglich allgemeine Leitlinien vorgegeben werden, die die Rechtsanwendung im konkreten Einzelfall unter Hinweis auf die allgemeinen Rechtsgrundsätze des Unionsrechts wiederum den mitgliedstaatlichen Gerichten überlassen. Tatsächlich kann angesichts bestehender informationeller Unsicherheiten eine derartige offene Regulierung im Wege flexibler *standards* statt konkreter und bestimmter *rules* auch in vielen Bereichen ersichtlich gerade der richtige regulatorische Ansatz sein. Zugleich ist aber im Interesse der dynamischen Entwicklung der datengetriebenen Innovation dafür zu sorgen, dass entsprechende Unsicherheiten nicht zu derart erheblichen *chilling effects* führen, dass diese – selbst im Verhältnis zu möglichen zukünftigen Effizienzgewinnen aufgrund solcherart abgesicherter Spielräume für die iterative Rechtsentwicklung – nicht mehr zu rechtfertigen wären.

Vor diesem Hintergrund setzt sich die vorliegende Untersuchung im Wesentlichen zwei Ziele. *Erstens* soll auf Grundlage der *lex lata* der regulatorische Rahmen für big data im europäischen Datenschutz- und Immaterialgüterrecht umfassend dargestellt und diskutiert werden, so dass eine entsprechend *verlässliche Informationsgrundlage bezüglich des bestehenden gesetzlichen Rahmens für big data* mit seinen schon de lege lata existierenden erheblichen *Gestaltungsspielräumen* zur Verfügung steht. Das soll auch dazu beitragen, durch Gewährleistung einer gewissen minimalen Berechenbarkeit die Möglichkeit für risikoaffine Marktteilnehmer zu stärken, bestimmte innovative Ansätze zum Ausgleich der Interessen in der Rechtsprechung „testen“ zu lassen. Nur so können sich schließlich auf iterativem Wege in der Rechtsprechung neue, angemessene Lösungsansätze kristallisieren.

Auf der solcherart erarbeiteten Basis soll, *zweitens*, ein *Abgleich* der zwischenzeitlich in der Forschung in bestimmten Szenarien als besonders wesentlich für die Datenökonomie identifizierten und strukturierten Funktionsbedingungen eines angemessenen *Zugangs zu und der Teilung von Daten in hinreichender Qualität* mit den diesbezüglich relevanten datenschutz- und immaterialgüterrechtlichen Rahmenbedingungen erfolgen. Hinsichtlich dieser zweitgenannten Zielsetzung geht es um einen ganzheitlichen Ansatz im Sinne einer Art „*Hin- und Herwandern des Blicks*“: Einerseits werden Defizite des bestehenden Datenschutzes- und Immaterialgüterrechts identifiziert und entsprechend *konkret dringliche Reformvorschläge* unterbreitet. Andererseits ist zugleich anzuerkennen, dass die künftige Regulierung der Datenökonomie Wertentscheidungen erfordert, die ihrerseits unvermeidlich von der objektiven Werteordnung des bestehenden Wettbewerbsrechts, des Vertragsrechts, aber auch des Datenschutzes- und Immaterialgüterrechts und weiterer Rechtsgebiete informiert und beeinflusst werden. Das heißt, das das Datenschutz- und insbesondere das Immaterialgüter-

recht halten nach der hier zugrunde gelegten Untersuchungsprämisse schon heute bestimmte gesetzgeberische Wertentscheidungen, Strukturen und Instrumente bereit stellt, die ihrerseits für bestimmte Aspekte der künftigen Regulierung der Datenökonomie relevant sind, ja teilweise Vorbildcharakter haben oder zumindest bestimmte konkrete building blocks für bestimmte regelungsbedürftige Einzelszenarien bereitstellen könnten.

Der Schwerpunkt der Untersuchung wird dabei hinsichtlich des identifizierten kurzfristigen Reformbedarfs wesentlich beim sui generis-Schutzrecht für Datenbanken, bei bestimmten Aspekten des Schutzes von Geschäftsgeheimnissen sowie bei Einzelheiten des datenschutzrechtlichen Rahmens liegen. Demgegenüber erscheinen das allgemeine Urheberrecht sowie das Patentrecht in Europa (mit kleineren Einschränkungen) vergleichsweise fit für die Datenökonomie. Hier werden eher bestimmte Details angesprochen und angemahnt, die zum Teil auch in der Praxis der Patentämter und der Rechtsprechung hinreichend gelöst werden könnten.

B. Grundlagen

I. Strukturwandel durch big data und AI

1. Big data

Eine *allgemeingültige Definition* des Begriffs „big data“ existiert nicht. Typischerweise wird auf die drei *Strukturmerkmale volume, velocity und variety* abgestellt.¹ Teilweise wird diese Definition noch um das Element der *veracity*, also Richtigkeit bzw. Zuverlässigkeit der Daten², sowie um weitere Elemente ergänzt.³

Die Strukturmerkmale des Umfangs der Datenmengen und der Verarbeitungsgeschwindigkeit verdeutlichen, dass es bei den neuen big data-Anwendungsmöglichkeiten in erster Linie um die Ableitung von Erkenntnisgewinn aufgrund der heute praktisch unbegrenzt *skalierbaren* Auswertung großer Datenmengen geht.⁴ Die insoweit neue Qualität beruht in erster Linie auf dieser *Skalierbarkeit* der zugrundeliegenden Datenmengen aufgrund heute praktisch unbegrenzter Speicherkapazitäten in der Cloud und der Geschwindigkeit der Verarbeitung dieser Daten – gerade soweit der Datenauswertung klassische kybernetische Methoden der sechziger Jahre zugrunde liegen, aber auch im Bereich der auf mathematischen Weiterentwicklungen seit den achtziger Jahren beruhenden neueren Methoden der AI und insbesondere des machine learning (ML).⁵ Das Element der

¹ Vgl. *Fasel/Meier*, in: Fasel/Meier (Hrsg.), *Big Data. Grundlagen, Systeme und Nutzungspotenziale*, S. 5–6; *Schütze/Hänold/Forgó*, in: Kolany-Raiser/Heil/Orwat et al. (Hrsg.), *Big Data und Gesellschaft, Eine multidisziplinäre Annäherung*, S. 233, 237 jeweils m. w. N.

² Zu den teilweise unklaren (Rechts-)Begriffen „Daten“ und „Informationen“ unten Fn. 33.

³ Vgl. zum Element der *Veracity* sowie weiteren Begriffsergänzungen *Gervais*, *JIPITEC* 2019, 22, 23 m. w. N.

⁴ Vgl. dazu *Sagstetter*, in: Husemann/Korves/Rosenkranz et al. (Hrsg.), *Strukturwandel und Privatrecht*, S. 249 Fn. 1 m. w. N. Zur Menge der weltweit produzierten Daten (33 Zettabyte im Jahr 2018; voraussichtlich 175 Zettabyte im Jahr 2025) jüngst etwa Mitteilung der Kommission v. 19.2.2020, Eine europäische Datenstrategie (im Folgenden *Datenstrategie*), COM(2020) 66 final, 2 m. w. N.

⁵ Vgl. dazu *Sagstetter*, in: Husemann/Korves/Rosenkranz et al. (Hrsg.), *Strukturwandel und Privatrecht*, S. 251–252 m. w. N.

variety verdeutlicht, dass die Datengrundlage aus einer *Vielfalt vollkommen unterschiedlicher strukturierter, semi-strukturierter oder unstrukturierter Daten aus einer Vielzahl unterschiedlicher Quellen* stammen kann, die mit Hilfe teils hergebrachter, teils neuerer Methoden und Algorithmen ausgewertet wird.⁶

2. Soziale und ökonomische Funktion entscheidend für die rechtliche Strukturierung

Für die juristische Annäherung an das Phänomen big data sind dabei weniger die technischen Grundlagen, als vielmehr die *soziale und ökonomische Funktion* der technologischen Entwicklungen entscheidend⁷: Durch die Modellierung und Analyse großer und vielfältiger Datenmengen aus einer Vielzahl kreativ kombinierter Quellen sowie Auswertungsinstrumente und -parameter sollen *neue Erkenntnisse gewonnen* werden, die sich in Ansehung einzelner Datensätze so nicht erschlossen hätten.⁸ Diese neuen Erkenntnisse können Ausgangspunkt der Entwicklung *neuer Dienste und Produkte* sein, die teils Effizienzgewinne ermöglichen (gezieltes Marketing, Bild- und Mustererkennungsverfahren in der Medizin und vielen anderen Bereichen), teils bestehende Bedürfnisse auf vollkommen neuartige, innovative Art und Weise befriedigen (smart grids, smart farming), damit neue Märkte erschließen und sich entsprechend *disruptiv auf bestehende Märkte* auswirken können.⁹ Wegen des Strukturmerkmals der *variety*, der marktübergreifenden Vielfalt zugrundeliegender Daten und des – teils unvorhersehbaren – marktübergreifenden oder markteröffnenden Werts der gewonnenen neuen Informationen, können derartig gewonnene Erkenntnisse überdies Ausgangspunkt *neuartiger Verbundeffekte* sein, die *marktübergreifend* neue Räume für Innovation überhaupt erst eröffnen.¹⁰

Daten und Informationen sowie die *Instrumente zu ihrer Auswertung* werden damit in höherem Maße als bisher zu einem eigenständigen Marktfaktor; ein Marktfaktor, der wegen der hierdurch ermöglichten werthaltigen Einsatz- und Innovationsmöglichkeiten einen *eigenständigen signifikanten Marktwert* über die Generierung marktbezogenen Wissens hinaus aufweist.

⁶ Vgl. dazu *Sagstetter*, in: Husemann/Korves/Rosenkranz et al. (Hrsg.), *Strukturwandel und Privatrecht*, S. 251–252; *Fasel/Meier*, in: Fasel/Meier (Hrsg.), *Big Data. Grundlagen, Systeme und Nutzungspotenziale*, S. 3, 5–6 jeweils m. w. N.

⁷ S. dazu *Surblytė-Namavičienė*, S. 8 ff.

⁸ Vgl. dazu *Sagstetter*, in: Husemann/Korves/Rosenkranz et al. (Hrsg.), *Strukturwandel und Privatrecht*, S. 249 Fn. 1 m. w. N.

⁹ Vgl. etwa auch die zahlreichen Beispiele in der Datenstrategie, COM(2020) 66 final, 2 ff.

¹⁰ Vgl. *Schweitzer*, GRUR 2019, 569 f.

Hinsichtlich der *Auswertungsinstrumente* in big data-Sachverhalten steht in der heutigen Diskussion der, wiederum schillernde und wenig trennscharfe¹¹, dabei zugleich linguistisch aus deutscher Sicht in die Irre führende¹² Begriff der *artificial intelligence* (AI) im Mittelpunkt. Die hierdurch bezeichneten Phänomene reichen selbst innerhalb des derzeit wesentlichsten innovativen Unterbereichs des sogenannten *machine learning* (ML) von klassischen lediglich weiterentwickelten *regelbasierten statistisch-empirischen Methoden* der Mustererkennung bis hin zu mehr oder weniger autonomem machine learning im Rahmen *neuroner Netze*.¹³ Hinzu kommen neue Methoden, die ebenfalls im Bereich des machine learning eingesetzt werden können, dabei aber über ein weiteres Einsatzfeld verfügen und damit den angestammten Bereich des machine learning sprengen, wie insbesondere *evolutionary algorithms* und verwandte Forschungsansätze.¹⁴

3. Datenzugang und Datenqualität als Bottleneck

Unabhängig von dieser Diversität der zugrundeliegenden Methoden ist angesichts der weitgehenden Verfügbarkeit von Rechenleistung das derzeit wesentlichste Bottleneck für Innovationen im Bereich des machine learning unstreitig der *Zugang* zu und die Generierung von *Trainingsdaten* in hinreichender *Qualität*, *Quantität* und *Varietät* sowie die innovative Entwicklung und Kombination entsprechender *Algorithmen*, um zweckgerichtete Analyseinstrumente zur Verfügung zu stellen und *biases*¹⁵ zu vermeiden.¹⁶ Hinsichtlich des Zugangs zu *Analy-*

¹¹ Vgl. *Drexl/Hilty/Beneke et al.*, Max Planck Institute for Innovation & Competition Research Paper No. 19-13, S. 1, 3; *Fink*, ZGE 2017, 288, 297: „AI is whatever hasn't been done yet“; *Sagstetter*, in: Husemann/Korves/Rosenkranz et al. (Hrsg.), Strukturwandel und Privatrecht, S. 249 Fn. 1 m. w. N.

¹² Suggestiert doch schon der Begriff der *intelligence* in der deutschen Sprache unvermeidlich einen engen Zusammenhang mit „Intelligenz“, während der Begriff im Englischen sehr viel neutraler auch für „Informationsgewinnung“ steht.

¹³ Für einen guten besonders bündigen Überblick über die technischen Grundlagen vgl. *Drexl/Hilty/Beneke et al.*, Max Planck Institute for Innovation & Competition Research Paper No. 19-13, 1 f.; *Stiemerling/Ehinger*, CR 2018, 761 f.; *Stiemerling*, CR 2015, 762 f. Vgl. allgemein zu *machine learning* auch COM(2018), 237 final, S. 10.

¹⁴ Vgl. etwa *Drexl/Hilty/Beneke et al.*, Max Planck Institute for Innovation & Competition Research Paper No. 19-13, S. 11 m. w. N.

¹⁵ Vgl. nur *Lemley/Caseys*, Fair Learning – Draft 23.3.2020, S. 42 ff. m. w. N.: „[...] *providing ML systems with broader access to data actually helps to mitigate some of the very negative outcomes that critics of ML systems fear*. [...]“; vgl. auch *Executive Office of the President*, Preparing for the future of Artificial Intelligence, S. 30: „AI needs good data. If the data is incomplete or biased, AI can exacerbate problems of bias.“

¹⁶ Vgl. zur Bedeutung der *Trainingsdaten* statt vieler *Drexl/Hilty/Beneke et al.*, Max Planck

seinstrumenten ist insoweit allerdings Differenzierung geboten: Zahlreiche Analyseinstrumente stehen inzwischen in der Cloud oder sogar allgemeinzugänglich im Internet wie eine Art „Toolbox“ zur Verfügung und werden auch entsprechend beworben und unter Open Source-Bedingungen angeboten.¹⁷ Dabei wird ihre Zurverfügungstellung seitens der Anbieter sogar häufig gleichsam als „Angel“ für die Gewinnung zusätzlicher Daten seitens der Nutzer dieser Analyseinstrumente eingesetzt. Lediglich die dahinterstehenden Kombinationen von Algorithmen und Gewichtungsfaktoren sowie der Sonderbereich besonders hochwertiger, innovativer und spezifischer Algorithmen oder Algorithmen, deren Aufdeckung zu Manipulationsmöglichkeiten im Markt führen würde, werden derzeit typischerweise geheim gehalten. Dennoch ist festzuhalten, dass gängige, auch ausreichende Analyseinstrumente für die Erkenntnisgewinnung im Rahmen von big data derzeit grundsätzlich in durchaus hinreichendem Maße in den Märkten zur Verfügung stehen.

Wesentlichstes Bottleneck ist damit nach dem heutigen Stand der Forschung zweifelsfrei der Zugang zu entsprechenden Rohdaten und für spezifische Modelle weiterentwickelten Trainingsdaten.¹⁸ Im Zusammenhang des Zugangs zu Daten spielt dabei auch die Qualität der Daten eine entscheidende Rolle (daher auch das Strukturmerkmal der *veracity* in der Beschreibung von big data Anwendungen).¹⁹ Werden Daten als Input genutzt bzw. als Bausteine für zur Verfügung stehende ML-Analyseverfahren eingesetzt, über deren Qualität Unsicherheit besteht, muss dies bei darauf basierender Entscheidungsfindung Berücksichtigung finden. Ansonsten besteht die Gefahr, dass die für sich genommen mathematisch

Institute for Innovation & Competition Research Paper No. 19-13, S. 1, 8: „*training data is the most valuable element of the machine learning process.*“; Fink, ZGE 2017, 288, 295 ff.

¹⁷ Vgl. etwa Datenstrategie, COM(2020) 66 final, 7f.; Drexl/Hilty/Beneke et al., Max Planck Institute for Innovation & Competition Research Paper No. 19-13, S. 1, 7; Stiemerling/Ehinger, CR 2018, 761 m. w. N.

¹⁸ Im Übrigen besteht gewisse Einigkeit, dass im Zusammenhang von big data und AI auch eine Verlagerung der Wertschöpfung auf einzelne Forscher und Ingenieure stattgefunden hat, so dass etwa auch der Aspekt der Arbeitnehmermobilität im AI-Bereich eine besonders wesentliche Rolle für die optimale Strukturierung der Innovationsprozesse spielt. Vgl. zu dem Einsatz heuristischer und erfahrungsbasierter Verfahren im Kontext des machine learnings und der Abhängigkeit vom Know-how der Mitarbeiter etwa Drexl/Hilty/Beneke et al., Max Planck Institute for Innovation & Competition Research Paper No. 19-13, S. 1, 6–7. Die vorliegende Studie greift dies etwa im Zusammenhang des Geschäftsgeheimnisschutzes am Rande auf, soweit es um die differenzierte Regelung des in diesem Zusammenhang besonders wesentlichen (und europaweit gleichermaßen von gewisser Rechtsunsicherheit charakterisierten) Bereichs nachvertraglicher Nutzung von Geschäftsgeheimnissen geht.

¹⁹ Vgl. dazu aus jüngerer Zeit etwa OECD, Enhancing Access to and Sharing of Data, S. 94 ff.; Tentative Draft No. 1 der ALI-ELI Principles for a Data Economy vom 22. Mai 2020, S. 126, online abrufbar unter: <https://www.ali.org/projects/show/data-economy/>.

richtigen Methoden der Algorithmen einer auf unsicherer Basis getroffenen, möglicherweise unzutreffenden Entscheidung bzw. Prognose den Anschein von Richtigkeit, Sicherheit bzw. hoher Wahrscheinlichkeit verleihen und diese dadurch unberechtigt legitimieren.²⁰ Aus fehlenden (standardisierten) Angaben zur Daten-/Analysequalität resultiert somit die Gefahr, dass Marktteilnehmer und Individuen unbemerkt zum Objekt nur vermeintlich verlässlicher big data-Analysen werden.²¹ Neben dem *Datenzugang* und dem Zugang zu AI-Ergebnissen als solchen ist daher *Transparenz* im Hinblick auf verwendete Input-Daten und Analysemethoden von wesentlicher Bedeutung.²² Die Bedeutung des Zugangs zu Daten mit entsprechender Qualität greift nunmehr zutreffend auch der Vorschlag der Kommission für einen Digital Markets Act auf, der in den vorgesehenen Regelungen zu Datenportabilität und Datenzugang explizit Bezug nimmt auf „effective, high quality, continuous and real-time access“ (s. Art. 6 Abs. 1 lit. i).²³

4. Angestammte und neuartige Geschäftsmodelle auf unterschiedlichen Marktebenen und mit marktübergreifender Relevanz

Der marktübergreifenden Vielfalt von Datenmengen und Datenverarbeitungsmethoden entspricht in der Datenökonomie eine entsprechende *Vielfalt erfolgversprechender Geschäftsmodelle auf ganz unterschiedlichen Marktebenen*, von denen nur wenige auf die Anreizwirkung eines bestehenden oder gar zusätzlichen rechtlichen Schutzes der immateriellen Basis angewiesen sind.

So hat sich im Rahmen der Datenökonomie ein weiter Bereich von *Infrastrukturdienstleistern in der Cloud* entwickelt, die für den Erfolg ihres Geschäftsmodells – der Zurverfügungstellung von Rechenkapazität und teilweise auch „Werkzeugkästen“ üblicher AI-Tools – keines zusätzlichen rechtlichen Schutzes bedürfen. Zusätzlicher Regelungsbedarf im Immaterialgüterrecht – sei es durch zusätzliche Anreize im Immaterialgüterrechtssystem oder (umgekehrt) Rückschnitt bestehenden immaterialgüterrechtlichen Schutzes – ist hier derzeit nicht erkennbar.

²⁰ In diese Richtung auch *Hoeren*, MMR 2016, 8, 11, der vor diesem Hintergrund eine Erneuerung der alten Datenqualitätsdiskussion im Lichte von big data fordert.

²¹ Zu den Risiken von big data vgl. allgemein *Mayer-Schönberger/Cukier*, Big Data, S. 189 ff. m. w. N.; eine weitere interessante Frage ist, ob und inwieweit der Mensch durch die Anwendung häufig nicht nachvollziehbarer selbstlernender KI-Algorithmen zum Objekt degradiert wird, vgl. *Martini*, JZ 2017, 1017 ff. m. w. N.

²² Vgl. allgemein zu dem Problem der mangelnden Offenlegung der Art und Weise, wie Daten gesammelt und verarbeitet werden (disclosure problem) *Mattioli*, BTJL 2017, 1 ff. m. w. N.

²³ Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final. S. näher unten S. 25 ff., 345 ff.

Wiederum andere Unternehmen setzen die ihnen zuwachsenden Datenmengen in erster Linie ein, um die *Qualität ihrer eigenen Produkte oder Dienstleistungen* zu erhöhen, ohne die entsprechenden potentiellen Erkenntnisgewinne auf breiter Front marktübergreifend zu nutzen. Insoweit wäre etwa Amazon als Beispiel zu nennen, das wegen der dokumentierten Verkaufsprozesse über vergleichsweise sehr hoch qualitative Daten verfügt, diese aber praktisch bisher weder in größerem Umfang zum Gegenstand eigenständiger Dienstleistungen noch zum Gegenstand neuartiger marktübergreifender Geschäftsmodelle macht. Stattdessen werden die Daten vorwiegend zur Verbesserung der eigenen, angestammten Geschäftsmodelle verwendet. Auch weite Bereiche der gezielten Maintenance und anderer effizienzsteigernder Anwendungen im internet of things (smart maintenance, smart farming etc.) gehören in diesen Kontext. Hier spielen faktische Datenkontrolle und flankierend auch Geschäftsgeheimnisschutz und teilweise das Schutzrecht sui generis für Datenbankhersteller eine signifikante Rolle. Entsprechend könnten für die Zukunft tatsächlich mehr oder weniger weitreichende *Reformen im Rechtssystem* mit dem Ziel, die Bereitschaft zur institutionell strukturierten *Offenlegung, Teilung und Übertragung* von Daten zu erhöhen, geboten sein. An dieser Stelle setzt auch die Diskussion um mögliche neue *sektorspezifische Zugangsregimes* an, in deren Rahmen sorgsam nach Rechtsverhältnissen und nutzungsbezogenen Fallgruppen zu differenzieren ist.

Massive Wertschöpfung auf der Grundlage von immensen Datenmengen (ohne erkennbaren Bedarf nach *zusätzlichem* immaterialgüterrechtlichen Schutz) findet auch heute schon im Rahmen der „*Aufmerksamkeitsökonomie*“ im *Internet*²⁴ statt, insbesondere soweit es um *gezieltes Marketing* auf der Grundlage von Suchmaschinen- oder sonstigen Plattformdaten sozialer Netzwerke und vergleichbarer Kommunikationsplattformen geht. An dieser Stelle drohen möglicherweise auch *neue datenbasierte, markttranszendierende Machtpositionen* einzelner Unternehmen, die nicht nur im eigentlich zugrundeliegenden Dienstleistungsmarkt bestehen. Vielmehr können sie wegen der faktischen Beherrschung des vorgelagerten Markts für Zugang zu den gesammelten Daten in marktübergreifender Form auch in vollkommen anders gelagerte oder gänzlich neuartige Innovationsmärkte vordringen.²⁵ Insoweit spielt allerdings wiederum auch die *Datenqualität* eine entscheidende mitigierende Rolle: Die immense Datenmenge entspricht in diesen Bereichen nicht selten einer hierzu umgekehrt proportional abnehmenden Datenqualität im Hinblick auf die eigentliche Funktion dieser Daten, soweit sie beispielsweise in unterschiedlichen Märkten für eine

²⁴ Zu dem Begriff der „Aufmerksamkeitsplattformen“ ausführlich *Stieper*, ZUM 2017, 132, 133 m. w. N. Vgl. in diesem Kontext etwa auch *Wu*, The Attention Merchants.

²⁵ Vgl. statt vieler *Schweitzer*; GRUR 2019, 569, 575 ff. m. w. N.

Sachregister

- Abgeleitete Daten
 - *siehe* inferred data
- Accountable AI 21, 154, 166, 313, 374
- AGB-Recht 258, **264–266**, **268 f.**, 292, **394 f.**, 403, 429
- Aggregated data 448–457
 - Datenzugang 448–457
- Alexa 262
- Algorithmen **6–9**, **11 f.**, **15 f.**, **19–21**, 29, 52, 72, 74, 116, 123, 129, 136, 141, 145, 151 f., 154 f., 157, 165 f., 173 f., 176, 178 f., 181 f., 184, 203, 300, 303, 314, 370–372, 376
 - Algorithmenqualität 178 f., 181 f.
 - Algorithmenregulierung 376 f., 379
 - Auskunftspflichten 300, 303, 370–372, 376
 - Black box 21, 129, 372 f.
 - Datenschutz 300, 303, 370–372
 - Digital Services Act 378
 - Geschäftsgeheimnisschutz 141, 145, **151–152**, 154 f., 157, 165 f., 173 f., 181 f., 184, **371 f.**
 - Involvierte Logik 370–372
 - Offenlegungspflichten 300, 303, 370–372
 - Patentrecht 136
 - Reverse engineering 59 f., 115, 152, **163–168**, 185, 224, 335, 416, 458
 - Right to reasonable inferences 393 f.
 - Risikobasierter Regulierungsansatz 377 f.
 - Transparenz 376, 378 f.
 - Urheberrecht 116, 123, 129
- ALI-ELI Principles for a Data Economy 90, 150, 159, 342, 422
- Allgemeines Persönlichkeitsrecht 198
- Anbieterwechsel 202, 204, 316 f., 319 f., 324, 326, 344, 398, 445 f., 457
- Angemessenheitsbeschluss 223, 231 f.
- Angemessene Geheimhaltungsmaßnahmen 139, 149–151, 153, 155, 304, 422
- Anonymisierung 214–225
 - Anonymously processed information 221 f.
 - Japan 221
 - Kritik 225 f.
 - Löschung durch Anonymisierung 214, 308 f.
 - Motivated intruder-Test 222
 - Probleme bei big data 216–218
 - Prüfpflichten 217
 - Re-Identifizierung 165 f., **216 f.**, **219 f.**, 223 f., 397, 402
 - Technische und organisatorische Maßnahmen 219
 - Rechtsunsicherheit 219
 - Reformvorschläge 225 f.
 - USA 220
 - Vorgaben der DSGVO 215 f.
 - Widerlegliche Vermutung 219–224, 402
 - Zwischenspeicherung zum Zwecke der Anonymisierung 225 f.
- API (application programming interface) **34**, 51, **116**, 202, 346, 348, 352
- Apps 202, 209, 264, 266, 270, 279
- Arbeitnehmererfindungsgesetz 118
- Arbeitnehmermobilität 171–173
- Art. 20-Datenschutzgruppe 216 f., 253, 257, 334, 355 f., 357, 365, 367, 371, 401
- Artificial Intelligence (AI) 11, 20, 43, 75, 123, 177, 193, 205, 233, 262, 271, 274, 282, 294, 310, **313–315**, 361, **364–380**, 394, 399, 442
- Auftragsverarbeiter 230, 234, 237, 239 f., 241, **245 f.**, 382
- Ausdrückliche Einwilligung **211–213**, 227, **237 f.**, 274, 292, 367, **369 f.**

- Ausführbare Offenbarung 129 f., 136
- Auskunftsrecht 296–307
- Abgrenzung zum Portabilitätsrecht 299
 - Automatisierte Entscheidungen 300 f.
 - Daten Dritter 304 f.
 - Datenverarbeitung zu Forschungszwecken 301
 - Einschränkungen 301–306
 - Format der Auskunft 299
 - Geistiges Eigentum 304
 - Geschäftsgeheimnisse **148 f.**, 302–305
 - Herausgabe von Dokumenten 298 f.
 - Interessenabwägung 301–306
 - Nicht identifizierbare Betroffene 305
 - Recht auf Kopie 296–299
 - Reichweite 296–301
 - Scoring 300 f.
 - Unzumutbarkeit 305 f.
- Ausschließlichkeitsrechte 197 f.
- Authentifizierung 330, **400**
- Automatisierte Einzelentscheidung 292, 300, 303, **364–379**
- *siehe näher* Verbot der automatisierten Einzelentscheidung
- Automatisiertes Fahren 206, 262 f., 273, 301
- *siehe auch* connected bzw. smart cars
- Begrenzte Drittwirkung 174–176, 420–426
- Berechtigter Nutzer 440–448
- Mindestrechte 440–448
- Berechtigtes Interesse des Verantwortlichen, Art. 6 Abs. 1 lit. f DSGVO **275–282**
- Abwägungsleitlinien 293, 403
 - Begriff des berechtigten Interesses 276 f.
 - Interessenabwägung im engeren Sinne 277–279
 - Struktur der Interessenabwägung 276 f.
 - Vernünftige Erwartung des Betroffenen 279 f., 293
 - Widerspruchsrecht des Betroffenen 279 f.
- Bereitgestellte Daten 318–320, 345
- Berichtigung 315
- Besondere Arten personenbezogener Daten **209–214**, 278, 311
- Begriff 210 f.
 - Einwilligung 211–213
 - „Hervorgehen“ 210
 - Öffentlich zugänglich gemachte Daten 213 f.
 - Verarbeitungsverbot 210 f.
- Best practices 115, 187, 199, 219, 343, 350, 361, 395, 398, 401, 413 f., 420
- Betroffenenleitbild 281, 293
- Betroffenenrechte (DSGVO) **294–351**, 416
- Allgemeine Vorgaben 295
 - Auskunftsrecht 296–306
 - Betroffenenleitbild 281, 293
 - Portabilitätsrecht 315–351
 - Recht auf Berichtigung 315
 - Recht auf Löschung/Vergessenwerden 214, 228, 296, **307–315**
 - Technische Umsetzung 352
 - Verhältnis zum Vertragsrecht 353
 - Verhältnismäßigkeitssatz 295
- Betroffener 239
- Vernünftige Erwartung des Betroffenen 279 f., 293
- Biases 7, 204, 250, 313, 373, 377, 444 f.
- Big data with privacy 192, 358–362
- Biometrische Daten 209 f.
- Binding Corporate Rules 235
- Blockchain 86, 108, 153, 155, 207, 244, 251, 309, 330, 361, 365 f., 369, 380
- Bußgelder (DSGVO) 383 f.
- BVerfG
- Kennzeichenerfassung 225
 - Recht auf Vergessenwerden 312 f.
 - Stadionverbot 375
 - Volkszählungsurteil 11, 45, 145, 288
- California Consumer Privacy Act 228
- Cloud 5, 8, 9, 77, 147, 171, 200, 228, **230**, **234 f.**, 246, 251, 290, 330, 350, 357, 400
- Codes of Conduct 209, 219, 223, 226, 235, 280, 293 f., 350, 361, 396
- Grenzüberschreitender Datenverkehr 235
- Computerprogrammenschutz 115–121
- Dekompilierung 119 f.
 - Schnittstellen 116 f.
 - Schranken 119 f.
 - Schutzvoraussetzungen 115–118
 - Tinkering 120, 458
 - Umarbeitung 119
 - Urheberpersönlichkeitsrecht 118 f.

- Computerprogramme 411, 417, 419, 440 f., 442, 446
- Computerprogramm-RL 416, 440.
- Connected cars 86, 156, 206 f.
- Connected devices 156, 437, 446 f.
- Consent fatigue 238, 250, 274, 292
- Content moderation 28 f, 378, 392
- Cookies 238, 263
- Data Act 2021 25, 345, 421
- Data Governance Act 25, 29, **331**, **349**, 398, 401, 405, 421, **436**
- Data Sharing 221, 322, 342, 344, 413
- Daten
- Bereitgestellte Daten 318–320, 345
 - Besondere Arten personenbezogener Daten **209–214**, 278, 311
 - Bewegungsdaten 211, 217
 - Biometrische Daten 209 f.
 - Datenbiotope 17, 32, 186, 410, 420
 - Datenminimierung 225, **282 f.**, 289, 305, 324, 359, 363, 388, 406
 - Datentransfer in Drittstaaten *siehe dort*
 - Fahrzeugdaten 207
 - Gegenleistung 203, 253 f., 256, 258 f., 268 f., 271, 330, 382
 - Gesundheitsdaten 209 f., 212 f., 294, 331 f.
 - Kommerzialisierung von Daten **24**, 198, 250, 267, 275, 391, 397, 403 f., **420–422**
 - Metadaten 15, 18 f., 47, 53, **74 f.**, 143, 145 f., 151, 169, 290, 320, 335, 453, 457
 - Nicht-personenbezogene Daten 196
 - Observed data 18, **68–72**, 410, 439, 442, 450
 - Öffentlich zugänglich gemachte Daten 213 f.
 - Personenbezogene Daten 194 f., **205–209** (*siehe näher dort*)
 - Portabilität 9, 16 f., 24, **35–37**, **58–60**, 80, 116 f., 127, 130, 167 f., 192, 202, 204, **315–353**, 363, **385**, 398, **404 f.**, 407, 426, 428, 434, 436 f., 440, **442 f.**, **445 f.**, 447, **457–459**
 - Pseudonymisierte Daten 18, 202, **208 f.**, 283, 289, 293, 359 f.
 - Reputationsdaten 319, 347
 - Sensible Daten 209 f., 211 f., 214, 237, 292, 294, 331 f., 401, 403, 406
 - Trainingsdaten **7 f.**, 20 f., 31, 43, 75, 82, 103, 113, 127, **129 f.**, 136, **147**, **151**, 217, 271, 274, **313 f.**, 410
 - Verschlüsselung 125, **131 f.**, 136, 208 f., 359 f., 361
 - Volunteered data 18, **68**, 81, 410
 - Wert **142 f.**, **144 f.**, 273, 382
 - Zugangsrechte 25, **35–37**, 133, 344, 346, 348, **428–457**
- Datenaltruismus 192, 331
- Datenanalyse 19–21
- Analyseergebnisse 21 f.
- Datenbank 42 f.
- Datenbank-RL **41 f.**, 46, 69, 76 f., 93 f., 97, 112, 440, 451 f.
- Reformbedarf **95 f.**, 446–448
 - Zwangslizenz 451–453
- Datenbankschutz
- Schranke für öffentliche Datenbanken 416
 - Spin off-Datenbanken **78 f.**, 438
- Datenbankschutzrecht sui generis **62 f.**, 74 f., 91 f., 98 f., 101, 112 f., 115, 337, 410, 419, 438, 451–453, 455
- Amtlich erstellte Datenbanken 93 f.
 - Beschaffen von Daten 64–75
 - BHB v. Hill 64–71
 - Datenbankhersteller 85–88
 - Dauernd aktualisierte Datenbanken 98
 - Entnahme 82
 - Inhaberschaft 85–88
 - Neuinvestition 96–98
 - Public sector information 93–95, 416
 - Rechtmäßiger Benutzer 93
 - Reformbedarf **95 f.**, 446–448
 - Schranken 91–96
 - Schutzdauer 96–100
 - Spin off-Theorie **78–80**, 438
 - Tagging 98 f.
 - Teiländerung 98 f.
 - Umwandlung in Registerrecht 100–110, 418 f.
 - Value-added Datenbank 83, 114
 - Verhältnis zum Lauterkeitsrecht 110–112
 - Weiterverwendung 82
 - Wesentliche Investition 62–82
 - Wesentlicher Teil 84 f.

- Datenbankwerke 46–62
 - Bearbeitung 54 f.
 - Datenbankstruktur 52–59
 - Eigene geistige Schöpfung 46–59
 - Reverse engineering 59 f.
 - Schutzdauer 60
 - Schutzzumfang 52 f.
 - Schutzvoraussetzungen 46–52
 - Technisch notwendige Vervielfältigung 53 f.
 - Urheberpersönlichkeitsrechte 55 f.
- Datenbeherrschung 113, 200
- Datenbeschaffung 17–19
- Dateneigentum 22–24
- Datenethikkommission 290, 377–379, 422
- Datenformate 34, 127, 130–132, 202, 320, 323, 329, 340, 348, 400, 404
 - Patentrecht 130–132
- Datenimport 324, 327, 348, 351, 400, 457
- Datenintermediäre 261, 267, 274, **326, 333, 349 f.**, 351 f., 353, **398–401**, 421, 457 f.
 - Data Governance Act 349, 398
- Datenlizenzen 397–401, 412 f.
- Datenmacht 26, 73, 200, 322, 349, 378, **386–388**, 434, 445, 448
- Datenmärkte 196, 198
- Datenmenge 5 f., **9–15**, 106, 108, 171, 183, 193, 199 f., 201 f., 204 f., 282, 301, 304, 308, 323, 347, 395
- Datenminimierung 225, **282 f.**, 289, 305, 324, 359, 363, 388, 406
- Datennutzungsrechte 13, 36 f., 41, 134, 152, 416, 430, 435 f., **440–457**
- Datenpools 87, 147, 412 f., 420 f., 423–425
- Datenportabilität 9, 16, **35–37**, 58 f., 80, 116 f., 127, 130, 167 f., **342–347, 428–459**
 - B2B 35 f., 344 f., 348, 412, **435–438**, 445, 457–459
 - Digital Markets Act 344, 346 f., 352
- Datenportabilität, Art. 16 Abs. 4 Digitale Inhalte-RL **339–342**, 440
- Datenportabilität, Art. 20 DSGVO **315–353**, 440
 - Anbieterwechsel 316 f., 319 f., 324, 326, 344
 - Automatisierte Lösungen 347, 351 f.
 - Betroffene Datenverarbeitungsvorgänge 315 f.
 - Berechtigtes Interesse 316
 - Bereitgestellte Daten 318–320, 345
 - Betroffene Datenkategorien 318–320, 345, 457 f.
 - Daten Dritter 333 f.
 - Datenbankschutz 337
 - Datenformat 320 f.
 - Datenintermediäre 261, 267, 274, **326, 333, 349 f.**, 351 f., 353, **398–401**, 421, 457 f.
 - Datentreuhänder 261, 267, 274, **320, 331 f., 333**, 349, 400, 421
 - Datenverwertungsgesellschaften 332
 - Digitale Inhalte-RL 339–342
 - Einschränkungen 333–339
 - Format 320 f.
 - Geistiges Eigentum 336–338
 - Gerätebasierte Datenverwaltung 332 f.
 - Geschäftsgeheimnisse 335 f.
 - Import 324, 327, 348, 351, 400, 457
 - Inferred data 318, 335 f., 345–347
 - Interoperabilität 348
 - Lauterkeitsrechtliche Durchsetzung 325 f.
 - Marktverhaltensregel 325, 384, 426 f.
 - Metadaten 320
 - Nicht identifizierbare Betroffene 339
 - Nutzungszweck 338
 - Öffentliche Stellen 316
 - Personal Information Management Systeme 213, 261, 267, 274, 292, **327–330**, 349, **397–401**, 404, 421
 - Präferenzen 319
 - Praktische Umsetzung **324–333**, 443, 457–459
 - Real time data **319 f., 345–347**, 404, 457 f.
 - Reformbedarf 320, 351–353
 - Reputationsdaten 319, 347
 - Schnittstellen 322 f.
 - Single sign on-Dienste 330 f.
 - Sinn und Zweck 316–318
 - Technische Umsetzung 322–324
 - Übermittlung an andere Anbieter 321 f.
 - Übertragbarkeit 326 f., 349
 - Technische Machbarkeit 321 f.
 - Tools 327, 347, 351
 - User centric approach 327–330
 - User generated content 337

- Verallgemeinerungsfähigkeit 342–347
- Verhältnis zur Löschung 317 f.
- Wahrnehmungsbefugnis 326 f., 349
- Zugriffstools 322
- Datenqualität 7–9, 32, 193, 201, 315, 373, 453
- Datenquellen 6, 17, 83, 87, 146, 166, 199 f., 205, 211, 213, 217, 344, 371, 398 f., 411
- Datenräume, persönliche 192, 398
- Datenschutzausschuss, Europäischer (EDSA) 253, 257, 264, 268, 359, 401
- Datenschutzbehörden 221, 224, 233 f., 235, 276, 292, 294, 298, 324, 354, 356, 358, 364, **380 f.**
- Datenschutzfolgenabschätzung 354–358
 - Bewertungskriterien 355 f.
 - Dezentralisierte Datenverarbeitung 357 f.
 - Erforderlichkeit 354
 - Leitlinien der Datenschutzbehörden 356 f.
 - Referenz-Folgenabschätzung 357 f.
- Datenschutzgrundverordnung **191–407**
 - Bußgelder 383 f.
 - Cloud 200, 228, **230, 234 f.**, 246, 251, 290, 330, 350, 357, 400
 - Datenschutzgrundsätze 193, 217, 231, 282 f., 358, 363
 - Durchsetzung 379–389
 - Evaluation 191, 234
 - Informationspflichten 217, 238, 243, 248, 251, 260, **261**, 270, 276, 282, 287, 295, 297, 302, 341, 370, 372, **380**, 456
 - Interessenabwägung 194 f., 200 f., **210**, 224, 239, 247, 259, **275–282**, 285 f., **291 f.**, **293, 301–307, 310 f.**, **313**, 316, 319, **333–339**, 341, 351 f., 353, 356, 358, 363 f., 397, **402 f.**, 405 f., 416
 - Künstliche Intelligenz 313–315, 364–380
 - Multipolare Datenverarbeitung 200
 - Privatrechtliche Durchsetzung 384–389
 - Regelungsziele 194–199
 - Risikobasierter Ansatz 353–364
 - Sanktionen 383 f.
 - Schadensersatz 381–383
 - Selbstregulierung 219, 226, 233, 236, 344, **395–397**, 401
 - Territorialer Anwendungsbereich 227–230
 - Verhältnis zum Kartellrecht 386–389
- Verhältnis zum Lauterkeitsrecht 384–386
- Datenschutzgrundsätze 193, 217, 231, **282 f.**, 358, 363
- Datenminimierung 225, **282 f.**, 289, 305, 324, 359, 363, 388, 406
- Zweckbindung **282–287**, 331, 388, 405
- Datenschutzrecht
 - Ausschließlichkeitsrecht 197 f.
 - Blockchain 207, 244, 251, 309, 330, 361, 365 f., 369, 380
 - Grundrechte **194 f.**, 198, 201, 205, 229 f., 258, 260, 276 f., 278, 295 f., 303, 306, 312 f., 341, 351, 366, 368, 375, 399
 - Interessenlage bei big data 197–205
 - Medizin **212 f.**, 263, 274, 331, 370, 398, 403
 - Technische und organisatorische Maßnahmen 219, 283, 289, 358, **362 f.**, 364, 397
 - Verhältnis zum Verbraucherrecht 258, 268, 394, 406
 - Verhältnis zum Vertragsrecht 199, 220 f., 224, 250, **253–256**, 258, **265 f.**, **268**, **271–372**, 275, 279, 281, **292**, 294, 333, **353, 394–401, 402–407**
 - Verhältnis zum UWG 273, 279, 281, 293, 325, 341, **384–386**, 396, 426
- Datenschutz-Richtlinie 194, 206, 216, 240, 242, 276, 297, 298
- Datenstrategie (EU-Kommission) **25**, 114, 138, **192, 344 f.**, 388, 398
- Datentransfer in Drittstaaten **230–239**, 278
 - Angemessenheitsbeschluss 231 f.
 - Ausdrückliche Einwilligung 237 f.
 - Ausnahmetatbestände, Art. 49 DSGVO 237–239
 - Berechtigtes Interesse 239
 - Brexit 232
 - Binding Corporate Rules 235
 - Codes of Conduct 235
 - Forschungszwecke 239
 - Privacy shield 232
 - Rechtmäßigkeitsvoraussetzungen 230 f.
 - Sichere Drittstaaten 231
 - Standardvertragsklauseln 233–235
 - Statistikzwecke 239
 - USA 231 f.
 - Vertragserfüllung 238 f.

- Voraussetzungen 230–239
- Zertifizierung 236
- Datentreuhänder 261, 267, 274, **320, 331 f., 333**, 349, 400, 421
- Datenvalidierung 17, 19, 86
- Datenverarbeitung
 - Arbeitsteilige Datenverarbeitung 211, 237, 240, 244, 250 f., 270, 308, 402
 - Berechtigtes Interesse des Verantwortlichen 275–282
 - Erforderlichkeit zur Vertragserfüllung 264–367, 292
 - Forschungszwecke 210, **212 f.**, 239, 263, 274, 278, **287–291**, 294, **301**, 307, 310, 331, 362, 370, 398, 403, 405 f., 436
 - Multipolare Strukturen 195, 200, 218, 240, **250 f.**, **262**, 308, 357, 383, 402, **412–414**
 - Phasen 14–22
 - Rechtmäßigkeit 247–291
 - Statistikzwecke 239, 285, **287–291**, 294, **301**, 397, 310, 314, 404 f., 436
 - Verarbeitungsgrundlage 247 f.
 - Verarbeitungszweck 290
 - Zweckänderung **282–291**, 362, 402, **405**
- Datenverkehr, freier 193, 194
- Datenverwertungsgesellschaften 332
- Datenzugang 25, **35–37**, 133, 344, 346, 348, **428–457**
 - *siehe auch* Zugangsrechte
- De facto-Standard 66 f., 433, 450
- Deep learning 21, 166, 301, 313
- Dekompilierung 119 f., 186
- Derivative Daten 72
 - *siehe auch* inferred data
- Dienste gegen Daten **253–260**, 272, 274, 292, 330, 403
 - datenschutzrechtliche Einwilligung 253–258
- Differential privacy 360, 364, 406
- Digital Content Directive 35, 197, **253–264**, 271, 323, **339–342**, 390, 405, 440, 445, 448
- Digital Markets Act 9, **25–27, 34–36, 344–347**, 348, 352 f., 385, 388, 405, 421, 427 f., **434**, 437, 445, **458**
 - Portabilität 36, 344, 346 f.
 - Privatrechtliche Durchsetzung 427
 - Verhältnis zum Kartellrecht 434
 - Verhältnis zum Geheimnisschutz 34, 346, 434
 - Verhältnis zum geistigen Eigentum 34, 346, 434
- Digital Services Act **25, 28 f.**, 30, **378**, 392, 405, 421, 427
 - Algorithmtransparenz 378
 - Privatrechtliche Durchsetzung 427
- Digital Single Market-RL (DSM-RL) 42, 55, 92, 95, 121–126, 416
- Digitale Inhalte-RL 35, 197, **253–264**, 271, 323, **339–342**, 390, 405, 440, 445, 448
- Diskriminierung 2, 195, 313, **375**, 367, **393**, 446, 454
- Distributed ledger-Technologie 108, 153, 155, 207, 244, 330
- Drei-Stufen-Test 124, 415
- Drittwirkung 164–176, 184 f., 420–426, 459
 - Begrenzte Drittwirkung 164–176, 420–426
 - Qualifizierte Drittwirkung 184 f., 422–426
- DSGVO **191–407**
 - *siehe auch* Datenschutzgrundverordnung
- Dynamische Einwilligung (dynamic consent) 213, 398
- Eigene geistige Schöpfung 46–59
- Eigentumsgarantie 277
- Einwilligung, datenschutzrechtliche 199, **248–275, 291–294, 397–401, 403, 420 f.**
 - Abgrenzung zur Datenverarbeitung gem. Art. 6 Abs. 1 lit. b DSGVO 264–267, 268
 - Abstraktionsprinzip 255, 273
 - AGB-Kontrolle 268 f.
 - Aktive Handlung 263
 - Ausdrückliche Einwilligung **211–213**, 227, **237 f.**, 274, 292, 367, **369 f.**
 - Bedeutung 248–250
 - Besondere Arten personenbezogener Daten **211–213**
 - Bestimmtheit 260 f.
 - Blanko-Einwilligung 213
 - Consent fatigue 238, 250, 274, 292
 - Dynamische Einwilligung (dynamic consent) 213, 398
 - Einwilligungsmanagement 327–330

- Freiwilligkeit 252–260, 268
- Gesamteinwilligung 251
- Informierte Einwilligung 261–263
- Konkludente Einwilligung 211, 263 f.
- Kopplungsverbot 252, 256 f., 268, 292
- Medizinischer Bereich 212 f.
- Meta-Einwilligung (meta consent) 213, 398
- Multipolare Strukturen 250–252
- Online-Bereich 237 f.
- Privacy icons 262, 267, 274, 292
- Rahmeneinwilligung 252, 261, 274
- Reformbedarf 273–275
- Smart devices 262
- Smart disclosure systems 262
- Transparenz 257, 268
- Unmissverständlichkeit 263 f.
- Widerruf 269–273, 274
- Wirksamkeitsvoraussetzungen 252–268
- Zweckänderung 285
- ePrivacy-RL 263, 273, **389 f.**
- ePrivacy-VO 273, **389 f.**
- Erforderlichkeit der Datenverarbeitung zur Vertragserfüllung 264–267, 292
- Erga omnes-Schutz 423
- Erschöpfung 441
- Essential facility 452 f.
- EuGH
 - Bedeutung für die Auslegung der DSGVO 401
 - BHB/Hill **56 f., 64–71, 80 f.**, 438 f., 450
 - Bronner 66, 452
 - Google Spain 227 f., 311 f.
 - Google/CNIL 229
 - IMS Health 57, 433, 449 f.
 - Magill 432, 449
 - Marketing Fixtures 438
 - Pelham 55, 119
 - Schrems II 232–234
 - Tom Kabinet 441
 - UsedSoft 441, 443
- EUIPO 104, 454
- Europäischer Datenschutzausschuss (EDSA) 253, 257, 264, 268, 359, 401
- Facebook 240 f., 327 f. 386–388
 - Beschluss des BKartA 386–388
 - Off Facebook-Daten 386–388
- Federal Trade Commission (FTC) 220 f.
- Forschungszwecke 210, **212 f.**, 239, 263, 274, 278, **287–291, 294, 301**, 307, 310, 331, 362, 370, 398, 403, 405 f., 436
 - Datentreuhand 331
 - Einwilligung 212 f.
 - Zweckänderung 287–290
- FRAND 128, **132–135**, 353, 424, **453 f.**, 455, 459
 - Patente 33, 37, **132–135**, 352, 450
 - Rücksichtnahmepflicht 134 f., 425
 - Selbstverpflichtung 33, **132–136**, 348, 405, 424 f., 459
 - Vergütung 453 f.
 - Zweiterwerber 134 f., 424, 459
- Free riding 336
- Freier Datenverkehr 193, 196, 201, 342
 - Verordnung für den freien Verkehr nicht-personenbezogener Daten 106 f., 196 f., 342, 344
- Freiwilligkeit der Einwilligung 252–260, 268
 - Äquivalenter Dienst 253
 - Bewertung in den Mitgliedstaaten 252 f.
 - Dienste gegen Daten 253–260
 - Kriterien 257
 - Transparenz 257 f.
- Free flow of data 193, 196, 201, 342
 - Free flow of non-personal data-Verordnung 106 f., 196 f., 342, 344
- G2B-Bereich 35, 113, 415, 436
- Gatekeeper **25–27, 34–36, 344–346**, 347, 352 f., 388, 428, 434, 437, 445, 458
- Gegenlizenzen 132, 134, 454 f.
- Geheimhaltungsmaßnahmen **149–151**, 155, 303, 422
- Gemeinsame Verantwortlichkeit 233, **240–247**, 357, **380**, 395
 - Abgrenzung zur Auftragsverarbeitung 245
 - Blockchain 244
 - Haftung 241, 380 f.
 - Online-Bereich 244
 - Verantwortungsbereiche 243–245
 - Vereinbarung 243 f.
 - Voraussetzungen 242 f.
- Gemeinwohlinteresse 204, 212, 278, 331

- Gerätebasierte Datenverwaltung 332 f.
- Geschäftsgeheimnis, 13, 120, **137–189**, 303, 310, 323, 335, 410, 412, 421 f., 424 f., 431 f., 451, 455–457
- Angemessene Geheimhaltungsmaßnahmen 139, 149–151, 153, 155, 304
 - Begrenzte Drittwirkung 164–176, 420–426
 - Big data 141–155
 - Definition 138–141
 - Freie Meinungsäußerung 177 f.
 - Geheimer Charakter 139, 146, 148, 154
 - Geheimhaltungsvereinbarung 160, 170, 176
 - Geheimnisschutzregister 159
 - Informationsfreiheit 177 f.
 - Inhaberschaft 156–163
 - Kommerzieller Wert 144 f., 153
 - Legitime Interessen 181 f.
 - Rechtmäßiger Erwerb 163–168
 - Rechtsdurchsetzung 182–184
 - Rechtsverletzende Produkte 176 f.
 - Rechtswidrige Nutzung/Offenlegung 170–174
 - Rechtswidriger Erwerb 169 f.
 - Reverse Engineering 152, **163–168**, 185
 - Registrierung 419
 - Whistleblowing-Ausnahme 178–181
- Geschäftsgeheimnisgesetz (GeschGehG) 22, **138 f.**, 144, 149, 151 f., 154 f., 156, 164, 171, 176, 178, **183**, 185, 421
- Gesundheitsdaten 209 f., 213, 294, 331 f.
- Gezielte Behinderung 385, 427 f.
- Grenzüberschreitender Datenverkehr 227–239
- *siehe auch* Datentransfer in Drittstaaten
- Grundrechte **28 f.**, 61, 126, 178, 181, **194 f.**, 198, 201, 205, 229 f., 258, 260, 276 f., 278, 295 f., 303, 306, 312 f., 341, 351, 366, 368, 375, 399
- Grundrechte-Charta 28, 181, 194
- GWB 13, **27**, 30, 386, **433 f.**, 452
- GWB-Modernisierungsgesetz 13, **27**, 30, **433 f.**, 452
- GWB-Novelle, zehnte 13, **27**, 30, **433 f.**, 452
- Hashwert **106 f.**, 108 f., **159–162**
- Hebelwirkung 35, 231, 410, 444
- Hold up 37, 55 f., 88, 113, 116, 415, 417
- Homomorphe Verschlüsselung 361, 406
- Human Review 365 f., 373 f., 377
- In camera-Verfahren 424
- Individual level use data 436, 440–448
- Industrie 4.0 86, 141, 192, 206
- Inferred data 21, **72–74**, 82, 113, 151, 318, 335 f., **345–347**, 404 f., 410, 450, 457
- Portabilität 318, 335 f., 345–347
- Informationelle Selbstbestimmung 225
- Informationsfreiheit 2, 28, **177 f.**, 195, 205, 229, 311 f., 368, 375
- Innovationsförderung 1, **27 f.**, 119, 140, 148 f., 174, 201, 204, 290, 422
- Interoperabilität 25, 33 f., 50 f., **57–60**, 115, **117**, 119, **167 f.**, 323, 344, **348**, **350 f.**, **352**, 395, 400, **404**, **407**, **414–416**, **457–459**
- Interessenabwägung 56, 61, 111, 118, 177, 194 f., 200 f., **210**, 224, 239, 247, 259, **275–282**, 285 f., **291 f.**, **293**, **301–307**, **310 f.**, **313**, 316, 319, **333–339**, 341, 351 f., 353, 356, 358, 363 f., 397, **402 f.**, 405 f., 416, 427, 430, 448
- *siehe auch* Berechtigtes Interesse des Verantwortlichen
 - Datenschutzrecht 194 f., 200 f., **210**, 224, 239, 247, 259, **275–282**, 285 f., **291 f.**, **293**, **301–307**, **310 f.**, **313**, 316, 319, **333–339**, 341, 351 f., 353, 356, 358, 363 f., 397, **402 f.**, 405 f., 416
 - Geschäftsgeheimnisschutz 177 f.
- Investitionsschutz 86, 111, 337, 417 f., 451–453
- IP-Adresse 206, 305
- Irreführungsschutz 396
- IT-Sicherheit 150 f., 179, 181, 222, 348, 356, **362 f.**, 364, 400
- Grundsätze 362 f.
- Joint Controllership 240–247
- *siehe auch* gemeinsame Verantwortlichkeit
- Kartellrecht 386–388, 429–435
- GWB-Novelle 13, **27**, 30, **433 f.**, 452
 - Kartellrechtliche Zugangsansprüche 432–435

- Verhältnis zur DSGVO 386–388
- KMU 103, 363, 405, 413
- Kommerzialisierung von Daten **24**, 198, 250, 267, 275, 391, 397, 403 f., **420–422**
- Kommerzialisierung von personenbezogenen Daten 198, 250, 267, 275, 391, 397, 403 f., **420–422**
- Kompatibilitätstest 285–287, 405
- Kopplungsverbot 252, 256 f., 268, 292
- Korpora 20, 43, 73, 75, 124, 126, 147
- Kreuzlizenzen 103, 435, 454 f.
- Kryptographischer Fingerabdruck **106 f.**, 108 f., **159–162**
- KUG 334
- Künstliche Intelligenz 11, 20, 43, 75, 123, 177, 193, 205, 233, 262, 271, 274, 282, 294, 310, **313–315**, 361, **364–380**, 394, 399, 442
 - Accountable AI 21, 154, 166, 313, 374
 - Datenschutzrechtliche Löschpflichten 313–315
 - Verbot der automatisierten Einzelentscheidung 364–380
- Lauterkeitsrecht 110–112, **325 f.**, **384–386**, **426 f.**
 - *siehe auch* UWG
- Lernen
 - Deep learning 21, 166, 301, 313
 - Maschinelles Lernen 199
- Leveraging 37, 231, 410, 444
- Liability rule 103, 418, 448
- Lizenzierung
 - Datenbankschutz 71 f., 76, 91, 94, 108
 - Datenlizenzen 397–401, 412 f.
 - Fiktive Lizenzgebühr 382
 - FRAND 128, **132–135**, 424, **453 f.**, 455, 459
 - Geschäftsgeheimnisschutz 73, 103, 106, 187
 - Gegenlizenzen 132, 134, 454 f.
 - Kreuzlizenzen 103, 435, 454 f.
 - Open Data-RL 95
 - Patentrecht 127 f., 132
 - Reziprozität 454 f.
 - Zwangslizenzen, *siehe dort*
- Lizenzgebühr 133, 382
- Lizenzmarkt 36, **433**, 438, 448
 - Lizenzvereinbarung 432
 - Lizenzverweigerung 30, 432
 - Lock in 35, 56, 80, 202, 316, 318–320, 322, 324 f., 339, 342, 347, 387, 404, 426, 436, 444, 446, 457
 - Löschpflichten 307 f.
 - Einschränkungen 310 f.
 - Löschkonzept 308
 - Speicherbegrenzung 307
 - Löschungsrecht 214, **307–315**
 - *siehe auch* Recht auf Löschung
- Machine Learning 5, 7, 15, 20 f., 105, 147, 199, 290, 301, 361, 406
 - Privacy preserving machine learning 361
- Marktbeherrschung 27, 30, 72, 152, 323, 343, 386–388, 432 f.
- Marktortprinzip 227
- Marktverhaltensregel 184, **325**, **426 f.**
- Marktversagen 14, 19, 24, 30 f., 35, 63, 101, 396, **412**, 436, **438 f.**, 444, 447
- Marktzutritt 33, 35, 66, 68, 114, 181, 198, 202, 267, 317, **344**, **346**, 390, 396, **452 f.**
- Maschinelles Lernen 5, 7, 15, 20 f., 105, 147, 199, 290, 301, 361, 406
 - Privacy preserving machine learning 361
- Meinungsäußerung, freie 177 f., 311 f., 375
- Meinungsfreiheit 28, 177 f., 205, 311 f., 375
- Menschliches Eingreifen 365 f., 373 f., 377
- Metadaten 15, 18 f., 47, 53, **74 f.**, 143, 145 f., 151, 169, 290, 320, 335, 453, 457
 - Portabilität 320
- Meta-Einwilligung (meta consent) 213, 398
- Microsoft-Entscheidung 433
- Mindestrechte des berechtigten Nutzers 440–448
- Montreal Data License 399
- Multiple Rechteinhaberschaft 412–414
- Multipolare Datenverarbeitung 119, 186, 195, 200, 218, 240, **250 f.**, **262**, 308, 357, 383, 402, **412–414**
 - Arbeitsteilige Datenverarbeitung 211, 237, 240, 244, 250 f., 270, 308, 402
 - Datenschutzrechtliche Einwilligung 250 f., 262
 - Datenschutzrechtliche Verantwortlichkeit 357, 383
- MyData 327–330

- Nebenpflicht, vertragliche 135, 424 f., 442
- Neuronale Netze 7, 141, **153**, 155, 157, 165, 173, 176, 184, 199, 217, 301, 313, 374
- Netzwerke, soziale 10, 202, 211, 214, 251, 305, 316, 326, 333 f., 337, 368, 386–388
- Netzwerkeffekte 67, 293
- Niederlassungsprinzip 227
- NoSQL 43 f., 53, 59
- Nudging 392
- Nutzerprofile 281, 288, 318, 335
- *siehe auch* Profiling
- Nutzerverhalten 391, 405
- Nutzungsrechte 13, 36 f., 41, 134, 152, 416, 430, **440–448**, **448–457**
- Observed data 18, **68–72**, 410, 439, 442, 450
- Öffentlich zugänglich gemachte Daten 213 f.
- Open access 89, 101, **400**
- Open data 149, 322
- Open Data-RL **95 f.**, 416, 436
- Open Source 8, **34**, 118, 328, 330
- Opt out 123, 203, 228, **392 f.**
- Overlaps 110, 114, 118, **414–417**
- P2B-Verordnung 378, 392, 395, 444 f.
- Parteiautonomie 157
- Patente
- Patentpools 413
- Standardessentielle Patente 33, 128, **132–135**, 352, **449**, **453 f.**, 459
- Patentrecht 127–137
- Ausführbare Offenbarung 129 f., 136
- Computerprogrammbezogene Erfindungen 128
- Datensequenzen 130 f.
- Schutz von Verfahrensprodukten **131 f.**, 136, 323, 410, 449
- Patientenakte 213, 298
- Personal Information Management Systeme 213, 261, 267, 274, 292, **327–330**, 349, **397–401**, 404, 421
- Personalisierung
- Personalisierte Dienste/Services 262, **266**, 268, 271, 319
- Personalisierte Medizin 368
- Personalisierte Nachrichten 368
- Personalisierte Preise 367, 379, 392
- Personalisierte Werbung 201, 215, 331, 365, 367, 389
- Personalized Law 368
- Personally identifiable information 220
- Personenbezogene Daten 194 f., **205–209**
- besondere Arten personenbezogener Daten **209–214**
- Blockchain 207
- Connected cars 206 f.
- Pseudonymisierung 18, 202, **208 f.**, 283, 289, 293, 359 f.
- Re-Identifizierung **216 f.**, **219 f.**, 223 f., 397, 402
- Verschlüsselung 125, **131 f.**, 136, 208 f., 359 f., 361
- Persönliche Datenräume 192, 398
- Petty Patents 103, 418
- Plattformen 10, **25–27**, **28 f.**, **34–36**, 125, 145, 266, 279, 319, 326 f., 328, 333, 336 f., 344–346, 347, 352 f., **378**, **388**, 400, 427, 434, 437, 445, 458
- Plug-ins 240 f., 273
- Portabilität 9, 16 f., 24, **35–37**, **58–60**, 80, 116 f., 127, 130, 167 f., 192, 202, 204, **315–353**, 363, **385**, 398, **404 f.**, 407, 426, 428, 434, 436 f., 440, **443 f.**, **445 f.**, 447, **457–459**
- *siehe auch* Datenportabilität
- Portabilitätsrecht, Art. 20 DSGVO 192, **315–353**
- *siehe näher* Datenportabilität
- Portabilitätsrecht, Art. 16 Abs. 4 Digitale Inhalte-RL 339–342
- Portabilitätsrechte, sonstige 440
- individual level use data 436, 440–448
- Praktische Konkordanz 194
- Pre-emption-Doktrin 112, 414
- Predictive Policing 368
- Preisdiskriminierung 393, 446
- Privacy
- Differential privacy 360, 364, 406
- ePrivacy-RL 263, 273, **389 f.**
- ePrivacy-VO 273, **389 f.**
- Privacy by default 205, 353, **358–362**, 364
- Privacy by design 205, 283, 293, 304, 348, 352, **358–362**, 364
- Privacy enhancing technologies/tools 360, 364, 397, 406
- Privacy icons 262, 267, 274, 292

- Privacy paradox 203, 274
 Privacy preserving machine learning 361
 Privacy shield 231 f., 236
 Privatautonomie 13, 24, **26 f.**, 88, **125 f.**,
157 f., 166, 201, 249 f., 260, 267, 274,
292, 330, 333, **349**, **353**, **391–394**, 397,
 403, 406 f., 421 f., 426, 457
 Privatkopieschranke 338
 Privatsphäre 194 f., 201, 391–394
 Profilbildung 281, 288, 292 f., 315, 318,
 335, 391
 Profiling 281, 292, 303, 315, 318, 354 f.,
364 f., 367
 Pseudonymisierung 18, 202, **208 f.**, 283,
 289, 293, 359 f.
 Public sector information 25, 29, 93–95
 PSI-RL 29, 93 f., 96, 416, 436

 RAND 455
 Re-Identifizierung **165 f.**, **216 f.**, **219 f.**,
 223 f., 397, 402
 Real time data 9, 59, 81, 161 f., 200, 319 f.,
 345–347, 404, 457 f.
 – Portabilität 319 f., 345–347, 404, 457 f.
 Recht auf Berichtigung 315
 Recht auf datenerhebungsfreie Produkte
 203, 391
 Recht auf datenerhebungsfreies Umfeld
 203, 392
 Recht auf Datenportabilität
 – *siehe* Datenportabilität
 Recht auf Löschung (Vergessenwerden)
 214, 228, 296, **307–315**
 – Blockchain 309
 – Digitales Vergessen 308 f.
 – Einschränkungen 310 f.
 – Geistiges Eigentum 310
 – Geschäftsgeheimnisse 310
 – Löschpflichten 207 f.
 – Löschung durch Anonymisierung 214,
 308 f.
 – Künstliche Intelligenz 313–315
 – Suchmaschinen 311–313
 Recht auf Vergessenwerden 214, 228, 296,
307–315
 – *siehe näher* Recht auf Löschung
 Rechtmäßiger Benutzer 93, 440–448
 Rechtsakt über Daten 2021 25, 345, 421

 Registerrecht 100–110, 159–163, 418 f.
 Reputationsdaten 319, 347
 Reverse engineering 59 f., 115, 152,
163–168, 185, 224, 335, 416, 458
 Risikobasierter Ansatz 353–364
 Risikobewertung 355 f.
 Royalty Stacking 134, 453

 Schadensersatz (DSGVO) 381–383
 Schnittstellen **33 f.**, 51, **57–59**, **116 f.**, 119 f.,
 184, 202, **322 f.**, 346, 348, 352, **400**,
404 f., 433
 – urheberrechtlicher Schutz 116 f., 119 f.
 – Zugang 34, 352
 Schranken (immaterialgüterrechtliche) 414–
 416
 Schutzfrist 417 f.
 – Computerprogramme 417
 – Datenbank sui generis-Recht 417 f.
 – Urheberrecht 417
 SCHUFA-Rspr. des BGH 303, 371, 376
 Schutzrechtsüberschneidung 110, 114, 118,
414–417
 – Multiple Rechtsinhaberschaft 412–414
 – Problem für Datenzugang 414–416
 Scoring 293, 300 f., 303, 315, 365, 368,
 371 f., 403
 – Auskunft 300 f., 303, 371, 376
 – SCHUFA-Rspr. des BGH 303, 371, 376
 Selbstregulierung 219, 226, 233, 236, 344,
395–397, 401
 Single sign on-Dienste 204, **330 f.**
 Smart cities 215, 287
 Smart contracts 330, 365 f., 368 f., 374, 380
 Smart devices 262, 316, 320, 340, 391,
440–445, 446 f.
 Smart disclosure systems 262
 Smart farming 6, 10, 70, 206
 Smart goods 361, 390
 Smart grid 6
 Smart home 262, 391
 Smart metering 144, 273
 Smartphone 68, 199, 207, 262, 279
 Social plug-ins 240 f., 273
 Sole source Daten 32, 45, 65, 67, 71 f., 80,
 114, 134, 410, 438, **451–453**
 Soziale Netzwerke 10, 202, 211, 214, 251,
 305, 316, 326, 333 f., 337, 368, 386–388

- Speicherbegrenzung 307
- Spin off-Datenbanken **78 f.**, 438
- Standardessentielle Patente 33, 128, **132–135**, 353, **449 f.**, **453 f.**, 459
 - FRAND 33, 37, **132–135**, 353, 449 f.
- Standardisierung **33–35**, 62, 130–132, 132–135, 344, 348, **350–352**, 399, 405, 407, **458 f.**
- ICT 350
- Standardverträge 395–397
- Standardvertragsklauseln (Datenschutzrecht) **233–235**, 246, 361, 395–397
- Statistikzwecke 239, 285, **287–291**, 294, **301**, 397, 310, 314, 404 f., 436
- Stimme 209
- Suchmaschinen 10, 36, 83, 113, 251, 309, **311–313**, 378, 392
 - Delisting 211, **229**, **311 f.**
 - Metasuchmaschinen 83, 113
 - Recht auf Löschung (Vergessenwerden) 311–313
- Switching costs 57, 428, 432

- Technikneutralität 16, 54, 61, 346, 361, 380
- Technisch notwendige Vervielfältigung 53 f.
- Technische Schutzmaßnahmen (TPM) 125
- Technische und organisatorische Maßnahmen 219, 283, 289, 358, **362 f.**, 364, 397
- Text and Data Mining (TDM) 20, 43, 73, 75, **121–125**, 126, 147, 416
- Tickbox 251, 263
- Tinkering 120, 458
- Tracking 18, 199, 238, 263, 273, 367, 389 f.
- Trade Secrets-RL **137–189**, 416, 421, 431 f., 457 f.
- Trainingsdaten **7 f.**, 20 f., 31, 43, 75, 82, 103, 113, 127, **129 f.**, 136, 217, 271, 274, **313 f.**, 410
- Transaktionskosten 16, **31 f.**, 37 f., 88–90, 118, 158–160, 184, 239, 276, 323, 348, **409–421**, 446
- Transparenz 9, 28 f., 100, 166, 258, 262, 283, 362, 372, 375, 376 f., 379, 393, **394 f.**, 406
 - Algorithmen 370–372, 376, 378 f., 393 f.
 - Automatisierte Einzelentscheidungen 364–379
 - Content moderation 28 f.
 - Datenaltruismus 331
 - Datenschutz 257, 268, 372, 375
 - Datenschutzrechtliche Einwilligung 257, 268
 - Digital Services Act 378
 - Transparenzgebot 233, 444 f.
 - Transparenzgrundsatz 258, 283, 394 f., 407
 - Transparenzkontrolle 264 f., 268 f., 394 f.
 - Transparenzpflichten 25, 303, **378 f.**, 392, 427
 - Transparenzregeln 426, 444 f.
 - Treu und Glauben (§ 241 BGB) 135, 341, **423–426**, 444
- Überschutz 31 f., 409–417
 - Datenbank sui generis Recht 409 f.
 - Patentrecht 410
 - Urheberrecht 410 f.
- UKlaG 385
- Urheberrecht 41–127
 - Computerprogrammenschutz 115–121
 - Datenbankschutz sui generis 62–115
 - Datenbankwerke 46–62
 - Eigene geistige Schöpfung 46–59
 - Registrierung 419
- Urheberpersönlichkeitsrecht 55 f., 118 f., 198, 404, 416
- User centric approach 327–330
- User generated content 337, 340
- Utility Model 103, 418
- UWG 273, 279, 281, 293, **325 f.**, 341, **384–386**, 396, 423, **426 f.**

- Value added-Datenbank 83, 114
- Variety 5 f., 146, 183
- Veracity 5, 8
- Verantwortlicher 239
 - Begriff 239 f.
 - Abgrenzung zum Auftragsverarbeiter 246 f.
 - Gemeinsame Verantwortlichkeit 233, **240–247**, 357, **380**, 395
 - Mehrere Verantwortliche 246 f.
- Verarbeitungsgrundlage 247 f.
 - Einwilligung 248–275
 - Berechtigtes Interesse 275–282
- Verbot der automatisierten Einzelentscheidung 364–379

- Anfechtung 373
- Auskunftspflichten 370–375
- Ausdrückliche Einwilligung 369
- Begriff 365 f.
- Blockchain 368 f.
- Erhebliche Beeinträchtigung 366–369
- Erlaubnistatbestände 369 f.
- Geeignete Maßnahmen und Garantien 373–375
- Menschliches Eingreifen 373 f., 377
- Menschliche Mitwirkung an der Entscheidung 365 f., 373 f., 377
- Offenlegung von Einzelentscheidungen 372 f., 376
- Offenlegung von Algorithmen 370–372, 376
- Personalisierte Angebote 367 f.
- Personalisierte Preise 367
- Personalisiertes Recht 367
- Right to reasonable inferences 393 f.
- Scoring 368
- Smart contracts 368 f.
- Stellung in der DSGVO 375 f.
- Transparenz 372
- Umfang der Offenlegungspflichten 370–375, 376
- Unmittelbare rechtliche Wirkung 366–369
- Vertragsabschluss oder -erfüllung 369 f.
- Voraussetzungen 365 f.
- Verbraucherrecht 39, 258, 268, 332, 391, 394, 406, 429 f., 445
- Verbraucherrechte-RL 378, 392
- Verhältnis zum Datenschutzrecht 258, 268, 394, 406
- Verfahrensprodukte **131 f.**, 136, 323, 410, 449
- Verhältnismäßigkeit 38, 178 f., 182, 185, 188, 195, 295, 369, 410
- Verimi 330
- Verkehrserwartung 135, 425
- Verschlüsselung 125, **131 f.**, 136, 208 f., 359 f., 361
 - homomorphe Verschlüsselung 361, 406
- Vertragsrecht 199, 220 f., 224, 250, **253–256**, 258, **265 f.**, **268**, **271–372**, 275, 279, 281, **292**, 294, 333, **353**, **394–401**, **402–407**, **411–414**, **420–425**, **440–446**, 447
 - personenbezogene Daten 199, 220 f., 224, 250, **253–256**, 258, **265 f.**, **268**, **271–372**, 275, 279, 281, **292**, 294, 333, **353**, **394–401**, **402–407**
 - Verträge über Daten (B2C) **271–273**, **394–401**
 - Datenschuldner 255, 272 f.
 - Kündigungsrecht 272
 - Rücktrittsrecht 255, 273
 - Schadensersatz 255
 - Volunteered data 18, **68**, 81, 410
 - Voreinstellungen
 - Datenschutzfreundliche Voreinstellungen 358 (*siehe auch* privacy by default)
 - Einwilligung 263
 - Warenkauf-RL 340
 - Wearables 199
 - Web-Tracking 199
 - Wesentliche Investition 62–82
 - Whistleblowing 178–181
 - Widerlegliche Vermutung (Anonymisierung) 219–224, 402
 - Widerrechtliche Aneignung von Geschäftsgeheimnissen **142 f.**, **169**, 423, 425
 - Widerrechtliche Überwindung technischer Schutzvorkehrungen 425
 - Widerruf der Einwilligung 269–273, 274, 292 f.
 - Künstliche Intelligenz 271
 - Personalisierte Services 271
 - Rechtsfolgen für Verträge 271–273
 - Reformbedarf 274 f.
 - Weiterverarbeitung nach Widerruf 270
 - WIPO-Proof 161 f., 411, 418
 - Wirtschaftliche Handlungsfreiheit 277
 - Wissenschaftsfreiheit 195
 - Zentralisierter Schutz 195
 - Zertifizierung
 - grenzüberschreitender Datenverkehr 236
 - Zugangsrechte 25, **35–37**, 133, 344, 346, 348, **428–457**
 - Abgrenzung zu Nutzungsrechten 429–435
 - Aggregierte Datensets 448–457
 - B2B 35 f., 344 f., 348, 412, **435–437**, 445, 458
 - B2C 35, 420 f., 436 f., 445

- B2G 35, 436
- Berechtigte Nutzer 440–448
- Bereichsspezifische Zugangsrechte 428 f.
- Fallgruppen 440–457
- G2B 35, 113, 415, 436
- Geschäftsgeheimnisse 431–435, 455–457
- Individual level use data 440–448
- Kartellrechtliche Zugangsansprüche 432–435
- Vergütung 443 f., 448 f.
- Zugriffsverwaltete Daten 423
- Zwangslizenzen 30, 35, 57, 59, 115, 120, 123 f., 323, 342, 409, 432, 438, **448–453, 454–457**
- Datenbank-RL **451–453**
- Kartellrecht 35, 57, 59, 120, 432, 438, **449 f.**
- Vergütung 448 f., 453 f.
- Zwangslizenzeinwand 409, 449 f.
- Zweckänderung **282–291**, 362, 402, **405**
- Einwilligung 285
- Forschungs- und Statistikzwecke 287–290
- Kompatibilitätstest 285–287, 405
- Zweckbindung **282–287**, 331, 388, 405
- Zweiterwerber 134 f., 424, 459