

STEFAN HERRMANN

Völkerrechtliche
Jurisdiktionsgrundlagen
für den Datenschutz
im Netz

Jus Internationale et Europaeum

173

Mohr Siebeck

Jus Internationale et Europaeum

herausgegeben von
Thilo Marauhn und Christian Walter

173



Stefan Herrmann

Völkerrechtliche
Jurisdiktionsgrundlagen für
den Datenschutz im Netz

Mohr Siebeck

Stefan Herrmann, geboren 1992; Studium der Rechtswissenschaft an der Universität München; 2015 Erste Juristische Staatsprüfung; wissenschaftlicher Mitarbeiter am Lehrstuhl für Völkerrecht und Öffentliches Recht an der LMU München; 2020 Promotion; Rechtsreferendariat im OLG-Bezirk München; 2020 Zweite Juristische Staatsprüfung.
orcid.org/0000-0001-9608-4517

ISBN 978-3-16-159969-9 / eISBN 978-3-16-159985-9
DOI 10.1628/978-3-16-159985-9

ISSN 1861-1893 / eISSN 2568-8464 (Jus Internationale et Europaeum)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet 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.

Gedruckt auf alterungsbeständiges Werkdruckpapier.

Printed in Germany.

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2020 von der juristischen Fakultät der Ludwig-Maximilians-Universität München als Dissertation angenommen.

Meinem Doktorvater, Professor Dr. Christian Walter, danke ich herzlich für seine Betreuung, für die damit verbundene Begeisterung am Thema und sein stetiges Interesse am Fortgang der Arbeit. Danken möchte ich ihm auch für die wertvollen Erfahrungen, die ich während meiner Zeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Völkerrecht und Öffentliches Recht sammeln durfte, sowie für die angenehme und sehr herzliche Atmosphäre am Lehrstuhl.

Professor Dr. Christian Walter und Professor Dr. Thilo Maruhn danke ich für die Aufnahme der Arbeit in die Schriftenreihe „Jus Internationale et Europaeum“.

Frau Professor Dr. Ann-Katrin Kaufhold gebührt mein Dank dafür, dass sie während ihres Forschungsaufenthalts in Australien zügig das Zweitgutachten zur Arbeit verfasste und darin wertvolle Anregungen zur Thematik gab. Professor Dr. Jens Kersten sei für seine Tätigkeit als Zweitprüfer in der mündlichen Prüfung gedankt.

Die Erstellung der Arbeit wurde von der Studienstiftung des deutschen Volkes gefördert. Dafür ein herzliches Dankeschön!

Meinen Kolleginnen und Kollegen an der Universität, unter ihnen Stephan Lorentz, Charlotte Mölter, Maria Monnheimer, Inge Neber-Germeier, Philip Nedelcu, Stefan Schäferling, Sabine Schäufler, Chun-Kyung Paulus Suh und Markus Vordermayer-Riemer, möchte ich für ihre große Unterstützung und ihre regelmäßige Bereitschaft zum Austausch danken. Es freut mich sehr, dass sich aus unserem gemeinsamen Weg echte Freundschaften entwickelt haben.

Ganz besonders danken möchte ich meinen Eltern, meinem Bruder Thomas sowie Raphaela. Danke für eure beständige Unterstützung, eure Motivation und euer großes Vertrauen! Ihr habt maßgeblich zum Gelingen der Arbeit beigetragen.

München, im Dezember 2020

Stefan Herrmann

Inhaltsverzeichnis

Vorwort	VII
Abkürzungsverzeichnis	XXIII
Einführung	1
A. Notwendigkeit von Datenschutz in Zeiten von Big Data	1
B. Völkerrechtliche Herausforderungen datenschutzrechtlicher Regulierung im Netz	4
I. Das Territorialitätsprinzip als Hindernis für die Regulierung?	5
II. Art. 3 Abs. 2 DSGVO: Zulässige neue Wege bei der Bestimmung des räumlichen Anwendungsbereichs im Datenschutzrecht?	9
III. Weltweite Löschpflichten im Netz?	10
C. Ziel und Vorgehensweise der Arbeit	12
Teil I: Die völkerrechtliche Jurisdiktionslehre für die Datenschutzregulierung im Netz	15
<i>Kapitel 1: Völkerrechtliche Anforderungen an die unilaterale Datenschutzregulierung im Cyberspace</i>	21
A. Geltung der völkerrechtlichen Jurisdiktionslehre im Cyberspace	21
I. Jurisdiktion: staatliche Kompetenz zur Ausübung von Hoheitsgewalt	22
1. Begriff und Träger von Hoheitsgewalt	22
2. Verschränkung von Kollisionsrecht und Jurisdiktions- lehre	24
3. Anwendungsbereich der Jurisdiktionslehre	26
II. Zulässigkeit unilateraler Jurisdiktion im Cyberspace	27
1. Regulierung in der Anfangsphase des Internets	27
2. Cyberspace als vierte Dimension?	28
3. Cyber-Regulierung als staatliche Aufgabe	29

B.	Territoriale Verankerung von Jurisdiktion und Regulierung im Netz	30
I.	Territoriale Jurisdiktion als Ausfluss der Gebietshoheit	30
II.	Von „Lotus“ zum „genuine link“-Erfordernis	32
1.	Differenzierung zwischen Durchsetzungs- und Regelungs- hoheit	32
2.	Notwendigkeit eines „genuine link“	33
III.	Die Charakteristika des Internets als Herausforderung für eine territoriale Regulierung im Netz	36
1.	Ubiquität des Netzes	36
2.	Volatilität von Daten	37
3.	Gefahr der Entstehung von Jurisdiktionskonflikten	39
C.	Umgang mit Extraterritorialität in der Jurisdiktionslehre	39
I.	Extraterritorialität im Völkerrecht	40
1.	Extraterritorialität als Begriff	40
2.	Notwendigkeit zur Rechtfertigung extraterritorialer Regulierung?	41
II.	Vereinbarkeit extraterritorialer Jurisdiktion mit dem Grundsatz der Gebietshoheit?	43
III.	Gebotene Vermeidung von Jurisdiktionskonflikten	45
IV.	Umgang mit der Ausübung von Hoheitsgewalt durch Drittstaaten ..	47
1.	Interventionsverbot	47
2.	Abwehr durch faktisches Handeln	49
D.	Stellung des Regelungsadressaten bei der grenzüberschreitenden Ausübung von Hoheitsgewalt	50
I.	Schutz staatlicher Rechtspositionen durch die Jurisdiktionslehre	50
1.	Vorhersehbarkeit ausländischer Einflüsse: Element zur Umgrenzung der staatlichen Ordnungshoheit	52
2.	Individualschutz als Rechtsreflex der Jurisdiktionsprinzipien? ..	53
II.	Auswirkung menschenrechtlicher Garantien auf die grenzüberschreitende Jurisdiktion	55
1.	Das Kriterium der Vorhersehbarkeit im europäischen Menschenrechtsschutz	55
2.	Das Kriterium der Vorhersehbarkeit im universellen Menschenrechtsschutz	58
III.	Verschränkung des völkerrechtlichen Legalitätsprinzips mit der Jurisdiktionslehre	59
IV.	Zwischenergebnis	60
 <i>Kapitel 2: Grenzüberschreitende Dimension des Datenschutzes im Cyberspace</i>		 63
A.	Ziele und Bedeutung des Datenschutzes in Zeiten von Big Data	64
I.	Grund- und menschenrechtliche Verankerung des Datenschutzes ..	64

1. Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG	64
2. Schutz des Privatlebens bzw. der Privatheit in den Menschenrechten	67
II. Datenverarbeitung durch private Akteure als Gefahr für die Freiheit	69
1. Profiling durch die datenverarbeitenden Akteure	70
2. Auswirkungen auf die Freiheit der Betroffenen	71
III. Folgen für das Datenschutzrecht	73
B. Herausforderungen bei der Ermittlung von „genuine links“ zur Datenschutzregulierung im Netz	74
I. Herausforderungen bei der territorialen Bestimmung des Anwendungsbereichs	76
1. Möglichkeiten der räumlichen Anknüpfung	76
2. Unterschiedliche Intensität territorialer Bezugspunkte	77
3. Anknüpfungsmöglichkeiten bei hohem Regelungsbedürfnis	79
II. Herausforderungen bei der personellen Bestimmung des Anwendungsbereichs	82
1. Möglichkeiten der personellen Anknüpfung	82
2. Risiken personeller Anknüpfung	83
III. Herausforderungen bei der Bestimmung des Umfangs von Löschungspflichten	84
C. Reaktion des Datenschutzrechts auf weltweite Bezugspunkte datenschutzrechtlicher Sachverhalte	86
I. Territoriale Anknüpfungspunkte	86
1. Anknüpfung an eine Datenverarbeitung im Inland	86
2. Weite Auslegung des Niederlassungsbegriffs	88
3. Festlegung von Anforderungen an eine Datenübermittlung an Drittstaaten	89
II. Extraterritoriale Anknüpfungspunkte	90
1. Nutzung des passiven Personalitätsprinzips	90
2. Einführung des Marktortprinzips	90
III. Anordnung weltweiter Löschpflichten	91
 Teil II: Datenschutzrechtliche Regulierung nach dem Territorialitätsprinzip	 93
 <i>Kapitel 3: Territoriale Anknüpfung an Datenverarbeitungsvorgänge</i>	 95
A. Datenverarbeitung auf technischen Anlagen im Inland	97
I. Datenverarbeitungsprozesse: constituent elements des Datenschutzrechts	98

1.	Notwendigkeit eines constituent elements im Staatsgebiet	98
2.	Einschätzungsspielraum bei der Bestimmung von constituent elements	99
3.	Territoriale Fassbarkeit von Datenverarbeitungsvorgängen	100
II.	Notwendigkeit eines Inlandsbezugs der Daten?.....	101
B.	Datenerhebung durch die Nutzung technischer Mittel im Inland	103
I.	Zulässigkeit territorialer Anknüpfung an den Aufruf von Webseiten?.....	105
1.	Spannungsverhältnis zwischen innerstaatlicher Ordnungshoheit und fremdstaatlicher Souveränität	105
2.	Notwendigkeit der Vorhersehbarkeit der Regulierung nach dem Territorialitätsprinzip	108
a)	Das Vorhersehbarkeitskriterium als Voraussetzung für die Jurisdiktionsausübung	108
b)	Maßstab zur Ermittlung einer vorhersehbaren Regulierung ..	109
c)	Vorhersehbarkeit staatlicher Regulierung bei einer Anknüpfung an den Aufruf einer Webseite im Inland?	112
3.	Zwischenfazit	112
II.	Anknüpfung an spezifische Bezugspunkte zwischen Webseite und regulierendem Staat	113
1.	Erfolgsorte bei Ehrverletzungsdelikten	113
a)	Rechtsprechung des EuGH.....	114
b)	Stellungnahme	116
2.	Übertragung der Ergebnisse auf die Nutzung von Cookies	118
C.	Fazit.....	119

Kapitel 4: Territoriale Anknüpfung an Niederlassungen im Staatsgebiet 121

A.	Extraterritoriale Reichweite des Art. 3 Abs. 1 DSGVO	124
I.	Weite Auslegung des Niederlassungsbegriffs	124
II.	Weite Auslegung des Merkmals „im Rahmen der Tätigkeiten einer Niederlassung“	127
1.	Keine Notwendigkeit der Wahrnehmung von Entscheidungsgewalt über die Datenverarbeitung innerhalb der Niederlassung	127
2.	Keine Notwendigkeit der Durchführung der Datenverarbeitung innerhalb der Niederlassung	128
a)	Auslegung des Merkmals „im Rahmen der Tätigkeiten einer Niederlassung“ im Urteil Google Spain.....	129
b)	Notwendigkeit eines engen Bezugs der Tätigkeit der Niederlassung zur Datenverarbeitung.....	130
c)	Übertragung der Auslegung auf Art. 3 Abs. 1 DSGVO	132

III. Extraterritoriale Wirkungen des Art. 3 Abs. 1 DSGVO im Kontext transnational tätiger Verantwortlicher bzw. Auftragsverarbeiter	134
1. Konstellation 1: Durchführung der Datenverarbeitung außerhalb der Union für einen Verantwortlichen in der Union	134
a) Variante a): Datenverarbeitung durch Niederlassungen	134
b) Variante b): Datenverarbeitung durch Auftragsverarbeiter ...	136
aa) Extraterritoriale Wirkung gegenüber dem Auftragsverarbeiter	136
bb) Zurechnung der Tätigkeit des Auftragsverarbeiters an den Verantwortlichen	139
2. Konstellation 2: Durchführung der Datenverarbeitung in der Union für einen außereuropäischen Verantwortlichen	140
a) Variante a): Datenverarbeitung durch Niederlassungen	140
b) Variante b): Datenverarbeitung durch Auftragsverarbeiter ...	141
B. Jurisdiktionelle Anknüpfung an Unternehmen in der völkerrechtlichen Debatte	142
I. Völkerrechtliche Diskussion um die Ausübung von Hoheitsgewalt gegenüber multinationalen Unternehmen	143
1. Parent-based approach	145
2. Zugriff auf ausländische Mutterunternehmen	146
II. Vergleichbarkeit der völker- und datenschutzrechtlichen Konstellationen	147
1. Parallelen zwischen völker- und datenschutzrechtlichen Fallgruppen	147
2. Unerheblichkeit gesellschaftsrechtlicher Strukturen für das Datenschutzrecht	148
III. Fazit für das weitere Vorgehen	152
C. Indirekte Einwirkung auf ausländische datenverarbeitende Stellen	154
I. Völkerrechtliche Zulässigkeit des parent-based approach	154
1. Primärebene	154
a) Nähe des parent-based approach zur Kontrolltheorie	154
b) Einwirkung in die Ordnungshoheit fremder Staaten durch den parent-based approach	156
2. Sekundärebene	159
a) Völkerrechtliche Zulässigkeit eines haftungs- bzw. sanktionsrechtlichen Zugriffs	160
b) Notwendigkeit der Anknüpfung an die gesellschaftsrechtliche Leitungsmacht	161
II. Zulässigkeit der Durchreichung datenschutzrechtlicher Vorgaben an verarbeitende Stellen in Drittstaaten	163
1. Durchreichung im Verhältnis zwischen Verantwortlichem und einer Niederlassung	164

a) Primärebene	164
b) Sekundärebene	164
2. Durchreichung im Verhältnis zwischen Verantwortlichem und Auftragsverarbeiter.....	165
a) Primärebene	165
b) Sekundärebene	168
III. Fazit	171
D. Direkter Zugriff auf ausländische Regeladressaten.....	171
I. Datenverarbeitung im Inland für einen Verantwortlichen im Ausland.....	172
1. Zurechnung von Verhalten nach der Theorie der Unternehmenseinheit.....	172
2. Das Territorialitätsprinzip als Basis der Zurechnung nach der Theorie der Unternehmenseinheit.....	174
3. Die Zurechnung einer Datenverarbeitung an einen ausländischen Verantwortlichen	176
a) Datenverarbeitung durch eine selbständige Niederlassung ...	176
b) Datenverarbeitung durch eine unselbständige Nieder- lassung	177
c) Datenverarbeitung durch einen Auftragsverarbeiter	177
II. Durchführung einer mit der Datenverarbeitung eng verbundenen Tätigkeit im Inland für einen Verantwortlichen im Ausland	179
1. Zugriff nach der Theorie der Unternehmenseinheit?.....	179
2. Anerkennung eines territorialen Konzernzugriffs nach den Grundsätzen der jurisdiction to adjudicate?	182
a) General jurisdiction	183
aa) Notwendigkeit der Ausübung einer dauerhaften, systematischen Geschäftstätigkeit	184
bb) Einschränkung der general jurisdiction durch den Supreme Court	185
cc) General jurisdiction: Ausprägung des Territorialitäts- prinzips?.....	186
b) Jurisdiction nach dem Alien Tort Statute	188
c) Zwischenfazit	191
3. Territorialer Zugriff nach den Jurisdiktionsgrundsätzen zur strafbaren Beteiligung?	191
4. Zwischenergebnis.....	192
III. Zugriff auf Auftragsverarbeiter im Ausland	192
1. Zugriff nach der Theorie der Unternehmenseinheit?.....	192
2. Territorialer Zugriff nach den Jurisdiktionsgrundsätzen im Strafrecht	193
IV. Fazit	194

<i>Kapitel 5: Territoriale Anknüpfung an Datenübermittlungen in Drittstaaten</i>	197
A. Regulierung von Datenübermittlungen an Drittstaaten im Datenschutzrecht	197
B. Das Angemessenheitserfordernis als Fall territorialer Extension von Jurisdiktion	200
I. Territoriale Extension: unilaterale Regulierung mit universeller Reichweite	200
II. Auswirkungen des Angemessenheitserfordernisses auf Drittstaaten	202
1. Einfluss der EU im Datenschutzbereich	202
2. Strenge materielle Anforderungen der Art. 44 ff. DSGVO	203
3. Erhöhung des Datenschutzniveaus in Drittstaaten	204
C. Vereinbarkeit des Angemessenheitserfordernisses mit dem Territorialitätsprinzip	206
I. Reaktionen in der Staatenpraxis	206
II. Territoriale Aspekte als Grundlage der Regulierung	208
D. Fazit	210
Teil III: Extraterritoriale Jurisdiktionsausübung im Datenschutzrecht	211
<i>Kapitel 6: Bedürfnis zur extraterritorialen Jurisdiktion im Datenschutzrecht</i>	213
A. Fehlen territorialer Anknüpfungspunkte	213
B. Keine internationale Harmonisierung des Datenschutzrechts	215
I. Menschenrechte	216
1. Universelle Ebene	216
2. Regionale Ebene	218
a) Art. 8 Abs. 1 EMRK	218
b) Art. 7 i.V.m. Art. 8 GRCh	219
c) Menschenrechtsdokumente im außereuropäischen Raum	220
3. Zwischenfazit	221
II. Datenschutzkonvention 108 des Europarats	221
1. Die Konvention und ihre Erweiterung durch das Zusatz- protokoll 181	222
2. Reichweite der Konvention und des Zusatzprotokolls	223
3. Modernisierung der Konvention 2018	225
III. Soft law auf universeller Ebene	227

1. OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.....	227
2. UN Guidelines for the Regulation of Computerized Personal Data Files	229
IV. Instrumente auf regionaler Ebene	230
1. Datenschutzrecht der EU	230
2. Datenschutz im afrikanischen Rechtsraum	232
3. Weitere regionale Instrumente.....	233
V. Zwischenfazit.....	233
C. Divergierende staatliche Ordnungsvorstellungen über den Datenschutz	234
I. Datenschutzrechtlicher Minimalkonsens	235
1. Personeller bzw. institutioneller Anwendungsbereich	235
2. Materiellrechtliche Gewährleistungen	235
II. Hohes Datenschutzniveau in der EU und einigen Drittstaaten	236
1. Kennzeichen eines hohen Datenschutzniveaus	236
2. Staaten mit hohem datenschutzrechtlichem Standard	237
III. Datenschutz in den USA	238
1. „Datenschutzrecht“ in den USA	239
2. Selbstregulierung des Marktes.....	242
a) Safe Harbor-Grundsätze.....	242
b) Privacy Shield.....	243
D. Fazit.....	246
 <i>Kapitel 7: Personalitäts- und Schutzprinzip</i>	 247
A. Aktives Personalitätsprinzip.....	248
I. Personelle Beziehung zum Staat als Jurisdiktionsgrundlage	248
1. Personelle Verankerung von Hoheitsgewalt in der Geschichte des Völkerrechts.....	248
2. Zulässigkeit des aktiven Personalitätsprinzips im heutigen Völkerrecht	249
II. Aktives Personalitätsprinzip im Datenschutzrecht	250
1. Aktives Personalitätsprinzip: Schutz vor einer Flucht in Datenoasen.....	251
2. Unterschiedliche Datenschutzniveaus als Problem für die Anknüpfung nach dem aktiven Personalitätsprinzip?	252
III. Reichweite des aktiven Personalitätsprinzips	254
1. Offenheit des Prinzips zur Erweiterung auf Nicht-Staatsangehörige	254
2. Personale Anknüpfung bei juristischen Personen neben dem Sitz- und Gründungsort	256
a) Hauptverwaltung und Hauptniederlassung im Inland	256

b) Geschäftliche Tätigkeit im Inland	256
3. Zulässigkeit der Erstreckung im Konzernkontext	258
a) Zu- bzw. Durchgriff auf ausländische Tochterunternehmen	258
aa) Grundsatz: Anerkennung der gesellschaftsrechtlichen Trennungstheorie	259
bb) Ausnahme: Durchbrechung in Missbrauchsfällen	261
cc) Folgen für einen datenschutzrechtlichen Zu- bzw. Durchgriff	264
b) Zugriff auf ein ausländisches Mutterunternehmen	264
B. Passives Personalitätsprinzip	267
I. Zulässigkeit der Jurisdiktionsanknüpfung	267
II. Anwendung des Prinzips im Datenschutzrecht	269
1. Prinzipielle Anwendung des Datenschutzrechts auf der Grundlage des passiven Personalitätsprinzips	269
2. Durchreichung von Datenschutzvorschriften auf der Grundlage des passiven Personalitätsprinzips?	271
C. Schutzprinzip	272
I. Jurisdiktion zugunsten der Sicherheit und des Bestands des Staates	272
II. Schutz der Demokratie als Anknüpfungspunkt im Datenschutz- recht?	274
D. Fazit	276
<i>Kapitel 8: Wirkungsprinzip</i>	279
A. Jurisdiktion nach dem Wirkungsprinzip am Beispiel von Art. 3 Abs. 2 DSGVO	280
I. Das Wirkungsprinzip als Erweiterung des Territorialitäts- prinzips	280
1. Differenzierung zwischen dem Territorialitäts- und Wirkungsprinzip	282
a) Constituent element-Ansatz?	284
b) Relevanz des Willens des Akteurs?	286
c) Stufenverhältnis zwischen Wirkungs- und objektivem Territorialitätsprinzip	287
2. Art. 3 Abs. 2 DSGVO als Beispiel des Wirkungsprinzips	290
a) Angebot von Waren und Dienstleistungen in der Union	291
b) Verhaltensbeobachtung	295
II. Schutz von Personen innerhalb der Union durch die Anwendung des Wirkungsprinzips	298
1. Schließung von Schutzlücken durch Art. 3 Abs. 2 DSGVO	298
2. Art. 3 Abs. 2 DSGVO: zwischen Wirkungs- und passivem Personalitätsprinzip?	300

3. Grenzen des Art. 3 Abs. 2 DSGVO	302
B. Zulässigkeit und Grenzen des Wirkungsprinzip im Allgemeinen	305
I. Das Wirkungsprinzip als Baustein der völkerrechtlichen Jurisdiktionslehre	305
II. Kriterien des Wirkungsprinzips im Wirtschaftsrecht	308
1. Unmittelbarkeit der Wirkungen	309
2. Wesentlichkeit der Wirkungen	312
3. Vorhersehbarkeit der Wirkungen	313
4. Zwischenergebnis: Funktionen der Voraussetzungstrias	314
III. Kriterien für die Erfassung von Internetsachverhalten	314
1. Herangehensweise der U.S.-Gerichte	315
a) Zippo-Test	316
b) Calder Effects-Test	319
2. Anknüpfung im Unionsrecht	323
a) Notwendigkeit der Ausrichtung von Webseiten auf einen Staat	323
b) Kriterien zum Nachweis der Ausrichtung einer Webseite	325
3. Ableitung von Kriterien für das Wirkungsprinzip in Internetfällen	328
a) Parallelen in der Rechtsprechung	328
b) Folgen für die Voraussetzungstrias des Wirkungsprinzips	329
C. Zulässigkeit und Grenzen des Wirkungsprinzips im Datenschutzrecht	330
I. Anknüpfung an die Datenverarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen im Territorium	331
1. Anerkennung der Anknüpfung in der Staatenpraxis	331
2. Regulierung ausländischer Einflüsse	333
3. Vorhersehbarkeit der Regulierung	334
4. Zwischenfazit	336
II. Anknüpfung an eine Datenverarbeitung im Zusammenhang mit einer Verhaltensbeobachtung im Territorium	336
1. Verhaltensbeobachtung: Einfallstor für universelle Jurisdiktionsansprüche	337
2. Notwendigkeit eines Korrektivs	339
3. Pflicht zur Nutzung von Geolocation-Technologien?	340
a) De lege lata	341
b) De lege ferenda	343
4. Folgen für die Auslegung von Art. 3 Abs. 2 lit. b) DSGVO	347
III. Zulässigkeit vorgreiflicher Pflichten	347
1. Der Wille des Akteurs als Bezugspunkt vorgreiflicher Pflichten	347
2. Akzeptanz vorgreiflicher Regulierung in der Staatenpraxis	348
3. Notwendigkeit vorgreiflicher Pflichten im Datenschutzrecht	349

D. Ergänzung des Wirkungsprinzips durch das passive Personalitätsprinzip	351
I. Grenze der Anknüpfung nach dem Wirkungsprinzip	351
II. Möglichkeit der Heranziehung des passiven Personalitätsprinzips	352
E. Fazit	354
Teil IV: Umgang mit Jurisdiktionskonflikten	355
<i>Kapitel 9: Entstehung und Lösung von Jurisdiktionskonflikten</i>	357
A. Entstehung von Jurisdiktionskonflikten	358
I. Konflikte bei der datenschutzrechtlichen Regulierung	359
1. Globales Recht auf Vergessenwerden	359
a) Umsetzung der Google Spain-Entscheidung des EuGH	359
b) Folgevverfahren: Google LLC	361
2. Verpflichtung zur Datenherausgabe in den USA	362
a) SWIFT-Konflikt	363
b) Microsoft v. USA	364
c) CLOUD Act	364
II. Weitere Konflikte bei der Regulierung im Netz	366
1. Google v. Equustek Solutions	366
a) Verfahren vor kanadischen Gerichten	366
b) Folgevverfahren in den USA und Kanada	368
2. Lösungsersuchen gegen Facebook zum Schutz vor Hate Speech	370
B. Lösung von Jurisdiktionskonflikten durch eine Abwägung im Einzelfall	371
I. Notwendigkeit einer Interessenabwägung im Einzelfall	371
1. Bedürfnis zur Lösung von Jurisdiktionskonflikten	371
2. Lösung des Konflikts durch eine Interessenabwägung	374
II. Ansätze zur Interessenabwägung in der Staatenpraxis	375
1. Reasonableness-Prüfung	375
2. Comity	377
a) Anerkennung von Rechtsakten fremder Staaten	377
b) Selbstbeschränkung bei der Regulierung grenzüberschreitender Sachverhalte	378
aa) Anwendung bei der Wettbewerbsregulierung in den USA	378
bb) Comity-Prüfung im Rahmen des CLOUD Act	379
cc) Anwendung in Kanada	380
3. Verhältnismäßigkeit	381

a) Anwendung des Grundsatzes bei der wirtschafts- rechtlichen Regulierung	381
b) Heranziehung des Grundsatzes in den Fällen Google LLC und Glawischnig-Piesczek	382
c) Art. 49 Abs. 1 DSGVO	385
III. Schwierigkeiten und Herausforderungen der Interessenabwägung	388
1. Gewohnheitsrechtlicher Stellenwert	389
2. Interessenabwägung nur im Fall echter Konflikte	390
3. Kein internationaler Maßstab für eine Interessenabwägung	392
IV. Fazit: Notwendigkeit von Leitlinien für die Durchführung einer Interessenabwägung	394
 <i>Kapitel 10: Konfliktlösung durch einen Zwei-Stufen-Test</i>	395
A. Interessenabwägung durch einen Zwei-Stufen-Test	396
I. Modell einer zweistufigen Prüfung	396
II. Verhältnis zum Modell eines Layered Approach von Dan Svantesson	398
III. Verhältnis zur Reasonableness-Prüfung nach § 403 des Restatement (Third)	400
B. Stufe 1: Rückführbarkeit des Ge-/Verbots auf internationale Verpflichtungen	402
I. Lösung von Konflikten im Falle von Auslistungs- oder Löschpflichten	403
1. Universelle Verpflichtung	403
2. Regionale Verpflichtung	406
3. Fehlen internationaler Verpflichtungen	410
a) Umsetzung staatlicher Ordnungsvorstellungen	410
b) Berufung auf international anerkannte Ziele bei der Regulierung	411
II. Lösung von Konflikten im Übrigen	414
1. Universelle Verpflichtung	414
2. Regionale Verpflichtung	415
3. Fehlen internationaler Vereinbarungen	416
C. Stufe 2: Ermittlung der Verbindungsintensität zwischen Sachverhalt und Staat	419
I. Notwendigkeit einer engen inhaltlichen Beziehung zwischen Staat und Sachverhalt	419
II. Tendenzieller Vorrang der Anknüpfung nach dem Wirkungsprinzip	422
D. Fazit	423

Zusammenfassung	425
Verzeichnis der verwendeten Rechtsprechung	431
Verzeichnis von Beschlüssen, Erklärungen und Dokumenten internationaler und supranationaler Organisationen.....	439
Verzeichnis sonstiger Dokumente	445
Literaturverzeichnis.....	447
Sachregister	477

Abkürzungsverzeichnis

AIPD	Association Internationale De Droit Pénal
AJCL	The American Journal of Comparative Law
AJIL	The American Journal of International Law
AJIL Supp.	The American Journal of International Law Supplement
Albany L. J. Sci. & Tech.	Albany Law Journal of Science and Technology
Amsterdam L. F.	Amsterdam Law Forum
AÖR	Archiv des öffentlichen Rechts
APEC	Asia Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
AVR	Archiv des Völkerrechts
BB	Betriebsberater
BDSG	Bundesdatenschutzgesetz
Berkeley Technology L. J.	Berkeley Technology Law Journal
BYIL	British Yearbook of International Law
CCZ	Corporate Compliance Zeitschrift
Chicago J. Int'l. L.	Chicago Journal of International Law
CLSR	Computer Law & Security Review
CML Rev.	Common Market Law Review
Columbia J. Transn'l. L.	Columbia Journal of Transnational Law
Columbia L. Rev.	Columbia Law Review
Connecticut J. Int'l. L.	Connecticut Journal of International Law
Connecticut L. Rev.	Connecticut Law Review
CR	Computer und Recht
CRi	Computer Law Review international
Crim. L. Forum	Criminal Law Forum
DePaul L. Rev.	De Paul Law Review
BerDGIR	Berichte der Deutschen Gesellschaft für Internationa- les Recht
BerDGVR	Berichte der Deutschen Gesellschaft für Völkerrecht
DÖV	Die Öffentliche Verwaltung
DSGVO/DS-GVO	Datenschutzgrundverordnung
DuD	Datenschutz und Datensicherheit
DVBl.	Deutsches Verwaltungsblatt
ECFR	European Company and Financial Law Review
ECOWAS	Economic Community of West African States
EGMR	Europäischer Gerichtshof für Menschenrechte
EJIL	The European Journal of International Law
EKMR	Europäische Kommission für Menschenrechte
EU	Europäische Union

EuR	Europarecht
European Foreign Affairs Rev.	European Foreign Affairs Review
EuZA	Europäische Zeitschrift für Arbeitsrecht
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWS	Europäisches Wirtschafts- und Steuerrecht
Fordham Intell. Pro. Media & Ent. L. J.	Fordham Intellectual Property, Media & Entertainment Law Journal
Fordham Int'l. L. J.	Fordham International Law Journal
GA	Goldammer's Archiv für Strafrecht
Georgetown L. J.	Georgetown Law Journal
Georgetown J. Int'l. Affairs	Georgetown Journal of International Affairs
German L. J.	German Law Journal
GPR	Zeitschrift für das Privatrecht der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR Int.	Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil
GYIL	German Yearbook of International Law
Harv. Int'l. L. J.	Harvard International Law Journal
Harv. L. Rev.	Harvard Law Review
Hastings Int'l. & Comp. L. Rev.	Hastings International and Comparative Law Review
HRLR	Human Rights Law Review
ICLQ	International and Comparative Law Quarterly
IDPL	International Data Privacy Law
IGH	Internationaler Gerichtshof
IJLIT	International Journal of Law and Information Technology
ILC	International Law Commission
Ind. J. Global Legal Stud.	Indiana Journal of Global Legal Studies
Int'l. Crim. L. Rev.	International Criminal Law Review
IPbpR	Internationaler Pakt über bürgerliche und politische Rechte
IPRax	Praxis des Internationalen Privat- und Verfahrensrechts
IPwskR	Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte
JA	Juristische Arbeitsblätter
JCMS	Journal of Common Market Studies
J. Comp. & Inform. L.	John Marshall Journal of Computer and Information Law
JDI	Journal de Droit International
J. Int'l. & Comp. L.	Journal of International and Comparative Law
J. Int'l. Criminal Justice	Journal of International Criminal Justice
John Marshall L. Rev.	John Marshall Law Review
J. Priv. Int'l. L.	Journal of Private International Law
JRP	Journal für Rechtspolitik
JZ	Juristen-Zeitung
K&R	Kommunikation & Recht
Law & Contemp. Probs.	Law and Contemporary Problems
Leiden J. Int'l. L.	Leiden Journal of International Law

Melb. J. Int'l. L.	Melbourne Journal of International Law
Minnesota J. L. Sci. & Tech.	Minnesota Journal of Law, Science & Technology
Minnesota L. Rev.	Minnesota Law Review
MMR	MultiMedia und Recht
MPEPIL	Max Planck Encyclopedia of Public International Law
NJW	Neue Juristische Wochenschrift
Nordic J. Int'l. L.	Nordic Journal of International Law
North Carolina J. Int'l. L. & Comm. Reg.	North Carolina Journal of International Law and Commercial Regulation
Northwestern University L. Rev.	Northwestern University Law Review
Notre Dame L. Rev.	Notre Dame Law Review
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NYIL	Netherlands Yearbook of International Law
NZA	Neue Zeitschrift für Arbeitsrecht
NZKart	Neue Zeitschrift für Kartellrecht
OAS	Organization of American States
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
ÖJZ	Österreichische Juristen-Zeitung
RdC	Recueil des Cours
RDV	Recht der Datenverarbeitung
RIW	Recht der internationalen Wirtschaft
SRIEL	Swiss Review of International and European Law
StIGH	Ständiger Internationaler Gerichtshof
Stan. J. Int'l. L.	Stanford Journal of International Law
Stan. L. Rev.	Stanford Law Review
Texas Int'l. L. J.	Texas International Law Journal
Texas L. Rev.	Texas Law Review
U. Chicago Legal F.	University of Chicago Legal Forum
U. Cincinnati L. Rev.	University of Cincinnati Law Review
UNO	Vereinte Nationen
UNSWLRS	University of New South Wales Law Research Paper
U. Pennsylvania L. Rev.	University of Pennsylvania Law Review
U. Pittsburgh L. Rev.	University of Pittsburgh Law Review
Utrecht J. Int'n'l. & Europ. L.	Utrecht Journal of International and European Law
Vand. J. Transn'l. L.	Vanderbilt Journal of Transnational Law
Vand. L. Rev.	Vanderbilt Law Review
Vill. L. Rev.	Villanova Law Review
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
Wayne L. Rev.	Wayne Law Review
WuW	Wirtschaft und Wettbewerb
Yale J. Int'l. L.	Yale Journal of International Law
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht
ZD	Zeitschrift für Datenschutz
ZEuP	Zeitschrift für Europäisches Privatrecht
ZfWG	Zeitschrift für Wett- und Glücksspielrecht

ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
ZÖR	Zeitschrift für öffentliches Recht
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht
ZVglRWiss	Zeitschrift für Vergleichende Rechtswissenschaft

Einführung

„One of the most significant challenges that twenty-first century information societies face is the task of reconciling the societal benefits offered by new information and communications technologies with the protection of fundamental rights such as the right to privacy.”

Joseph A. Cannataci, Special Rapporteur on the right to privacy¹

A. Notwendigkeit von Datenschutz in Zeiten von Big Data

Die rasanten technischen Entwicklungen der vergangenen Jahrzehnte haben die Gesellschaft in vielerlei Hinsicht verändert. Computer, Smartphones, Tablets und Smartwatches, internetfähige Fernseher und Smart Home-Steuerungen sind für viele Menschen zu wichtigen Bestandteilen des täglichen Lebens geworden. Sie bestimmen nicht nur den privaten Alltag mit, sondern prägen mittlerweile auch das Berufsleben in nahezu jedem Bereich. Die Geräte digitalisieren, automatisieren und ökonomisieren Vorgänge. Sie unterstützen dabei, menschliche Fehler zu vermeiden oder jedenfalls zu minimieren. Sie haben neue Formen der Kommunikation entstehen lassen. Mit ihrer Hilfe können sich Personen aus der ganzen Welt in Sekundenschnelle miteinander verbinden. Und wie sich an der Entwicklung künstlicher Intelligenz zeigt, schaffen es Algorithmen sogar, den digitalen Fortschritt selbst weiter voranzutreiben. Kurzum: Die Technologisierung und Digitalisierung des Lebens haben dem Menschen immense Vorteile gebracht.

Wichtige Motoren der Entwicklung sind einige weltweit führende Tech-Konzerne. Google, Amazon, Facebook, Apple und Microsoft beherrschen den digitalen Weltmarkt.² Angetrieben sind die Akteure von visionären Ideen, mit

¹ *Special Rapporteur on the right to privacy*, Report, UN Doc. A/72/43103 v. 19.10.2017.

² Die Unternehmen werden als die „Großen Fünf“ bezeichnet, vgl. <https://netzpolitik.org/2018/ein-leben-ohne-apple-microsoft-google-facebook-und-amazon/>; gelegentlich wird auch unter Nichtberücksichtigung von Microsoft nur von den „Großen Vier“ gesprochen, vgl. *S. Galloway*, *The four: Die geheime DNA von Amazon, Apple, Facebook und Google* (2018); um die Dominanz der vier Unternehmen zum Ausdruck zu bringen, wird häufig entsprechend der Initialien der Unternehmen von „GAFA“ gesprochen, vgl. *J. Bott/U. Milkau*, *The Development of Digital Business Platforms as a Challenge for Regulation* (2019), S. 6.

denen sie es geschafft haben, sich von kleinen Startups zu den mächtigsten und wertvollsten Unternehmen der Welt zu entwickeln. Abgesehen von den Börsenwerten³ spiegelt sich ihre beherrschende Rolle darin wider, dass sie zahllose Daten von Personen verarbeiten, die ihre Dienste nutzen. Faktisch betrifft das nahezu jeden Menschen, denn mittlerweile ist es schier unmöglich geworden, den Angeboten und Dienstleistungen der Unternehmen auszuweichen.⁴

Personenbezogene Daten sind für die Konzerne in unserem heutigen *Big Data*-Zeitalter zu einer wichtigen Geschäftsgrundlage geworden.⁵ Zu Recht werden sie insoweit als „*the new oil and the new currency of the digital world*“ bezeichnet.⁶ Wie die sog. „Fünf V“ von „Big Data“ zum Ausdruck bringen, versprechen riesige Datenmengen Erkenntnisgewinne und Innovation. Durch Big Data können zahllose Daten („*volume*“) unterschiedlicher Art und Qualität („*variety*“) in hoher Geschwindigkeit („*velocity*“) verarbeitet, auf ihre Stimmigkeit hin geprüft („*veracity*“) und für eine neue Wertschöpfung verwendet werden („*value*“).⁷ Dies kommt nicht nur der Wirtschaft selbst, sondern auch der Gesellschaft zugute.

Die Verarbeitung personenbezogener Daten ist aus Sicht der hiervon betroffenen Datensubjekte nicht ganz unbedenklich. Insbesondere das Persönlichkeitsrecht des Einzelnen ist erheblich in Gefahr, wenn Daten von Dritten

³ Vgl. <https://www.handelsblatt.com/finanzen/anlagestrategie/trends/apple-google-amazon-das-sind-die-zehn-wertvollsten-unternehmen-der-welt/22856326.html>.

⁴ Vgl. dazu den Selbstversuch der Journalistin *K. Hill*: <https://www.sueddeutsche.de/digital/amazon-facebook-apple-google-microsoft-1.4304826>.

⁵ Vgl. zum Begriff des „Big Data“-Zeitalters: *V. Mayer-Schönberger/K. Cukier*, *Big Data: Die Revolution, die unser Leben verändern wird* (2013).

⁶ *M. Kuneva* (EU-Kommissarin für Verbraucherschutz), Vortrag vom 31.3.2009, *Speech/09/156*, abrufbar unter: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm; diese Metapher wird aufgenommen von *R. Büst*, *Daten sind das neue Öl*, *Wirtschaftsinformatik & Management* 2013, 40 (41); *B. Braun*, *Daten als „Öl des 21. Jahrhunderts“*, *Controlling & Management Review* 58 (2014), 88; *T. Bauernhansl*, *Digitalisierung – Daten als Rohstoff der Zukunft?!*, Vortrag Siemens Wirtschaftsforum (16.9.2014), vgl. http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-3198080.pdf; *P. Otto*, *Leben im Datenraum – Handlungsauftrag für eine gesellschaftlich sinnvolle Nutzung von Big Data*, in: *H. Hill/D. Kugelmann/M. Martini* (Hrsg.), *Perspektiven der digitalen Lebenswelt* (2017), 9 (18); *M. Martini*, *Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht*, *DVBl.* 2014, 1481 (1482).

⁷ Vgl. *W. Hoffmann-Riem*, *Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data*, in: *ders.* (Hrsg.), *Big Data – Regulative Herausforderungen* (2018), 11 (19 f.).

erhoben und zu Wertschöpfungs Zwecken verwendet werden.⁸ Personenbezogene Daten verkörpern Informationen über Individuen.⁹ Sie lassen Einblicke in ihre persönlichen und sachlichen Verhältnisse zu und können damit nicht nur Aufschluss über das Verhalten, den Aufenthaltsort oder etwaige Ortswechsel von Personen geben, sondern auch über ihre Arbeitsleistung und Zuverlässigkeit, ihre wirtschaftliche Lage, ihre Gesundheit sowie persönliche Vorlieben und Interessen.¹⁰ Sie können folglich nicht nur äußere Tatsachen, sondern auch intime Details eines Menschen offenbaren.¹¹ Das gilt umso mehr, als sich verschiedene Daten mosaikartig zu einem Profil zusammensetzen lassen, das umso facettenreicher wird, je mehr Informationen über eine Person vorliegen.¹² Die Datensubjekte werden dadurch gläsern und zugleich beeinflussbar.¹³

Es verwundert deswegen kaum, dass die Akteure zunehmend in den Fokus einer datenschutzrechtlichen Regulierung durch unterschiedliche Hoheitsträger und Behörden, vor allem aus der EU, geraten sind.¹⁴ Diese stehen in der

⁸ Vgl. *W. Hoffmann-Riem*, Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: ders. (Hrsg.), *Big Data – Regulative Herausforderungen* (2018), 11 (27); *ders.*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, *JZ* 69 (2014), 53 f.; *B. P. Paal/M. Hennemann*, Big Data im Recht, *NJW* 2017, 1697 (1700 f.); *J.-P. Ohrtmann/S. Schwiering*, Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, *NJW* 2014, 2984.

⁹ Vgl. nur die Definition des Art. 4 Nr. 1 DSGVO; personenbezogene Daten sind danach „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“.

¹⁰ Vgl. Art. 4 Nr. 4 DSGVO.

¹¹ Die EU-Kommissarin für Justiz, Verbraucherschutz und Gleichstellung, *V. Jourová*, drückt dies mit den Worten aus: „When it comes to personal data today, people are naked in an aquarium“, Pressemitteilung v. 24.5.2018, abrufbar unter: http://europa.eu/rapid/press-release_STATEMENT-18-3889_en.htm.

¹² Vgl. EuGH (GK), Urt. v. 8.4.2014, Rs. C-293/12 u.a. – *Digital Rights Ireland*, Rn. 26 f., 37; *Special Rapporteur on the right to privacy*, Report, UN Doc. A/HRC/31/64 v. 24.11.2016, Rn. 8; *Council of Europe*, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling v. 25.11.2010.

¹³ Vgl. dazu schon die Aussage in BVerfGE 65, 1 (42) in Bezug auf eine staatliche Datenerhebung; gleiches gilt, wenn die Datenerhebung von privater Seite erfolgt, vgl. dazu näher unten Kap. 2, A.II.; s. auch *W. Hoffmann-Riem*, Freiheitsschutz in den globalen Kommunikationsinfrastrukturen, *JZ* 69 (2014), 53 f.; *V. Boehme-Neßler*, Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, *NVwZ* 2014, 825 (826); zu konkreten Beispielen einer Verhaltenssteuerung vgl.: *W. Hoffmann-Riem*, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, *AÖR* 142 (2017), 1 (11 ff.); *P. Richter*, Die Wahl ist geheim... so what? Big Data Mining im US-Wahlkampf. Und hier?, *DÖV* 2013, 961.

¹⁴ Vgl. dazu schon die zahlreichen bekannt gewordenen Fälle der jüngeren Zeit: EuGH (GK), Urt. v. 13.5.2014, Rs. C-131/12 – *Google Spain*; EuGH, Urt. v. 1.10.2015, Rs. C-230/14 – *Weltimmo*; EuGH, Urt. v. 28.7.2016, Rs. C-191/15 – *Verein für Konsumenten*