Recht der Informationsgesellschaft 36

Johanna Heberlein

Datenschutz im Social Web

Materiell-rechtliche Aspekte der Verarbeitung personenbezogener Daten durch Private in sozialen Netzwerken

Nomos

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Recht der Informationsgesellschaft

herausgegeben von

Prof. Dr. Jörg Fritzsche, Universität Regensburg, Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht
Prof. Dr. Jürgen Kühling, LL.M., Universität Regensburg, Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht
Prof. Dr. Gerrit Manssen, Universität Regensburg, Lehrstuhl für Öffentliches Recht, insbesondere deutsches und europäisches Verwaltungsrecht
Prof. Dr. Robert Uerpmann-Wittzack, Maître en droit, Universität Regensburg, Lehrstuhl für Öffentliches Recht und Völkerrecht

Band 36

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Johanna Heberlein

Datenschutz im Social Web

Materiell-rechtliche Aspekte der Verarbeitung
personenbezogener Daten durch Private in sozialen Netzwerken

Nomos

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Gefördert durch einen Druckkostenzuschuss der Frauenbeauftragten der Fakultät für Rechtswissenschaft der Universität Regensburg im Rahmen des finanziellen Anreizsystems zur Förderung der Gleichstellung.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Regensburg, Univ., Diss., 2017

ISBN 978-3-8487-4607-1 (Print)

ISBN 978-3-8452-8773-7 (ePDF)

Die Bände 1 bis 33 sind im Lit-Verlag erschienen.

1. Auflage 2017
© Nomos Verlagsgesellschaft, Baden-Baden 2017. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2017 von der Fakultät für Rechtswissenschaft der Universität Regensburg als Dissertation angenommen.

Besonderer Dank gebührt meinem Doktorvater, Herrn Prof. Dr. Jürgen Kühling, LL.M.. Die Tätigkeit als wissenschaftliche Mitarbeiterin an seinem Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht hat mir sehr viel Freude bereitet und mich fachlich wie persönlich bereichert. Als Lehrstuhlinhaber und Doktorvater hat Herr Prof. Dr. Kühling stets ein offenes Ohr für seine Mitarbeiter/-innen und ist jederzeit als kompetenter Ansprechpartner für fachliche Fragen zugänglich. Für diese hervorragende Betreuung und wissenschaftliche Förderung bedanke ich mich herzlich.

Herrn Prof. Dr. Robert Uerpmann-Wittzack danke ich vielmals für die zügige Erstellung des Zweitgutachtens und vertiefende Hinweise zur Bearbeitung. Ein großes Dankeschön geht zudem an Frau Prof. Elizabeth DeArmond für die engagierte Betreuung während eines Forschungsaufenthalts am IIT Chicago-Kent College of Law zu US-amerikanischem Datenschutzrecht. Desweiteren bedanke ich mich bei der Frauenbeauftragten der Fakultät für Rechtswissenschaft der Universität Regensburg, Frau Prof. Dr. Katrin Gierhake, LL.M., für die Förderung der Veröffentlichung durch einen Druckkostenzuschuss.

Außerordentlicher Dank gebührt meinem persönlichen Umfeld, aus dem mir in vielfältiger Weise Unterstützung zuteilwurde und das dazu beigetragen hat, dass ich an die Promotionszeit stets gerne zurückdenken werde: Nicht genug danken kann ich Cornelia Kibler, LL.M. (UNC) und Alexandra Hehr für viele bereichende wissenschaftliche Diskussionen und den jederzeitigen Beistand während der gesamten Zeit der Bearbeitung. Für die zügige Korrekturlektüre sowie den durchweg ermunternden Zuspruch bin ich Helen Obermeier zu Dank verpflichtet. Dankend erwähnt sei auch Dr. Claudia Busch, die mir immer mit gutem Rat zur Seite stand.

Mein größter Dank gilt meinem Freund Peter. Sein steter liebevoller Rückhalt und sein aufrichtiges Interesse an dem Projekt verhalfen der Arbeit ganz wesentlich zu einem erfolgreichen Abschluss.

Regensburg, im Oktober 2017 *Johanna Heberlein*

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Inhaltsverzeichnis

Abkürzungsverzeichnis 19

Einleitung und Gang der Untersuchung 25

A. Problemaufriss 25
B. Gang der Untersuchung 28

Kapitel 1: Grundlagen 31

A. Hinweis zur rechtlichen Terminologie 31
B. Soziale Netzwerke und zentrale Funktionen 33
I. Klassifikation der Plattformen 33
II. Vorstellung ausgewählter Plattformen 34
1. Facebook 35
2. Instagram 36
3. Twitter 36
4. Snapchat 37
C. Finanzierung sozialer Netzwerke 37
I. Finanzierung durch Werbung 38
II. Technische Trackingmethoden 40
1. Cookies 41
2. Fingerprinting 43
III. Zusammenfassung 43
D. Überblick über grundrechtliche Interessenpositionen 44
I. Betroffeneninteressen 44
1. Das Recht auf informationelle Selbstbestimmung 44
2. Schutz personenbezogener Daten 45
II. Verarbeiter- und Drittinteressen 46
1. Berufsfreiheit und unternehmerische Freiheit 46
2. Meinungs- und Informationsfreiheit 47
III. Zusammenfassung 48

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kapitel 2: Territorial anwendbares Recht 49

A. Problemaufriss 49
B. Datenschutzrechtliche Vorgaben der DSRL 51
I. Für die Verarbeitung Verantwortlicher i. S. d. Art. 4 Abs. 1 DSRL 53
1. Verantwortlichkeit bei mehreren Niederlassungen 54
2. Konsequenzen am Beispiel von *Facebook* 55
3. Zulässigkeit einer rechtlichen Zuweisung der Verantwortlichkeit 58
II. Niederlassung i. S. d. Art. 4 Abs. 1 lit. a DSRL 59
1. Merkmale des Niederlassungsbegriffs 60
a) Vorliegen einer festen Einrichtung 60
b) Effektive und tatsächliche Ausübung einer Tätigkeit 61
c) Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung i. S. d. Art. 4 Abs. 1 lit. a DSRL 62
2. Territorial anwendbares Recht innerhalb der EU bei mehreren Niederlassungen 64
a) Abgrenzung mitgliedstaatlicher Datenschutzregimes als Folgefrage 64
b) Übertragbarkeit der Auslegung des Art. 4 Abs. 1 lit. a DSRL auf rein innereuropäische Sachverhalte 65
aa) Keine Beschränkung auf Drittlandsachverhalte durch den Wortlaut des Art. 4 Abs. 1 lit. a DSRL 66
bb) Keine Beschränkung auf Drittlandsachverhalte durch die *EuGH*- Rechtsprechung 66
i) Keine Beschränkung durch *Google* Spain und Weltimmo 66
ii) Keine Beschränkung durch Verein für Konsumenteninformation 67
cc) Zwischenergebnis 69
c) Abgrenzung mitgliedstaatlicher Datenschutzregimes bei innereuropäischen Sachverhalten 69
aa) Anwendbarkeit nationaler Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben Verantwortlichen 70
bb) Anwendbarkeit nationaler Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben Verarbeitungsvorgang 72
i) Definition „desselben" Verarbeitungsvorgangs 73

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ii) Abgrenzung anhand des Merkmals der „engsten Verknüpfung“ 74
iii) Die Ausrichtung auf den Mitgliedstaat als weiterer Anknüpfungspunkt 76
iv) Konfligierende Datenschutzregimes 77
d) Zwischenergebnis 78
III. Rückgriff auf Mittel i. S. d. Art. 4 Abs. 1 lit. c DSRL 79
1. Keine Niederlassung in der EU 79
2. Rückgriff auf im Mitgliedstaat belegene Mittel 80
C. Änderungen durch die DSGVO 83
I. Verarbeitung personenbezogener Daten nach Vorgabe der DSGVO 83
II. Keine spezifische Kollisionsnorm bei der Aktivierung von Öffnungsklauseln 85
D. Territorial anwendbares Recht im Nutzer-Nutzer-Verhältnis 88
E. Fazit 89

Kapitel 3: Datenschutzrechtliche Bewertung der Verarbeitung personenbezogener Daten in sozialen Netzwerken 92

A. Zulässigkeit der Verarbeitung personenbezogener Daten im Nutzer-Nutzer-Verhältnis 92
I. Datenverarbeitung ausschließlich zu persönlichen oder familiären Tätigkeiten 93
1. Öffentliche Inhalte 93
a) BDSG bzw. DSRL 93
b) DSGVO 94
2. Beschränkung auf bestimmte Personengruppen 95
a) BDSG bzw. DSRL 95
b) DSGVO 96
3. Datenverarbeitung mittels der Nutzung von Nachrichtenfunktionen 97
II. Nutzer als Verantwortlicher 97
1. Betreiber privater Profile 98
2. Betreiber öffentlicher Profile 99
a) Funktionsweise von öffentlichen Profilen am Beispiel von *Facebook* 100
b) Verantwortlichkeit der Fanpage-Betreiber 101
aa) Datenschutzrechtliche Verantwortlichkeit 102
bb) Verantwortlichkeit i. S. d. TMG 103
c) Fanpages als Form der Auftragsverarbeitung 104
d) Fanpagebetreiber als Auswahlverantwortliche 105

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aa) Auswahlverantwortlichkeit als Teil der Auftragsverarbeitung 105
bb) Grundrechtliche Implikationen der Auswahlverantwortlichkeit 107
cc) Zumutbarkeit der Auswahlverantwortlichkeit 108
e) Zusammenfassung 109
III. Zulässigkeit der Verarbeitung von Informationen Anderer 110
1. Rechtliche Einordnung 111
2. Zulässigkeit des Hochladens bzw. Teilens von Informationen Anderer durch Erlaubnistatbestände 113
a) Zulässigkeit nach dem BDSG 113
aa) Abgrenzung zwischen § 28 und § 29 BDSG 113
i) Übermittlung als Zweck der Verarbeitung 113
ii) Geschäftsmäßigkeit des Hochladens und Teilens 114
iii) Fehlen der Geschäftsmäßigkeit 115
(1) Kein Rückgriff auf § 28 BDSG bei Fehlen der Geschäftsmäßigkeit 116
(2) Anwendbarkeit des § 29 BDSG bei Fehlen der Geschäftsmäßigkeit 116
bb) Erlaubnistatbestände in § 29 BDSG 117
i) Allgemein zugängliche Beiträge, § 29 Abs. 1 S. 1 Nr. 2 BDSG 117
ii) Nicht allgemein zugängliche Beiträge, § 29 Abs. 1 S. 1 Nr. 1 BDSG 119
iii) Zulässigkeit der Übermittlung i. S. d. § 29 Abs. 2 BDSG 120
(1) Historischer Ursprung der Norm 120
(2) Verfassungskonforme Auslegung durch den BGH 121
(3) Vereinbarkeit des § 29 Abs. 2 S. 1 Nr. 1 BDSG mit Art. 7 lit. f DSRL 122
(4) Zwischenergebnis 123
iv) Zusammenfassung 123
b) Zulässigkeit nach der DSRL 123
c) Zulässigkeit nach der DSGVO 125
aa) Art. 6 Abs. 1 S. 1 lit. f DSGVO als umfassende Erlaubnisnorm 125
bb) Maßstab des Art. 6 Abs. 1 S. 1 lit. f DSGVO 127

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

i) Berechtigtes Interesse des Datenverarbeiters oder eines Dritten 128
ii) Betroffeneninteressen 128
iii) Abwägung 129
3. Zulässigkeit der Verarbeitung von Informationen Anderer durch Einwilligung 130
a) Voraussetzungen der Zulässigkeit nach dem BDSG bzw. der DSRL 131
aa) Freiwilligkeit 131
i) Imagepflege durch Interaktion in sozialen Online-Netzwerken 132
ii) Soziale Online-Netzwerke und Suchterkrankungen 134
iii) Auswirkungen auf die Freiwilligkeit der datenschutzrechtlichen Einwilligungserklärung 135
(1) Auswirkungen von sozialem Druck auf die Wirksamkeit der Einwilligung 135
(2) Auswirkungen von Abhängigkeitserkrankungen auf die Wirksamkeit der Einwilligung 136
iv) Zwischenergebnis 137
bb) Informiertheit und Bestimmtheit 138
cc) Schriftformerfordernis 138
i) Schriftformerfordernis als Grundsatz im BDSG 138
ii) Vereinbarkeit des Schriftformerfordernisses mit den Vorgaben der DSRL 139
iii) Nutzereinstellungen als konkludente Einwilligungserklärung 141
b) Voraussetzungen der Zulässigkeit nach der DSGVO 142
IV. Zulässigkeit der Verarbeitung von Fotos Anderer 143
1. Divergierende Zulässigkeitsvoraussetzungen i. S. d. KUG und BDSG/DSRL sowie DSGVO 144
2. Sachlicher Anwendungsbereich des KUG 145
a) Bildnis 146
b) Verbreiten oder öffentliches Zurschaustellen 146
aa) Verbreiten 146
bb) Öffentliches Zurschaustellen 147
3. Verhältnis KUG und BDSG 149
a) KUG als Spezialgesetz 149

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Ansätze zur Auflösung des Spannungsverhältnisses 150
aa) Übertragbarkeit der Grundsätze des BDSG auf das KUG und vice versa 150
bb) Verfassungskonforme Auslegung des KUG 151
4. Verhältnis KUG und DSGVO 152
V. Zusammenfassung 153
B. Zulässigkeit der Verarbeitung personenbezogener Daten im Anbieter-Nutzer-Verhältnis 154
I. Gesetzliche Erlaubnistatbestände 154
1. Sachlich anwendbares Recht 154
a) Sachlich anwendbares Recht im deutschen Datenschutzrecht 154
aa) Grundsätzliche Unterschiede der Zulässigkeitsnormen 155
bb) Unvereinbarkeit der § 14 Abs. 1 und § 15 Abs. 1 TMG mit der DSRL 156
cc) Konsequenzen der Unvereinbarkeit mit der DSRL 157
dd) Klassifikation als Bestands-, Nutzungs-, oder Inhaltsdatum 158
i) Bestandsdaten 159
ii) Nutzungsdaten 160
iii) Inhaltsdaten 160
ee) Zwischenergebnis 162
b) Sachlich anwendbares Recht unionsrechtlicher Normen 162
2. Verarbeitung von Angaben durch den Nutzer selbst 163
a) Registrierungsdaten 163
aa) Zulässigkeit des Datenumgangs nach dem BDSG bzw. der DSRL 164
i) Abgrenzung zwischen § 28 und § 29 BDSG 164
ii) Zulässigkeit gem. § 28 Abs. 1 BDSG bzw. Art. 7 DSRL 164
bb) Zulässigkeit der Datenverarbeitung nach der DSGVO 167
b) Weitere vom Nutzer selbst preisgegebene personenbezogene Daten 169
aa) Zulässigkeit nach dem BDSG 169
i) Zulässigkeit zu Zwecken der Funktionalität des sozialen Netzwerks 170

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ii) Zulässigkeit der Datenverwendung zu Werbezwecken 170
(1) Keine Generalerlaubnis durch § 28 Abs. 1 S. 1 BDSG 170
(2) Privilegierung der Datenverwendung i. S. d. § 28 Abs. 3 BDSG 171
(a) Verarbeitung und Nutzung bei Einwilligung 171
(b) „Listenprivileg" i. S. d. § 28 Abs. 3 S. 2 BDSG 171
(c) Nutzung für fremde Angebote i. S. d § 28 Abs. 3 S. 5 BDSG 172
(d) Übermittlung an Dritte 173
bb) Zulässigkeit nach der DSGVO 174
3. Verarbeitung von mittels Tracking Tools erhobenen Daten 175
a) RL 2002/136/EG bzw. RL 2009/136/EG 175
aa) Sachlicher Anwendungsbereich hinsichtlich Cookies 176
bb) Sachlicher Anwendungsbereich hinsichtlich anderer Tracking Tools 176
cc) Vorgaben der ePrivacy-RL für den Einsatz von Tracking Tools 177
dd) Umsetzung in deutsches Recht 178
b) Entwurf einer ePrivacy-VO 180
II. Zulässigkeit der Verarbeitung durch Einwilligung 182
1. Inhaltliche Anforderungen 182
a) Freiwilligkeit 182
aa) Koppelungsverbot i. S. d. § 28 Abs. 3b BDSG 183
i) Nutzerinteressen als Maßstab für die Gleichwertigkeit 183
ii) Zumutbarkeit 184
iii) Strenger Maßstab bei Minderjährigen 185
bb) Koppelungsverbot i. S. d. Art. 7 Abs. 4 DSGVO als Auslegungskriterium 186
b) Informiertheit und Bestimmtheit 189
2. Anforderungen an die Form, insbesondere elektronische „opt-in"-Einwilligung 190
a) Formvorgaben des TMG und BDSG 190
b) Formvorgaben der DSGVO 191
c) Formvorgaben bei Tracking Tools 192

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aa) Formvorgabe durch die ePrivacy-RL als Ergänzung zur DSRL 192
bb) Formvorgabe durch den ePrivacy-VO-E 193
3. Einwilligung eines Kindes i. S. d. DSGVO 194
a) „Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird“ 195
b) Prüfpflichten und Umsetzbarkeit 196
III. Zusammenfassung 198
C. Zulässigkeit der Verarbeitung personenbezogener Daten durch Dritte am Beispiel von Social Plug-Ins 199
I. Verantwortlichkeit der Websitebetreiber am Beispiel des „Like-Buttons“ 201
1. Entscheidung über das „Ob“ und „Wie“ der Verarbeitung 201
2. Gewichtung des „Ob“ und „Wie“ der Verarbeitung 203
3. Keine Auftragsverarbeitung durch den „Like-Button“ 205
4. Websitebetreiber und Plug-In-Anbieter als Dienstanbieter i. S. d. TMG 205
5. Zwischenergebnis 206
II. Zulässigkeit der Einbindung von Social Plug-Ins am Beispiel von *Facebooks* „Like-Button“ 207
1. Zulässigkeit durch gesetzlichen Erlaubnistatbestand 207
a) Zulässigkeit nach dem BDSG und dem TMG 207
aa) Zulässigkeit nach dem BDSG 208
bb) Zulässigkeit nach dem TMG 209
b) Zulässigkeit nach der DSGVO und dem ePrivacy-VO-E 210
2. Erlaubnis durch Einwilligung 211
a) Richtiger Empfänger der Einwilligungserklärung 211
b) Keine Einwilligung durch *Facebooks* AGB 211
c) Ausgestaltung der Einwilligungserklärungen 212
3. Umfang der Betroffenenrechte 215
III. Zusammenfassung 216
D. Betroffenenrechte und Durchsetzbarkeit 216
I. Betroffenenrechte im BDSG und Änderungen durch die DSGVO 216
1. Betroffenenrechte im BDSG 216
2. Änderungen durch die DSGVO 217
a) Betroffenenrechte bei der Verarbeitung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO 217
aa) Widerspruchsrecht, Art. 21 DSGVO 218

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

i) Verschobener Abwägungsmaßstab, Art. 21 Abs. 1 S. 1 DSGVO 218
ii) Widerspruchsgründe und entgegenstehende Verarbeiterinteressen, Art. 21 Abs. 1 S. 1 DSGVO 218
iii) Widerspruch bei Verarbeitung zu Zwecken der Direktwerbung, Art. 21 Abs. 1 S. 2 DSGVO 219
bb) Löschpflichten, Art. 17 DSGVO 219
b) Recht auf Datenübertragbarkeit 220
aa) Zielsetzung des Art. 20 DSGVO 220
bb) Schwierigkeiten der Umsetzbarkeit 221
i) Unterschiedliche Strukturen der sozialen Netzwerke 221
ii) Praktische Umsetzbarkeit hinsichtlich Daten Dritter 221
cc) Art. 20 DSGVO als Erweiterung des Auskunftsrechts 222
3. Beschränkungen der DSGVO-Betroffenenrechte durch nationales Recht 223
a) Änderungen im BDSG-neu 223
b) Reichweite der Öffnungsklausel des Art. 23 Abs. 1 DSGVO 225
II. Durchsetzbarkeit des Datenschutzrechts 227
1. Aufsichtsbehörden 227
a) Rolle der Aufsichtsbehörden 227
b) Zuständigkeit bei grenzüberschreitenden Sachverhalten 228
aa) Zuständigkeit nach der DSRL 228
bb) Zuständigkeit nach der DSGVO 229
2. Sanktionen 230
3. Datenschutz-Folgenabschätzung 230
4. Zivilrechtliche Durchsetzung 232
a) Durchsetzung im nationalen Recht 232
b) Durchsetzung in der DSGVO 233
c) Änderungen hinsichtlich der gerichtlichen Zuständigkeit 234
III. Zusammenfassung 235

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kapitel 4: Rechtsvergleich mit den USA vor dem Hintergrund des Datentransfers in die USA 237

A. Verfassungsrechtliche Grundlagen 239
I. Das right to privacy und right to information privacy 239
1. Entwicklung des right to privacy 239
2. Das right to information privacy 241
II. Das vierte Amendment 243
1. Durchsuchung oder Beschlagnahme 243
a) Schutzobjekt des vierten Amendments 243
b) Reasonable expectation of privacy-Test 245
aa) Die third party-doctrine als Ausschlussgrund 245
bb) Schutz von Daten auf mobilen Endgeräten 246
2. Willkürliche („unreasonable“) Durchsuchung oder Beschlagnahme 248
a) Einwilligung durch den Gesprächspartner (misplaced trust-doctrine) 248
b) Einwilligung in die Durchsuchung 249
c) Weitere Ausnahmen 249
III. Das fünfte Amendment 250
1. Vergleichbarkeit mit Zeugenaussagen 251
2. Die foregone conclusion-doctrine als Ausschlussgrund 251
IV. Erstes Amendment 252
B. Einfachgesetzliche Regelungen 253
I. Datenschutzrechtliche Bestimmungen im Anbieter-Nutzer-Verhältnis 254
1. Datenschutzrechtliche Bestimmungen hinsichtlich Tracking Tools 255
a) Wiretap Act 255
aa) Datenerhebung mittels Tracking Tools 255
i) Kommunikationsbegriff (“communication“) 256
ii) Abfangen von Inhalten 257
(1) Abfangen 257
(2) Inhalte 257
iii) Die one consent-rule als Hindernis der Durchsetzbarkeit 258
bb) Datenverwendung und Datenweitergabe 259
b) Stored Communications Act 259
aa) Platzieren von Cookies 259
i) Einrichtung i. S. d. Norm 260
ii) Elektronische Speicherung 261

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

iii) Ausschluss durch die one consent-rule 261
bb) Weitergabe von gespeicherten Nachrichten 262
c) Deliktsrecht 263
aa) Intrusion upon seclusion 263
bb) Appropriation of name or likeness 264
2. Datenschutzrechtliche Bestimmungen hinsichtlich vom Nutzer selbst bereitgestellter Daten 265
3. Regulierung durch die Federal Trade Commission 267
a) „Unfair and deceptive“ 268
b) Datenschutzrechtliche Durchsetzung durch die FTC 268
c) Einwilligung nach den fair information practice-Grundsätzen 269
4. Weitere datenschützende Normen 271
a) Computer Fraud and Abuse Act 271
b) Regelungen für Kinder: Children's Online Privacy Protection Act 272
II. Datenschutzrechtliche Bestimmungen im Nutzer-Nutzer-Verhältnis 273
1. Public disclosure of private facts 273
2. Stored Communicatios Act 275
III. Zusammenfassung 275
C. Datentransfer in die USA 276
I. Die Angemessenheit des Schutzniveaus 277
1. Auslegung durch den *EuGH* 277
2. Konsequenzen der Auslegung durch den *EuGH* 278
3. Beurteilungsmaßstab der DSGVO 278
II. Regelungen für den Transfer in die USA 279
1. Safe Harbor-Entscheidung der Kommission 280
a) System der Selbstzertifizierung 280
b) Grundsätze und Ungültigkeit 281
2. EU-U.S.-Privacy Shield 282
a) Grundsätze 282
b) Kritische Würdigung der Änderungen durch das EU-U.S.-Privacy Shield 283
aa) Ausnahmen vom EU-U.S.-Privacy Shield und Begrenzung behördlicher Zugriffe 283
bb) Wirksame Rechtsbehelfe 284
cc) Anforderungen des Art. 25 Abs. 6 DSRL 285
III. Zusammenfassung 286
1. Keine Datentransfers in die USA als drohende Konsequenz 286
2. Notwendigkeit ausgewogener Interessenabwägungen 287

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

3. Achtung gegenseitiger Interessen bei bilateralen Vereinbarungen 288
D. Fazit 288

Schlussbetrachtungen 290

A. Entterritorialisierte Sachverhalte als Herausforderung des Datenschutzrechts 290
I. Einführung des Marktortprinzips in der DSGVO 290
II. Datenfluss in die USA als Folge der Datenverarbeitung in sozialen Netzwerken 291
B. Der Nutzer als Verantwortlicher (nur) für die eigene Datenverarbeitung 293
C. Die DSGVO als Pfadbereiter für ein vollzugstarkes Datenschutzrecht 294
I. Von der DSRL zur DSGVO: Altbekannte Prinzipien mit neuen Vollzugsmöglichkeiten 294
II. Vom deutschen Datenschutzrecht zur DSGVO 295
1. Ende der bereichsspezifischen Zersplitterung bei Datenverarbeitungen durch Private 295
2. Art. 6 Abs. 1 S. 1 lit. f DSGVO als allumfassender Legitimationstatbestand 296
3. Gleichbleibende Bedeutung der Einwilligung 297
III. Modifikationen der DSGVO-Regelungen durch das BDSG-neu 298
IV. Ablösung der ePrivacy-RL durch eine ePrivacy-VO 299
V. Ausblick: Notwendigkeit einer raschen Konturierung der Zulässigkeitstatbestände 300
D. Datenschutzrecht zwischen Privaten als multipolares Grundrechtsgefüge 301

Literaturverzeichnis 302

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Abkürzungsverzeichnis

a. A.	andere Ansicht
a. E.	am Ende
AAAI	The Association for the Advancement of Artificial Intelligence
ABl.EG	Amtsblatt der Europäischen Gemeinschaften
ABl.EU	Amtsblatt der Europäischen Union
Abs.	Absatz
ACLU	American Civil Liberties Union
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
Alt.	Alternative
Anm.	Anmerkung
AöR	Archiv des öffentlichen Rechts
APA	American Psychological Association
Art.	Artikel
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BeckOK	Beck‘scher Online-Kommentar
Beschl.	Beschluss
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BMI	Bundesministerium des Innern
BR-Drucks.	Bundesratsdrucksache
BT-Drucks.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
bzw.	beziehungsweise
C.A.A.F.	United States Court of Appeals for the Armed Forces
C.D. Cal.	United States District Court for the Central District of California
C.F.R.	Code of Federal Regulations

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Cal. Pen. Code	Penal Code of California
CCS	Conference on Computer and Communications Security
CFAA	Computer Fraud and Abuse Act
Cir.	Circuit
Clin Pract Epidemiol Ment Health	Clinical Practice & Epidemiology in Mental Health
COPPA	Children's Online Privacy Protection Act
CR	Computer und Recht
d.	des/der
D. Del.	United States District Court for the District of Delaware
d. h.	das heißt
D. Mass.	United States District Court for the District of Massachusetts
D. Minn.	United States District Court for the District of Minnesota
D. Nev.	United States District Court for the District of Nevada
D. Vt.	United States District Court for the District of Vermont
D.C.	District of Columbia
D.N.J.	United States District Court for the District of New Jersey
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSGVO	Datenschutz-Grundverordnung
DSM	Diagnostic and Statistical Manual of Mental Disorders
DSRL	Datenschutzrichtlinie
DuD	Datenschutz und Datensicherheit
E	Entwurf
ECLI	European Case Law Identifier
ECPA	Electronic Communications Privacy Act
EG	Erwägungsgrund
EMRK	Europäische Menschenrechtskonvention
endg.	Endgültig
EU	Europäische Union
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWR	Europäischer Wirtschaftsraum
F. Supp.	Federal Supplement
f./ff.	die Folgende/die Folgenden
Fn.	Fußnote
FR	Federal Register
FTC	Federal Trade Commission

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

GA	Generalanwalt
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GRCh	Charta der Grundrechte der Europäischen Union
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
h. L.	herrschende Lehre
Harv. L. Rev.	Harvard Law Review
Hervorh.	Hervorhebung
Hous. L. Rev.	Houston Law Review
Hrsg.	Herausgeber(in)
Hs.	Halbsatz
HTML	Hypertext Markup Language
http	Hypertext Transfer Protocol
i. d. F.	in der Fassung
i. E.	im Ergebnis
i. H. v.	in Höhe von
i. Ü.	im Übrigen
i. S. d.	im Sinne des
i. V. m.	in Verbindung mit
ICD	International Classification of Diseases
Inc.	Incorporated
Int J Environ Res Public Health	International Journal of Environmental Research and Public Health
IP	Internet Protocol
J Appl Dev Psychol	Journal of Applied Developmental Psychology
J. Crim. L. & Criminology	Journal of Criminal Law and Criminology
J. Legal Stud.	Journal of Legal Studies
J. L. Pol'y for Info. Soc'y	Journal of Law and Policy for the Information Society
jM	juris – Die Monatszeitschrift
jurisPK	juris PraxisKommentar
K&R	Kommunikation und Recht
Kap.	Kapitel
KG	Kammergericht
KOM	Kommission
KUG	Kunsturhebergesetz
LG	Landgericht
lit.	Litera
Ltd.	Limited

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

m. Anm.	mit Anmerkung
m. w. N.	mit weiteren Nachweisen
m. W. v.	mit Wirkung von
M.D. Ala.	United States District Court for the Middle District of Alabama
M.D. Tenn.	United States District Court for the Middle District of Tennessee
M.J.	Military Justice Reporter
MdEP	Mitglied des Europäischen Parlaments
Minn.	Minnesota
Minn. Ct. App.	Minnesota Court of Appeal
Mio.	Millionen
MMR	Multimedia und Recht
Mrd.	Milliarden
N.D. Cal.	United States District Court for the Northern District of California
N.J. Super. Ct. App. Div.	New Jersey Superior Court, Appellate Divsion
nat.	national(e, -es)
NILR	Netherlands International Law Review
NJW	Neue Juristische Wochenschrift
No.	Number
Nr.	Nummer
NSDI	Symposium on Networked Systems Design and Implementation
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZA	Neue Zeitschrift für Arbeitsrecht
o. ä.	oder ähnliche(s)
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OGH	Der Oberste Gerichtshof der Republik Österreich
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
PC	Personal Computer
PETS	Privacy Enhancing Technologies Symposium
Pkt.	Punkt
RDV	Recht der Datenverarbeitung
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
S.	Satz; Seite

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

S.D.N.Y.	United States District Court for the Southern District of New York
SCA	Stored Communications Act
Sec.	Section
sog.	sogenannte(r)
stRspr	ständige Rechtsprechung
TDDSG	Teledienstedatenschutzgesetz
TMG	Telemediengesetz
u. a.	unter anderem
U. Pa. J. Const. L. Height. Scrutiny	University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny
u. U.	unter Umständen
U.S.C.	United States Code
UAbs.	Unterabsatz
UKlaG	Unterlassungsklagengesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UrhG	Urheberrechtsgesetz
UrhR	Urheberrecht
URL	Uniform Resource Locator
Urt.	Urteil
USA	Vereinigte Staaten von Amerika
USD	United States Dollars
v.	von/vom; versus
Vand. J. Transnat'l L.	Vanderbilt Journal of Transnational Law
Var.	Variante
Verf.	Verfasser(in)
VG	Verwaltungsgericht
vgl.	Vergleiche
VO	Verordnung
Vol.	Volume
Vorb.	Vorbemerkung
W.D. Tex.	United States District Court for the Western District of Texas
Wash. U. L. Rev.	Washington University Law Review
WHO	Weltgesundheitsorganisation
Wis. 2d	Wisconsin Reports, second series
WL	Westlaw
WOSN	Workshop on Online Social Networks
WP	Working Party

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Yale J. Int'l L.	Yale Journal of International Law
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Einleitung und Gang der Untersuchung

A. Problemaufriss

Diesseits wie jenseits des Atlantiks ist der Datenschutz in sozialen Netzwerken ein Thema, das mit gewisser Besorgnis diskutiert wird, teilweise gar zum Anlass für exklamatorische Weckrufe genommen wird. So zögerte eine US-amerikanische Professorin nicht, den „Tod des Datenschutzes" im Zusammenhang mit sozialen Netzwerken zu verkünden.[1] „Kämpf um deine Daten"[2] forderte indes der österreichische Datenschützer *Max Schrems* und ging mit gutem Beispiel voran: Ein Jahr später erklärte der *EuGH* die Safe Harbor-Regelungen, auf deren Grundlage ein Gros von Internet-Diensteanbietern personenbezogene Daten in die USA transferierten, für ungültig – aufgrund einer Vorlage des Irischen *High Court* zu einem von *Schrems* initiierten Rechtsstreit.[3]

Angesichts der Fakten zu sozialen Netzwerken verwundert es nicht, dass das Thema in Populär-[4] wie Fachliteratur[5] rege diskutiert wird: *Facebook* gibt an, täglich 1,32 Mrd. aktive Nutzer zu haben[6] – das entspricht einem Sechstel der Weltbevölkerung, die sich täglich in dem Netzwerk austauschen. Längst sind die Betreiber sozialer Netzwerke marktmächtige Unternehmen, teilweise mit Umsätzen in Milliardenhöhe, geworden – wobei der Umsatz durch zielgerichtete Werbeplatzierungen generiert wird.[7] Dass die

---

1 Vgl. *Andrews,* I know who you are and I saw what you did, mit dem Untertitel „Social Networks and the Death of Privacy".

2 *Schrems,* Kämpf um deine Daten.

3 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems.

4 Vgl. etwa *Kurz/Rieger,* Die Datenfresser.

5 Vgl. etwa *Piltz,* Soziale Netzwerke im Internet; *Achtruth,* Der rechtliche Schutz bei der Nutzung von Social Networks; *Kühnl,* Persönlichkeitsschutz 2.0, *Kampert,* Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda.

6 *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017).

7 Vgl. etwa *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 62 mit einem Umsatz von 27,6 Mrd. USD im Jahr 2016, davon 26,8 Mrd. durch Werbeeinnahmen; vgl. Kap. 1, Pkt. C, S. 37.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Frage nach dem Umgang mit personenbezogenen Daten durch Plattformbetreiber laut wird, liegt vor diesem Hintergrund auf der Hand.

Aber auch datenschutzrechtliche Aspekte im Umgang mit personenbezogenen Daten durch die Nutzer selbst werfen Fragen nach der Zulässigkeit dieses Umgangs auf. So ist es durchaus üblich, dass Nutzer Informationen oder Fotos nicht nur über sich selbst, sondern auch über andere in sozialen Netzwerken einem breiteren Publikum zugänglich machen.

Diese Arbeit geht den materiell-rechtlichen Aspekten der Datenverarbeitung in sozialen Netzwerken zwischen Privaten[8] nach und untersucht die Verarbeitung personenbezogener Daten durch die Nutzer selbst, durch die Plattformbetreiber und durch Dritte. Es handelt sich um eine Auseinandersetzung mit dem Thema im horizontalen Grundrechtsgefüge. Die Notwendigkeit der sorgfältigen Abwägung sich gegenüberstehender Interessen und das Ineinklangbringen dieser Interessen stellt eine besondere Herausforderung datenschutzrechtlicher Fragen zwischen Privaten dar.

Die Entterritorialisierung der in Frage stehenden Sachverhalte stellt das Datenschutzrecht vor weitere Herausforderungen: Die sozialen Netzwerke mit den höchsten deutschen Nutzerzahlen haben ihren Hauptsitz in den USA.[9] Sie entspringen damit einem Rechtssystem, das in datenschutzrechtlicher Sicht einem völlig anderen Ansatz folgt als die EU. Das wirft erstens die Frage nach dem territorial anwendbaren Recht auf. Hier stellt sich zum einen die Frage, ob sich US-amerikanische Diensteanbieter dem europäischen Datenschutzregime unterwerfen müssen und – falls ja – welchem konkreten mitgliedstaatlichen Datenschutzregime sie folgen müssen. Zum anderen muss der Frage nachgegangen werden, wie der freie Fluss personenbezogener Daten unter gegenseitiger Achtung von Grundrechten ermöglicht werden kann. Der ständige Fluss personenbezogener Daten zwischen der EU und den USA verdeutlicht paradigmatisch, dass sich datenschutzrechtliche Fragen nicht aus rein nationaler, auch nicht lediglich aus unionaler Perspektive beantworten lassen, sondern ein Blick über den Atlantik unerlässlich ist.

---

8 Vgl. zur Terminologie Kap. 1 Pkt. A, S. 31.

9 Vgl. *Statista GmbH*, Reichweite der größten Social Networks nach dem Anteil der Unique User in Deutschland im 1. Halbjahr 2016, abrufbar unter https://de.statista.com/statistik/daten/studie/157885/umfrage/reichweite-der-groessten-social-networks-in-deutschland/ (abgerufen am 13.10.2017), das *Facebook* als größtes soziales Netzwerk in Deutschland identifiziert. *Facebook* hat indes seinen Hauptsitz in Kalifornien, vgl. *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Eine Analyse der materiell-rechtlichen Aspekte der Datenverarbeitung in sozialen Netzwerken durch Private ist insbesondere aufgrund einer umfassenden Reformierung des europäischen Datenschutzes durch die Ablösung der Datenschutzrichtlinie (im Folgenden: DSRL)[10] bzw. ihrer nationalen Umsetzungsgesetze, etwa dem Bundesdatenschutzgesetz (im Folgenden: BDSG)[11] durch die unmittelbar geltende Datenschutzgrundverordnung (im Folgenden: DSGVO)[12] sowie hinsichtlich der jüngsten Entwicklungen in der *EuGH*-Rechtsprechung[13] erforderlich. Hinzukommend enthält die DSGVO zahlreiche Öffnungsklauseln, die den Mitgliedstaaten erlauben, in Teilbereichen durch nationale Regelungen von den Bestimmungen der DSGVO abzuweichen.[14] Dies betrifft zwar ganz besonders die Datenverarbeitung im öffentlichen Bereich,[15] ist jedoch im Rahmen der Betroffenenrechte, die durch nationale Gesetzgebung i. S. d. Art. 23 Abs. 1 DSGVO beschränkt werden können, auch für die vorliegende Analyse der Datenver-

10 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl.EG 1995 L 281, 31.

11 Bundesdatenschutzgesetz (BDSG). Bekanntmachung der Neufassung des Bundesdatenschutzgesetzes vom 14. Januar 2003, BGBl. 2003 I, 66.

12 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl.EU 2016 L 119, 1.

13 Exemplarisch *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google und Google Spain; *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639 – Weltimmo; *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems; *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779 – Breyer; *EuGH,* Urt. v. 04.05.2017, Rs. C-13/16, ECLI:EU:C:2017:336 – Rīgas.

14 Für eine Übersicht der Öffnungsklauseln vgl. *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 14 ff.

15 Vgl. nur die Öffnungsklausel des Art. 6 Abs. 1 S. 1 lit. e i. V. m. Abs. 2, 3 DSGVO bei Datenverarbeitungen, die zur Wahrung einer Aufgabe im öffentlichen Interesse erforderlich sind oder in Ausübung öffentlicher Gewalt erfolgen; für den im privaten Bereich relevanten Zulässigkeitstatbestand des Art. 6 Abs. 1 S. 1 lit. f DSGVO ist demgegenüber keine Öffnungsklausel vorgesehen.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

arbeitung in sozialen Netzwerken durch Private relevant. So hat der Gesetzgeber in einem „BDSG-neu“[16], das die Bestimmungen der DSGVO ergänzen wird,[17] u. a. von der genannten Öffnungsklausel des Art. 23 Abs. 1 DSGVO Gebrauch gemacht[18]. Die vorliegende Arbeit bietet daher eine Untersuchung materiell-rechtlicher Aspekte des Datenschutzes in sozialen Netzwerken gerade zum aktuellen Recht.

B. Gang der Untersuchung

Ziel der Arbeit ist es, die datenschutzrechtlichen Problemfelder im Zusammenhang mit sozialen Netzwerken herauszuarbeiten und die Zulässigkeit der Datenverarbeitung in sozialen Netzwerken im Lichte jüngster Veränderungen der Rechtslage zu bewerten. Als Referenzfall wird dabei hauptsächlich *Facebook* herangezogen, anhand dessen sich eine Vielzahl von Verarbeitungssituationen analysieren lässt und das mit knapp zwei Milliarden monatlich aktiver Nutzer das derzeit größte soziale Netzwerk darstellt.[19]

Zu diesem Zweck ist die Arbeit in vier Kapitel unterteilt. Im ersten Schritt werden grundlegende Aspekte wie zentrale Begrifflichkeiten, die Funktionsweise von sozialen Netzwerken und grundrechtliche Fragen geklärt (dazu Kapitel 1).

Im Anschluss befasst sich die Arbeit mit dem territorial anwendbaren Recht im Lichte der DSRL und den Änderungen durch die DSGVO (dazu Kapitel 2). In dem Kapitel wird der Frage nachgegangen, unter welchen Voraussetzungen sich Plattformbetreiber, die ihren Hauptsitz meist in den USA haben, dem europäischen Datenschutzregime unterwerfen müssen und wie die mitgliedstaatlichen Datenschutzregimes voneinander abzugren-

16 Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) vom 30. Juni 2017, BGBl. 2017 I, 2097; im Folgenden wird die Bezeichnung „BDSG-neu“ zur Unterscheidung vom BDSG (Rn. 11) gewählt.

17 Vgl. hierzu auch *Kühling*, NJW 2017, 1985, 1986 f.

18 Vgl. Kap. 3 Pkt. D.I.3, S. 223.

19 *Statista GmbH*, Ranking der größten Social Networks und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im August 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

zen sind. Im Übrigen stellt sich diese Frage ebenso im Nutzer-Nutzer-Verhältnis, wenn Nutzer, die sich physisch in unterschiedlichen Staaten befinden, miteinander interagieren.

Die Identifikation des territorial anwendbaren Rechts bildet die Basis für die im Anschluss folgende datenschutzrechtliche Bewertung der Verarbeitung personenbezogener Daten in sozialen Netzwerken (dazu Kapitel 3). Zu diesem Zweck erfolgt eine Bewertung der Zulässigkeit der Verarbeitung personenbezogener Daten im Nutzer-Nutzer-Verhältnis, im Anbieter-Nutzer-Verhältnis sowie der Verarbeitung durch Dritte im Lichte der einschlägigen unionalen wie nationalen Regelwerke nach der derzeitigen wie künftig anwendbaren[20] Rechtslage. Im Nutzer-Nutzer-Verhältnis muss dabei zunächst diskutiert werden, ob im Lichte von Privilegierungen von Verarbeitungen zu ausschließlich familiären oder persönlichen Zwecken im BDSG bzw. der DSRL sowie der DSGVO die Verarbeitung zwischen Nutzern überhaupt datenschutzrechtlichen Regelungen unterworfen ist. Anschließend wird darauf eingegangen, für welche Datenverarbeitungen der Nutzer datenschutzrechtlich verantwortlich ist, bevor die Zulässigkeit konkreter Datenverarbeitungen durch Nutzer diskutiert wird. Im Anbieter-Nutzer-Verhältnis wird insbesondere das sachlich anwendbare Recht zu analysieren sein, bevor auf dieser Grundlage die Zulässigkeit der Verarbeitung personenbezogener Daten unter Unterscheidung verschiedener Erhebungsmethoden bewertet wird. Schließlich wird die Zulässigkeit von Datenverarbeitungen durch Dritte evaluiert. Als Referenzbeispiel eignen sich hierzu Social Plug-Ins diverser sozialer Netzwerke: Zahlreiche Websitebetreiber integrieren Social Plug-Ins in ihre Websites,[21] die geeignet sind, schon bei Klick auf die Website eine Datenverarbeitung durch Dritte – nämlich durch die Plattformbetreiber – auszulösen. Zuletzt werden Betroffenenrechte und die Durchsetzbarkeit des Datenschutzrechts nach der DSRL bzw. dem BDSG sowie der DSGVO diskutiert.

Schließlich werden die aufgezeigten Problemfelder nach US-amerikanischem Recht vor dem Hintergrund des Datentransfers in die USA bewertet

20 Vgl. Art. 99 DSGVO, nach dem die DSGVO bereits in Kraft getreten ist und ab Mai 2018 gilt.

21 Nur beispielhaft genannt seien die Websites der Tageszeitungen Süddeutsche Zeitung und Frankfurter Allgemeine Zeitung, *Süddeutsche Zeitung*, abrufbar unter http://www.sueddeutsche.de/ (abgerufen am 13.10.2017); *Frankfurter Allgemeine Zeitung*, abrufbar unter http://www.faz.net/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

(dazu Kapitel 4). Dies ist besonders relevant, da die Betreiber populärer sozialer Netzwerke personenbezogene Daten in die USA übermitteln.[22] Dies ist nach der Konzeption der DSRL bzw. der DSGVO jedoch nur gestattet, sofern das Drittland, in das die Daten transferiert werden, ein angemessenes Schutzniveau aufweist.[23] So soll ein Überblick über den Persönlichkeitsschutz in der Entwicklung des US-amerikanischen Verfassungsrechts sowie einfachen US-amerikanischen Bundesrechts die unterschiedlichen Ansatzpunkte zwischen europäischem und US-amerikanischem Datenschutzverständnis aufzeigen. Darauf aufbauend wird sodann der Transfer personenbezogener Daten von der EU in die USA unter Einbeziehung der für diesen Anwendungsfall geschaffenen „Sonderregelungen" sowie der relevanten *EuGH*-Rechtsprechung analysiert.

Die Arbeit endet mit einem Fazit.

22 Vgl. etwa *Facebook Inc.,* Facebook Inc. and the EU-U.S. Privacy Shield, abrufbar unter https://www.facebook.com/about/privacyshield (abgerufen am 13.10.2017); *Snap Inc.,* Datenschutzbestimmungen, abrufbar unter https://www.snap.com/de-DE/privacy/privacy-policy (abgerufen am 13.10.2017).

23 Vgl. Art. 25 Abs. 1 DSRL; Art. 44 ff. DSGVO.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kapitel 1: Grundlagen

Dieses Kapitel dient der Klärung allgemeiner Grundlagen. So muss mit Blick auf die unterschiedlichen zu besprechenden Regelwerke zunächst auf die verwendete Terminologie der Arbeit hingewiesen werden (dazu A). Anschließend werden die sozialen Netzwerke nach ihren Erscheinungsformen klassifiziert und bekannte soziale Netzwerke samt zentraler Funktionen vorgestellt (dazu B.). Sodann soll ein Einblick in die Finanzierungslage sozialer Netzwerke die Bedeutung personenbezogener Daten als Finanzierungsmodell erklären. Damit in engem Zusammenhang steht der anschließende Überblick über verbreitete Tracking Tools, mit denen Nutzer bestimmbar gemacht werden können und ihr Surfverhalten beobachtet werden kann (dazu C.). Abschließend wird im Rahmen einer grundrechtlichen Analyse ein Überblick über die sich gegenüberstehenden, verfassungsrechtlich verankerten Interessen der Betroffenen, der Plattformbetreiber und Dritter dargestellt. Dieser Interessenskonflikt ist datenschutzrechtlichen Sachverhalten zwischen Privaten immanent und seine Darstellung ist daher die Grundlage der Diskussion einfachgesetzlicher und sekundärrechtlicher Bestimmungen.[24]

A. Hinweis zur rechtlichen Terminologie

Die Terminologie der zu besprechenden Regelwerke – insbesondere DSGVO, DSRL sowie BDSG und BDSG-neu – weicht teilweise nicht unerheblich voneinander ab. So umfasst der Begriff der „Verarbeitung" i. S. d. Art. 4 Nr. 2 DSGVO, wie bereits der Verarbeitungsbegriff i. S. d. 2 lit. b DSRL, sämtliche Verarbeitungsvorgänge von der Erhebung bis zur Nutzung der Daten. Demgegenüber trennt das BDSG diese Schritte in die Unterkategorien „Erheben", § 3 Abs. 3 BDSG, „Verarbeiten" mit weiteren Untergliederungen, § 3 Abs. 4 BDSG, und „Nutzen", § 3 Abs. 5 BDSG. Der Begriff der Verarbeitung i. S. d. § 3 Abs. 4 BDSG umfasst dabei etwa das

24 Diese Bewertung einfachgesetzlicher und sekundärrechtlicher Zulässigkeitstatbestände erfolgt im Wesentlichen in Kap. 3, vgl. exemplarisch Kap. 3 Pkt. A.II.2.d.bb, S. 107; Kap. 3 Pkt. A.III.2.a.bb.iii, S. 120; Kap. 3 Pkt. A.III.2.c, S. 125.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Speichern, Übermitteln oder Sperren der Daten, nicht jedoch das Erheben oder Nutzen. Daher wird im Zusammenhang mit dem BDSG häufig der Begriff des „Umgangs mit personenbezogenen Daten" herangezogen,[25] wenn auf die Gesamtheit dieser Vorgänge Bezug genommen wird. Eine weitere Bezeichnungsmöglichkeit ist die Heranziehung des Begriffs der „Verwendung" der personenbezogenen Daten. Dieser Begriff kann jedoch insofern irreführen, als das TMG[26] zwischen der Erhebung und der Verwendung von personenbezogenen Daten unterscheidet, vgl. etwa § 12 Abs. 1 TMG, der Verwendungsbegriff des TMG also nicht die Erhebung umfasst.

Zudem ist im BDSG eine straffe Trennung zwischen „öffentliche[n] Stellen" und „nicht-öffentliche[n] Stellen" angelegt, vgl. § 2 BDSG, die auch im BDSG-neu beibehalten wird, vgl. §§ 1, 2 BDSG-neu. Diese Trennung spiegelt sich in der konsequenten Unterscheidung der Erlaubnistatbestände wider: §§ 12 ff. BDSG regeln die Rechtsgrundlagen für den Umgang mit personenbezogenen Daten durch öffentliche Stellen, §§ 27 ff. BDSG den Umgang mit personenbezogenen Daten durch nicht-öffentliche Stellen. Weder die DSRL noch die DSGVO sieht eine solche Trennung vor; die Erlaubnistatbestände dort sind grundsätzlich auf alle Verantwortlichen anwendbar, soweit nicht etwas Anderes aus den Normen und den dazugehörigen Erwägungsgründen selbst hervorgeht. Terminologisch spricht die DSGVO in diesem Zusammenhang etwa von öffentlichen wie privaten Akteuren[27] bzw. Stellen oder spezifisch von Behörden[28]. Soweit diese Arbeit also von „Privaten" spricht sind damit private Stellen i. S. d. DSGVO bzw. nicht-öffentliche Stellen i. S. d. BDSG gemeint.

Ein weiterer signifikanter terminologischer Unterschied liegt in der Bezeichnung desjenigen, der für die Verarbeitung von bzw. den Umgang mit personenbezogenen Daten verantwortlich ist: Im BDSG wird hierfür der Begriff der „verantwortliche[n] Stelle" herangezogen, § 3 Abs. 7 BDSG, in der DSRL der Begriff des „für die Verarbeitung Verantwortliche[n], Art. 2 lit. d DSRL, und in der DSGVO der Begriff des „Verantwortliche[n]", Art. 4 Nr. 7 DSGVO.

In der vorliegenden Arbeit wird grundsätzlich auf die Terminologie der DSGVO zurückgegriffen, d. h., dass beispielsweise der Begriff der „Verarbeitung" als alle Vorgänge von der Erhebung bis zur Nutzung umfassend

25 Vgl. etwa *Schild*, in: BeckOK DatenschutzR, BDSG, § 3, Rn. 47 ff.
26 Telemediengesetz (TMG) vom 26. Februar 2007, BGBl. 2007 I, 179.
27 Vgl. etwa EG 5 S. 2 DSGVO.
28 Vgl. etwa EG 47 S. 5 DSGVO.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

zu verstehen ist. Davon abweichend wird jedoch auf die Terminologie desjenigen Regelwerkes zurückgegriffen, dessen Normen gerade speziell analysiert werden. Wird also die Zulässigkeit einer Verarbeitung nach dem BDSG bewertet,[29] wird in diesem Zusammenhang die im BDSG angelegte Terminologie verwendet.

B. Soziale Netzwerke und zentrale Funktionen

Soziale Online-Netzwerke zeichnen sich durch die Möglichkeiten der Vorstellung der eigenen Person in Verbindung mit Interaktionsmöglichkeiten mit anderen Nutzern aus. Sie können klassisch über einen Browser und inzwischen meist auch über Apps aufgerufen werden. Im Folgenden werden die sozialen Online-Netzwerke und ihre Erscheinungsformen dargestellt und anschließend ein Überblick über ihre zentralen Funktionen gegeben.

I. Klassifikation der Plattformen

Online-Plattformen mit Interaktionsmöglichkeiten treten im Wesentlichen in drei Erscheinungsformen auf: Klassische soziale Online-Netzwerke, webbasierte Messenger-Dienste und Hybridformen, die Messengerkomponenten mit Funktionen klassischer sozialer Netzwerke kombinieren.

Unter klassischen sozialen Online-Netzwerken soll eine Plattform verstanden werden, die ihren Mitgliedern die Möglichkeit der Vorstellung der eigenen Person sowie der Interaktion bietet, wobei die Interaktion klassischerweise auch für andere Mitglieder einsehbar ist. Funktionen dieses Typus umfassen etwa die Erstellung eines Profils, üblicherweise versehen mit einem Profilbild und der Preisgabe gewisser Eckdaten. Diese Plattformen sind auf die Vernetzung ihrer Mitglieder ausgelegt und bieten ihren Nutzern folglich die Option, ein Netzwerk mit anderen Mitgliedern aufzubauen. Diesem Netzwerk, Teilen des Netzwerks oder für jeden Internetnutzer einsehbar können Mitglieder weitere Informationen mitteilen, indem sie Texte oder Fotos posten. Weitere Möglichkeiten sind netzwerkinterne Bewertungssysteme für diese Texte oder Fotos, das Kommentieren der Informationen oder das Hinterlassen von Nachrichten auf dem für einen bestimmten Personenkreis einsehbaren Profil. Darüber hinaus bieten viele soziale Netz-

29 Vgl. etwa Kap. 3 Pkt. A.III.2.a, S. 113.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

werke auch die Möglichkeit, sich in Interessensgruppen zusammenzuschließen und sich dort auszutauschen. Im Vordergrund steht also die Präsentation der eigenen Person und darauf aufbauend die Interaktion mit Anderen.

Demgegenüber verfolgen web-basierte Messenger-Dienste den Zweck der direkten Kommunikation, ähnlich wie E-Mails oder SMS.[30] Im Fokus steht dabei die gezielte Interaktion zwischen zwei oder mehreren Gesprächspartnern.

Die Abgrenzung kann also dahingehend erfolgen, dass in sozialen Netzwerken die Interaktion durch eine einem bestimmten Personenkreis zugängliche Darstellung der eigenen Person und Reaktionen Anderer darauf basiert, während Messenger-Dienste eine private Kommunikation ermöglichen sollen. Es gibt zunehmend auch Hybridformen dieser Plattformen, die beide Funktionen vereinen, etwa indem es sich bei dem betreffenden Dienst vorwiegend um einen Messenger-Dienst handelt, der jedoch zusätzlich die Möglichkeit bietet, Texte und Fotos hochzuladen, die dann von allen verbundenen Kontakten eingesehen werden können, ohne – anders als bei einer Nachricht über einen Messenger-Dienst – gezielt Adressdat dieser Nachricht zu sein.

II. Vorstellung ausgewählter Plattformen

Im Folgenden werden ausgewählte Plattformen und ihre Funktionsweisen vorgestellt.

30 Inwiefern diese Dienste den telekommunikationsrechtlichen Datenschutzbestimmungen der §§ 91 ff. TKG unterworfen sind, ist nicht Gegenstand dieser Betrachtung, da es sich bei diesen Diensten nicht um soziale Netzwerke im eigentlichen Sinne handelt; vgl. hierzu *Kühling/Schall*, CR 2015, 641 645 ff.; *Schneider*, ZD 2014, 231, 233 ff.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

1. Facebook

Das größte soziale Netzwerk ist *Facebook*[31] mit rund 2,05 Mrd. monatlich aktiven Nutzern.[32] Auf *Facebook* erstellen Nutzer ein Profil von sich mit Angaben u. a. zu Wohnort, Heimatstadt, Arbeitsplatz, Ausbildungsstätten, Studienkollegen, Geburtstag, aber auch zu besonderen Lebensereignissen wie einer Verlobung, Scheidung – oder einer Organspende. Jedes Profil ist mit einer sog. „Timeline" ausgestattet, auf der Nutzer Informationen oder Fotos hochladen können, die wahlweise für all ihre Kontakte, nur für ausgewählte Kontakte oder für jeden Internetnutzer einsehbar sind. Zudem können Nutzer sich gegenseitig in Beiträgen, Fotos und Kommentaren „verlinken", d. h., dass der Name des Nutzers in dem betreffenden Beitrag angezeigt und zusätzlich mit einem Hyperlink auf dessen Profil unterlegt wird. Mitglieder können hochgeladene Informationen mittels integrierter Bewertungssysteme – beispielsweise dem sog. „Like-Button" – bewerten und damit ihr Gefallen, ihre Wut, ihre Trauer oder ihre Belustigung über den entsprechenden Inhalt ausdrücken.

Facebook wird nicht nur von Privatpersonen, sondern auch von Personen des öffentlichen Lebens[33], Unternehmen[34] und Behörden[35] genutzt. Auf sog. Fanpages suchen sie die Interaktion mit interessierten Nutzern. Fanpages werden aber auch zum Austausch von Nutzern untereinander genutzt.[36]

---

31 *Facebook Inc.*, abrufbar unter https://www.facebook.com/ (abgerufen am 13.10.2017).

32 *Statista GmbH*, Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im August 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/ (abgerufen am 13.10.2017).

33 Exemplarisch sei die Fanpage von Angela Merkel genannt, https://www.facebook.com/AngelaMerkel/?fref=ts (abgerufen am 13.10.2017).

34 Exemplarisch seien die Fanpages von Adidas Original genannt, https://www.facebook.com/adidasoriginals/?fref=ts (abgerufen am 13.10.2017), sowie, als Beispiel für ein lokales Unternehmen, der Regensburger Brauerei Kneitinger, https://www.facebook.com/kneitinger.de/?fref=ts (abgerufen am 13.10.2017).

35 Exemplarisch sei die Fanpage der Polizei München genannt, https://www.facebook.com/polizeimuenchen/?fref=ts (abgerufen am 13.10.2017).

36 Exemplarisch sei die Gruppe „Diskussionsforum Innenstadt Ingolstadt" genannt, https://www.facebook.com/groups/163504970482100/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Facebook bietet Websitebetreibern überdies die Möglichkeit, auf deren Website sog. Social Plug-Ins zu integrieren, etwa den „Like-Button".[37] Das bedeutet, dass auf der Website eines mit *Facebook* nicht verbundenen Betreibers der „Like-Button" integriert wird.[38] Zudem gibt *Facebook* in seiner Datenschutzrichtlinie bekannt, die Nutzerdaten innerhalb der „Unternehmensgruppe" zu teilen.[39]

2. Instagram

Instagram[40] ist als App für Smartphones und Tablets konzipiert, jedoch auch über einen Internetbrowser aufrufbar. Die App besteht vorwiegend aus der Darstellung von Fotos, wobei zahlreiche Nutzer ihre Fotos für jeden Nutzer einsehbar posten. *Instagram* wurde im Jahr 2012 von *Facebook* übernommen. Ausweislich der Datenschutzrichtlinien von *Facebook* und *Instagram* werden die Nutzerdaten zwischen den Unternehmen miteinander ausgetauscht.[41]

3. Twitter

Twitter[42] ist ein soziales Netzwerk, bei dem jedes Posting durch einen Nutzer auf 140 Zeichen begrenzt ist. Die Nachrichten, sogenannte „Tweets",

---

37 Vgl. *Facebook Inc.,* FAQ zu sozialen Plug-Ins, abrufbar unter https://developers.facebook.com/docs/plugins/faqs (abgerufen am 13.10.2017).

38 Vgl. Kap. 3 Pkt. C, S. 199.

39 *Facebook Inc.,* Datenrichtlinie, abrufbar unter https://www.facebook.com/about/privacy (abgerufen am 13.10.2017) i. V. m. *Facebook Inc.,* Die Facebook-Unternehmen, abrufbar unter https://www.facebook.com/help/111814505650678 (abgerufen am 13.10.2017).

40 *Instagram LLC.*, abrufbar unter https://www.instagram.com/?hl=de (abgerufen am 13.10.2017).

41 *Facebook Inc.,* Datenrichtlinie, abrufbar unter https://www.facebook.com/about/privacy (abgerufen am 13.10.2017) i. V. m. *Facebook Inc.,* Die Facebook-Unternehmen, abrufbar unter https://www.facebook.com/help/111814505650678 (abgerufen am 13.10.2017); *Instagram LLC.,* Datenrichtlinie, abrufbar unter https://help.instagram.com/155833707900388 (abgerufen am 13.10.2017), allerdings lediglich mit dem Verweis auf das Teilen der Informationen mit „verbundenen Unternehmen"; *Facebook* wird zu Beginn der Datenschutzrichtlinie mit dem Hinweis erwähnt, dass *Instagram* von *Facebook* aufgekauft wurde.

42 *Twitter Inc.*, abrufbar unter https://twitter.com/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

sind standardmäßig öffentlich, können in ihrer Einsehbarkeit jedoch beschränkt werden. Viele Mitglieder nutzen einen Account in ihrer öffentlichen Funktion, um sich über Belange von öffentlichem Interesse auszutauschen.[43] Im Kern ist *Twitter* im Vergleich zu *Facebook* stärker auf Postings und weniger auf Interaktion ausgelegt. Auch *Twitter* stellt die Möglichkeit der Einbindung von Social Plug-Ins für Websitebetreiber bereit.

4. Snapchat

Snapchat[44] kann als Hybrid zwischen Messenger-Dienst und sozialem Netzwerk bezeichnet werden. Die App war ursprünglich derart aufgebaut, dass Nutzer sich gegenseitig Fotos senden konnten, die nach einigen Sekunden wieder verschwanden, war also zunächst rein als Messenger-Dienst konzipiert. Inzwischen können Nutzer jedoch auch Fotos und Videos von sich für mit ihnen verbundenen Nutzern zugänglich machen, ohne dass bestimmte Nutzer gezielt angesprochen werden müssen. Diese Fotos oder Videos sind dann für 24 Stunden einsehbar.

C. Finanzierung sozialer Netzwerke

Der überwiegende Teil der sozialen Netzwerke, und insbesondere der Netzwerke mit den meisten Nutzerzahlen, verlangt für die Bereitstellung ihrer Dienste keinen monetären Gegenwert. Vor dem Hintergrund, dass im Internet viele Leistungen vermeintlich kostenfrei abgerufen werden können – wie etwa E-Mail-Dienste, Suchmaschinendienste oder Zeitungsartikel – scheint dies zunächst wenig überraschend. Allerdings haben die Betreiber von sozialen Netzwerken hohe Kosten für die Bereitstellung ihrer Dienste, sodass selbstredend andere Methoden zur Finanzierung des Betriebs solcher Plattformen herangezogen werden. Im Folgenden wird ein Überblick über die Kosten und Finanzierungsmethoden sozialer Netzwerke sowie über die technischen Methoden, mittels derer ihnen die Bestimmbarkeit von Nutzern gelingt, gegeben.

---

43 Exemplarisch sei auf den regen Austausch auf *Twitter* zu datenschutzrechtlichen Belangen hingewiesen, vgl. nur das Profil des MdEP Jan Philipp Albrecht, abrufbar unter https://twitter.com/JanAlbrecht (abgerufen am 13.10.2017).

44 *Snap Inc.*, abrufbar unter https://www.snapchat.com/l/de-de/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

I. Finanzierung durch Werbung

Im Jahr 2016 hatte *Facebook* etwa Gesamtausgaben von 15,2 Mrd. USD,[45] das Netzwerk *Twitter* mit rund 1/6 der monatlich aktiven Nutzer[46] etwa 2,9 Mrd. USD.[47] Die Kostenfaktoren sind dabei vielfältig: Schon die Bereitstellung der physischen Infrastruktur für den Betrieb der Computerprogramme ist kostenintensiv. Die großen sozialen Netzwerke, die Millionen[48] oder sogar über eine Milliarde[49] Nutzeranfragen pro Tag bewältigen müssen, benötigen hierzu eine Vielzahl von Servern. Hinzu kommen Kosten für Personal, Forschung und Verwaltung. Durch den Wettbewerb, in dem die unterschiedlichen Anbieter zueinanderstehen, erhöht sich zudem der Druck, in bessere Infrastruktur und hochqualifiziertes Personal zu investieren.[50]

Da soziale Netzwerke für die Bereitstellung ihrer Diense in der Regel keinen monetären Gegenwert verlangen, ziehen sie ihre Einnahmen aus anderen Quellen: So geht beispielsweise aus dem Jahresbericht von *Facebook* hervor, dass Werbeeinnahmen über 96 % des Umsatzes ausmachen.[51] Diese Einnahmen erzielt *Facebook* durch das Schalten von Online-Werbung. Online-Werbung bedeutet die Werbeeinblendung auf einer Website, die deren

---

45 *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 31.

46 *Statista GmbH*, Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im August 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/ (abgerufen am 13.10.2017).

47 *Twitter Inc.,* Annual Report 2016, abrufbar unter https://investor.twitterinc.com/annuals-proxies.cfm (abgerufen am 13.10.2017), S. 40.

48 *Twitter Inc.,* Twitter Nutzung / Fakten zum Unternehmen, abrufbar unter https://about.twitter.com/company (abgerufen am 13.10.2017).

49 So hatte *Facebook* nach eigenen Angaben im Juni 2017 täglich 1,32 Mrd. Nutzer weltweit, *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017).

50 Vgl. etwa die Ausführungen im Jahresbericht von *Twitter*, *Twitter Inc.,* Annual Report 2016, abrufbar unter https://investor.twitterinc.com/annuals-proxies.cfm (abgerufen am 13.10.2017), S. 20.

51 *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 62.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Besuchern zur „[…] Unterstützung von Marketing- und Kommunikationszielen“ [52] angezeigt wird. Die Werbung wird gezielt denjenigen Nutzern angezeigt, die potentiell Interesse an dem beworbenen Produkt haben könnten, sog. Targeting.[53] Targeting tritt in vielen Formen auf, etwa als soziodemographisches Targeting, bei dem die Zielgruppe durch Alter, oder Berufsgruppenzugehörigkeit eingeschränkt wird, als Content-Targeting, bei dem die Werbung an den Inhalt der besuchten Website angepasst wird, als Geo-Targeting, bei dem die angezeigte Werbung abhängig vom Standort des Nutzers ist oder als Behavioral Targeting, d. h. die Erfassung des Surfverhaltes des Nutzers um die anzuzeigende Werbung darauf abzustimmen.[54] So bietet etwa *Facebook* die Werbeplatzierung nach Ort, Demographie, Interessensangaben, Surfverhalten, verwendeter Technik und nach Verbindungen zu anderen Nutzern an.[55] Für die Plattformbetreiber ist die Verarbeitung der personenbezogenen Daten ihrer Nutzer daher essentielles Finanzierungsmodell: Im Jahr 2016 erzielte *Facebook* mit Werbeeinnahmen einen Umsatz von 26,9 Mrd. USD, bei einem Gesamtumsatz von 27,6 Mrd. USD.[56] Anhand des Gesamtumsatzes pro Quartal und der Anzahl der monatlich aktiven Nutzer berechnet *Facebook* außerdem den Umsatz pro Nutzer in einer bestimmten Gegend. Weltweit ergab sich im letzten Quartal des Jahres 2016 damit ein Pro-Nutzer Umsatz von 4,83 USD, wobei allerdings der Umsatz pro Nutzer pro Quartal bei Nutzern in den USA und Kanada mit 19,81 USD deutlich höher lag als der Umsatz pro Nutzer bei europäischen Nutzern mit 5,98 USD.[57]

---

52 *Lammenett,* Praxiswissen Online-Marketing, S. 282.

53 *Kreutzer/Rumler/Wille-Baumkauff,* B2B-Online-Marketing und Social Media, S. 126.

54 Ausführlich *Kreutzer/Rumler/Wille-Baumkauff,* B2B-Online-Marketing und Social Media, S. 126 f.

55 *Facebook Inc.,* Core Audiences, abrufbar unter https://www.facebook.com/business/learn/facebook-ads-choose-audience (abgerufen am 13.10.2017).

56 *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 62.

57 *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 36.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

II. Technische Trackingmethoden

Zur zielgerichteten Platzierung von Werbung greifen viele Plattformbetreiber auf verschiedene technische Mechanismen zurück.[58] Sie bedienen sich dieser Mechanismen, um das Nutzerverhalten zu beobachten, aber auch, um die Bedienung ihres Angebots zu optimieren und um die Übertragung des Angebots zu ermöglichen. Im Folgenden werden diese Mechanismen als Tracking Tools bezeichnet.

Zunächst muss unterschieden werden zwischen Tracking Tools, die die vom Nutzer besuchte Website selbst auf ihrer Website implementiert hat und solchen Tracking Tools, die von Dritten gesteuert werden, also Parteien, mit denen der Nutzer nicht interagiert, sog. Third Party-Tools. Dabei aktivieren Dritte das Tracking Tool auf der besuchten Website.[59] Beispielhaft kann hierfür die Implementierung sog. Social Plug-Ins auf einer Website genannt werden, d. h. ein Verweis auf ein soziales Netzwerk, etwa in Form eines Icons auf dieser Website. Teilweise hinterlassen diese Plug-Ins automatisch mit dem Besuch einer Website Tracking Tools auf dem Endgerät des Nutzers.[60]

Aufgrund der schnellen Entwicklung und zunehmenden Anzahl solcher Tracking Tools wird teilweise von einem „Wettrüsten“[61] gesprochen. Ein abschließender Überblick über die existierenden Trackingmethoden ist damit kaum möglich,[62] für das bessere Verständnis der technischen Hintergründe und den damit einhergehenden juristischen Problemen sollen im Folgenden jedoch die bekanntesten Tracking Tools vorgestellt werden.

---

58 So spricht *Facebook* von „Cookies und anderen Speichertechnologien“, vgl. *Facebook Inc.,* Cookies und andere Speichertechnologien, abrufbar unter https://www.facebook.com/policies/cookies/ (abgerufen am 13.10.2017).

59 *Roesner/Kohno/Wetherall*, Detecting and Defending Against Third-Party Tracking on the Web, abrufbar unter https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (abgerufen am 13.10.2017), S. 1.

60 Ausführlich zu Social Plug-Ins, vgl. Kap. 3 Pkt. C, S. 199.

61 *Acar/Eubank/Englehardt/Juarez/Narayanan/Diaz*, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, in: Association for Computing Machinery (Hrsg.), CCS’14, S. 674 ff.; *Roesner/Kohno/Wetherall*, Detecting and Defending Against Third-Party Tracking on the Web, abrufbar unter https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (abgerufen am 13.10.2017), S. 1.

62 So auch *Roesner/Kohno/Wetherall*, Detecting and Defending Against Third-Party Tracking on the Web, abrufbar unter https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (abgerufen am 13.10.2017), S. 3.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

1. Cookies

Das wohl bekannteste und verbreitetste Tracking Tool ist der sog. HTTP-Cookie.[63] HTTP-Cookies sind kleine Textdateien, die die besuchte Website oder ein Dritter über den benutzten Browser auf dem Rechner des Nutzers entweder mittels eines Skripts in der Website oder durch die Übertragung eines Set-Cookie Headers durch den Server an den anfragenden Browser platziert.[64] In dieser Datei können verschiedene Informationen gespeichert werden, etwa eine bestimmte Nutzerkennung, mit der der Nutzer identifizierbar ist. Bestimmte Cookies können auch websiteübergreifend Informationen aufnehmen.

Durch einen Cookie-Abgleich können verschiedene Parteien, die denselben Nutzer mithilfe von Cookies tracken, dessen Cookies außerdem miteinander synchronisieren.[65] Dies geschieht beispielsweise indem Partei A den Browser seines Nutzers auf eine URL von Partei B umleitet, wobei in den Parametern der URL die Cookie-Informationen der umleitenden Partei A enthalten sind. Nachdem Partei B die Umleitungsanfrage der URL mit den veränderten Parametern erhalten hat, kann sie die in der URL enthaltenen Cookie-Informationen mit ihren eigenen abgleichen.[66] So können eine oder beide Parteien die Cookie-Informationen miteinander abgleichen.

Da Cookies in ihrer ursprünglichen Form grundsätzlich nicht browserübergreifend funktionieren und durch die Browser-Einstellungen der gängigen Browser gelöscht werden können, wurden mit der Zeit verschiedene andere Tracking Tools entwickelt, die sowohl browserübergreifend anwendbar sind, als auch schwerer für den Nutzer zu löschen oder blocken sind. Ein solches Tool sind Flash Cookies. Flash Cookies werden durch das *Adobe-Flash*[67] Plug-In in Browsern auf den Nutzer-Computern platziert.

---

63 *Roesner/Kohno/Wetherall*, Detecting and Defending Against Third-Party Tracking on the Web, abrufbar unter https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (abgerufen am 13.10.2017), S. 2.

64 *Roesner/Kohno/Wetherall*, Detecting and Defending Against Third-Party Tracking on the Web, abrufbar unter https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (abgerufen am 13.10.2017), S. 2.

65 *Olejnik/Tran/Castelluccia*, Selling Off Privacy at Auction, abrufbar unter https://www.researchgate.net/publication/269197027_Selling_Off_Privacy_at_Auction (abgerufen am 13.10.2017), S. 2.

66 *Olejnik/Tran/Castelluccia*, Selling Off Privacy at Auction, abrufbar unter https://www.researchgate.net/publication/269197027_Selling_Off_Privacy_at_Auction (abgerufen am 13.10.2017), S. 2.

67 *Adobe Systems Inc.*, abrufbar unter http://www.adobe.com/de/products/flashplayer.html?promoid=ISMSA (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Sie können mehr Informationen speichern, werden – anders als HTTP-Cookies – nicht automatisch gelöscht und in Speicherorten auf dem PC platziert, die für den Nutzer nicht immer erkennbar oder auffindbar sind. Hinzukommend funktionieren sie browserübergreifend.[68] Darüber hinaus können mithilfe von Flash Cookies bereits gelöschte HTTP-Cookies wiederhergestellt werden, sog. „Respawning". Hierzu wird dieselbe Information, die in den HTTP-Cookies gespeichert wurde, in den Flash Cookies dupliziert. Da die Flash Cookies, anders als die HTTP-Cookies, nicht über die Browser-Einstellungen gelöscht werden, bleibt die Information in den HTTP-Cookies somit trotz Löschung erhalten. Die Informationen werden nach Löschung der HTTP-Cookies in dem ursprünglichen, eigentlich gelöschten, Verzeichnis wiederhergestellt.[69] Somit stehen auch bereits gelöschte HTTP-Cookies wieder für einen Cookie-Abgleich zur Verfügung.[70] Inzwischen lässt sich, wohl auch aufgrund reger Kritik, ein Rückgang der Flash Cookies verzeichnen.[71]

Weitere Methoden, um das Surfverhalten zu beobachten, sind HTML5 Cookies. Ebenso wie Flash Cookies können HTML5 Cookies mehr Informationen als HTTP-Cookies speichern und werden nicht automatisch gelöscht.[72]

Zuletzt sind noch sog. Evercookies zu nennen. Sie duplizieren, anders als Flash Cookies, nicht nur HTTP-Cookie Verzeichnisse, sondern die Verzeichnisse aller möglichen Tracking Tools.[73]

---

68 *Soltani/Canty/Mayo/Thomas/Hoofnagle*, Flash Cookies and Privacy, abrufbar unter http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1070/1505 (abgerufen am 13.10.2017), S. 1.

69 *Soltani/Canty/Mayo/Thomas/Hoofnagle*, Flash Cookies and Privacy, abrufbar unter http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1070/1505 (abgerufen am 13.10.2017), S. 3.

70 *Acar/Eubank/Englehardt/Juarez/Narayanan/Diaz*, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, in: Association for Computing Machinery (Hrsg.), CCS'14, S. 676.

71 *McDonald/Cranor*, 2011 I/S: J.L. & Pol'y for Info. Soc'y 639; *Ayenson/Wambach/Soltani/Good/Hoofnagle*, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390 (abgerufen am 13.10.2017), S. 12.

72 *Ayenson/Wambach/Soltani/Good/Hoofnagle*, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390 (abgerufen am 13.10.2017), S. 6.

73 *Acar/Eubank/Englehardt/Juarez/Narayanan/Diaz*, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, in: Association for Computing Machinery (Hrsg.), CCS'14, S. 676.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

2. Fingerprinting

Eine weitere Methode, den Nutzer aus der Masse der Internetnutzer zu individualisieren und sein Surfverhalten verfolgen zu können, ist das sog. Fingerprinting. Hierbei wird das benutzte Gerät des Nutzers auf dessen Beschaffenheit und Settings ausgelesen, etwa nach dem verwendeten Browser, Bildschirmauflösung und Art des Betriebssystems. Aus dem Zusammentreffen dieser Informationen kann der Betroffene bestimmbar werden.[74] Besonders bekannt ist das sog. Canvas Fingerprinting. Wenn der Nutzer eine Website besucht, die Canvas Fingerprinting verwendet, weist diese Website den Browser an, einen bestimmten Text auf Canvas, eine in HTML-Code definierte Zeichenoberfläche, zu zeichnen. Damit kann der verwendete Browser und das Betriebssystem ausgewertet werden.[75] Canvas Fingerprinting ist für den Nutzer kaum bemerkbar.[76] Das Hinterlassen eines solchen „Fingerabdrucks" ist zudem kaum reversibel. Denn auch wenn sich die Fingerprints rasch ändern, können mittels Algorithmen die neuen Fingerprints mit den alten in Verbindung gebracht werden.[77] Ferner ist es mit dieser Methode in Verbindung mit der IP-Adresse möglich, gelöschte HTTP-Cookies wiederherzustellen.[78]

III. Zusammenfassung

Plattformbetreiber finanzieren ihre Angebote in der Regel nicht durch die Erhebung eines Nutzungsentgeltes, sondern beinahe ausschließlich durch die Schaltung von Werbung. Sie haben daher ein besonderes Interesse an personenbezogenen Daten der Nutzer, um Werbung zielgerichtet anzeigen zu können. Dazu bedienen sie sich u. a. der Nutzung von Tracking Tools.

---

74 Vgl. *Acar/Eubank/Englehardt/Juarez/Narayanan/Diaz*, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, in: Association for Computing Machinery (Hrsg.), CCS'14, S. 675 f.

75 *Acar/Eubank/Englehardt/Juarez/Narayanan/Diaz*, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, in: Association for Computing Machinery (Hrsg.), CCS'14, S. 679.

76 *Eckersley*, How Unique Is Your Browser?, in: Attalah/Hopper (Hrsg.), Privacy Enhancing Technologies, S. 3.

77 *Eckersley*, How Unique Is Your Browser?, in: Attalah/Hopper (Hrsg.), Privacy Enhancing Technologies, S. 2.

78 *Eckersley*, How Unique Is Your Browser?, in: Attalah/Hopper (Hrsg.), Privacy Enhancing Technologies, S. 3 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Die Entwicklung von diesen Tracking Tools schreitet in hohem Tempo voran und bietet vielfältige Möglichkeiten, die Nutzer bestimmbar zu machen und ihr Surfverhalten zu beobachten.

D. Überblick über grundrechtliche Interessenpositionen

Eine der größten Herausforderungen im Datenschutzrecht ist die Frage, wie der Konflikt sich gegenüberstehender, grundrechtlich verankerter Interessen im multipolaren Grundrechtsgefüge aufzulösen ist. Zwar wirken die Grundrechte nicht unmittelbar zwischen Privaten, sie errichten jedoch eine objektive Werteordnung, die bei der Auslegung ausfüllungsbedürftiger Begriffe zu beachten ist (mittelbare Drittwirkung).[79] In diesem Zuge müssen insbesondere Betroffeneninteressen, Interessen der Verantwortlichen und letztlich Drittinteressen gegeneinander abgewogen und in Ausgleich gebracht werden. Diese Interessenabwägung ist dem sekundärrechtlichen Datenschutz auf Unionsebene und dem einfachgesetzlichen Datenschutz auf nationaler Ebene inhärent, etwa in Art. 7 lit. f DSRL, §§ 28 f. BDSG sowie Art. 6 Abs. 1 S. 1 lit. f DSGVO. Als Grundlage für die weitere Analyse sekundärrechtlicher wie einfachgesetzlicher Normen im Einzelfall[80] wird daher an dieser Stelle ein kurzer Überblick über die relevanten Grundrechtspositionen gegeben.[81]

---

79 stRspr *BVerfG,* Beschl. v. 15.01.1958, Az. 1 BvR 400/51, BVerfGE 7, 198 – Lüth; *BVerfG,* Beschl. v. 26.02.1969, Az. 1 BvR 619/63, BVerfGE 25, 256, 263 – Blinkfüer; *BVerfG,* Beschl. v. 11.05.1976, Az. 1 BvR 671/70, BVerfGE 42, 143, 147 – Deutschland-Magazin; *BVerfG,* Beschl. v. 23.04.1986, Az. 2 BvR 487/80, BVerfGE 73, 261, 268 – Barabgeltung für Hausbrandkohle.

80 Vgl. insbesondere die Analyse der Zulässigkeit der Datenverarbeitung, etwa in Kap. 3 Pkt. A.II.2.d.bb, S. 107; Kap. 3 Pkt. A.III.2.a.bb.iii, S. 120; Kap. 3 Pkt. A.III.2.c, S. 125.

81 Im Folgenden werden Grundrechtspositionen des GG und der GRCh dargestellt. Da es sich vorliegend um eine Darstellung der relevanten Interessenpositionen für die spätere Diskussion der einfachgesetzlichen und sekundärrechtlichen Normen handelt, bleiben EMRK-Grundrechte außer Betracht.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

I. Betroffeneninteressen

1. Das Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist eine Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG. Das *BVerfG* hat in seinem „Volkszählungsurteil“[82] hierzu ausgeführt, dass aus dem Gedanken der Selbstbestimmung die Befugnis des Einzelnen folge, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart würden.[83] Daraus leitet das *BVerfG* das Recht der Bürger ab, zu wissen „[…] wer was wann und bei welcher Gelegenheit über sie weiß.“[84] Das Recht auf informationelle Selbstbestimmung soll folglich vor der allumfassenden Datenerfassung und Profilbildung sowie vor der fehlerhaften Erfassung von Daten schützen.[85] Daher ist auch die Feststellung des *BVerfG* von besonderer Bedeutung, dass es „[…] unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr [gibt]“.[86] Das Recht auf informationelle Selbstbestimmung hat damit besondere Bedeutung im Schutz der personenbezogenen Daten. Sein weiter Schutzbereich verdeutlicht, dass es nicht auf eine bestimmte Qualität der Daten ankommt, sondern auch die Gefährdung durch die Kumulation an sich wenig aussagekräftiger Daten erfasst ist.[87]

Als Ausdruck des Rechts auf informationelle Selbstbestimmung des Einzelnen spielt die Einwilligung eine wichtige Rolle:[88] Es liegt ebenso in der Hand des Betroffenen, seine Einwilligung zu verweigern wie sich bewusst für eine Preisgabe seiner personenbezogenen Daten zu entscheiden.

---

82 *BVerfG,* Urt. v. 15.12.1983, Az. 1 BvR 209/83, BVerfGE 65, 1 – Volkszählung.
83 *BVerfG,* Urt. v. 15.12.1983, Az. 1 BvR 209/83, BVerfGE 65, 1, 42 – Volkszählung.
84 *BVerfG,* Urt. v. 15.12.1983, Az. 1 BvR 209/83, BVerfGE 65, 1, 43– Volkszählung.
85 *Di Fabio*, in: Maunz/Dürig, GG, Art. 2, Rn. 173.
86 *BVerfG,* Urt. v. 15.12.1983, Az. 1 BvR 209/83, BVerfGE 65, 1, 45 – Volkszählung.
87 *Di Fabio*, in: Maunz/Dürig, GG, Art. 2, Rn. 174.
88 *Kühling/Seidel/Sivridis,* Datenschutzrecht, S. 143.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Das Recht am eigenen Bild ist eine Konkretisierung des Rechts auf informationelle Selbstbestimmung.[89] Es schützt den Einzelnen vor der Anfertigung, Zurschaustellung, Verbreitung und sonstigen Verwertung seines Abbildes.[90]

2. Schutz personenbezogener Daten

Auf Unionsebene gewährleistet Art. 8 GRCh ausdrücklich den Schutz personenbezogener Daten. Art. 8 GRCh verankert primärrechtlich zentrale Vorgaben des europäischen Datenschutzes, die zuvor bereits sekundärrechtlich in der DSRL festgehalten wurden:[91] So regelt Art. 8 Abs. 2 S. 1 GRCh ein Verbot mit Erlaubnisvorbehalt sowie den Zweckbindungsgrundsatz. Art. 8 Abs. 2 S. 2 GRCh setzt essentielle Betroffenenrechte fest: Der Betroffene soll ein Auskunfts- und Berichtigungsrecht haben. Gegenüber dem Recht auf Achtung des Privat- und Familienlebens aus Art. 7 GRCh ist Art. 8 GRCh für den Bereich des Datenschutzes lex specialis.[92]

II. Verarbeiter- und Drittinteressen

Auf Seiten der Verarbeiter sind zunächst die Interessen der Plattformbetreiber zu beachten. Hier kommt vorrangig das Interesse in Betracht, die Daten kommerziell zu nutzen. Auf Seiten der Nutzer, die Daten verarbeiten, kommt insbesondere das Recht auf Meinungsfreiheit in Betracht. Für Dritte spielt vor allem das Recht auf Informationsfreiheit eine Rolle.

1. Berufsfreiheit und unternehmerische Freiheit

Art. 12 Abs. 1 GG garantiert das Recht der Berufswahl und Berufsausübung. Vom Berufsbegriff umfasst ist auch die Freiheit, ein Gewerbe zu

89 *Di Fabio*, in: Maunz/Dürig, GG, Art. 2, Rn. 193.
90 *Di Fabio*, in: Maunz/Dürig, GG, Art. 2, Rn. 193.
91 *Nebel*, ZD 2015, 517, 521.
92 *Knecht*, in: Schwarze, EU-Kommentar, GRCh, Art. 8, Rn. 5; ausführlich zum Verhältnis von Art. 7 zu Art. 8 GRCh *Michl*, DuD 2017, 349.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

betreiben,[93] also auch die Tätigkeiten der Plattformbetreiber. Plattformbetreiber sind als juristische Personen auch vom persönlichen Schutzbereich umfasst, da die Berufsfreiheit ihrem Wesen nach auch auf juristische Personen anwendbar i. S. d. Art. 19 Abs. 3 GG ist,[94] sofern sich ihr Sitz im Inland befindet. Sitz meint dabei den „Ort der tatsächlichen Hauptverwaltung“[95].

Auf unionsrechtlicher Ebene ist der Schutz der unternehmerischen Freiheit aus Art. 16 GRCh für die wirtschaftliche Tätigkeit durch juristische Personen vorrangig zu Art. 15 GRCh;[96] Art. 16 GRCh schützt also auch juristische Personen.[97] Von seinem Schutz umfasst sind „[…] die Wirtschafts- und Geschäftstätigkeit, die Vertragsfreiheit, die Handelsfreiheit, die Werbefreiheit und die Wettbewerbsfreiheit […]“.[98]

2. Meinungs- und Informationsfreiheit

Im Grundgesetz ergibt sich die Meinungsäußerungsfreiheit aus Art. 5 Abs. 1 S. 1 Hs. 1 GG. Geschützt sind grundsätzlich alle Meinungsäußerungen, insbesondere bedarf es keiner besonderen Qualität der Meinung.[99]

Die Meinungsäußerungsfreiheit ist insbesondere im Nutzer-Nutzer-Verhältnis von Belang; sie erstreckt sich jedoch auch auf kommerzielle Meinungsäußerungen und ihr Schutz kann daher unter Umständen auch den

93 *BVerfG,* Beschl. v. 04.04.1967, Az. 1 BvR 84/65, BVerfGE 21, 261, 266 – Arbeitsvermittlungsmonopol.

94 stRspr *BVerfG,* Beschl. v. 04.04.1967, Az. 1 BvR 84/65, BVerfGE 21, 261, Rn. 15 – Arbeitsvermittlungsmonopol; *BVerfG,* Beschl. v. 29.11.1967, Az. 1 BvR 175/66, BVerfGE 22, 380, 383 – Kuponsteuer; *BVerfG,* Beschl. v. 16.03.1971, Az. 1 BvR 52/66, 1 BvR 665/66, 1 BvR 667/66, 1 BvR 754/66, BVerfGE 30, 292, 311 – Erdölbevorratung.

95 *Remmert*, in: Maunz/Dürig, GG, Art. 19, Rn. 78 m. w. N.

96 *Jarass*, GRCh, Art. 15, Rn. 9; ähnlich *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, GRCh, Art. 15, Rn. 8, der juristische Personen nicht vom persönlichen Schutzbereich des Art. 15 GRCh umfasst sieht; a. A. *Wollenschläger*, in: v. d. Groeben/Schwarze/Hatje, Europäisches Unionsrecht, GRCh, Vorb. zu Art. 15–16, Rn. 3 ff.

97 *Grabenwarter*, in: Grabenwarter, Europäischer Grundrechteschutz, § 13, Rn. 34.

98 *Schwarze*, in: Schwarze, EU-Kommentar, GRCh, Art. 8, Rn. 3., Rn. 7.

99 *Grabenwarter*, in: Maunz/Dürig, GG, Art. 5, Rn. 47.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Plattformbetreibern zukommen.[100] Dabei umfasst die Meinungsäußerungsfreiheit jedoch nicht Werbung jeglicher Art, sondern nur solche, die zum Meinungsprozess beiträgt.[101]

In der GRCh findet sich der Schutz der Meinungsäußerungsfreiheit in Art. 11. Die Meinungsäußerungsfreiheit aus Art. 11 Abs. 1 GRCh hat einen weiten Schutzbereich, der auch kommerzielle Meinungsäußerungen deckt.[102]

Die Informationsfreiheit im GG ergibt sich aus Art. 5 Abs. 1 S. 1 Hs. 2. Der Begriff der Informationsquelle ist weit zu verstehen[103] und umfasst also auch allgemein zugängliche Quellen aus dem Internet wie öffentliche Postings in sozialen Netzwerken. Auch die Informationsfreiheit aus Art. 11 Abs. 1 GRCh schützt den Empfang von Informationen aus dem Internet.[104] Sie entfaltet insbesondere Relevanz, wenn der Zugang zu Informationsquellen versperrt wird, etwa durch ein Löschungsgesuch des Betroffenen.

III. Zusammenfassung

Datenschutzrechtliche Sachverhalte sind geprägt von der Notwendigkeit, grundrechtlich verankerte Interessen miteinander abzuwägen. Diese Interessenabwägung ist in zahlreichen datenschutzrechtlichen sekundärrechtlichen wie einfachgesetzlichen Normen angelegt. Sie muss einzelfallbezogen erfolgen und ist oftmals zentrales Element bei der Beurteilung der Zulässigkeit der Verarbeitung personenbezogener Daten.[105]

---

100 *BVerfG,* Beschl. v. 19.11.1985, Az. 1 BvR 934/82, BVerfGE 71, 162 – Autobiographie eines Chefarztes.

101 Ausführlich *Kühling*, in: BeckOK InfoMedienR, GG, Art. 5, Rn. 26 ff.

102 *Walter*, in: Grabenwarter, Europäischer Grundrechteschutz, § 12, Rn. 11 f.

103 *Schemmer*, in: BeckOK GG, Art. 5, Rn. 25; *Kühling,* in: BeckOK InfoMedienR, GG, Art. 5, Rn. 40; *Fink,* in: Spindler/Schuster, Recht der elektronischen Medien, Erster Teil, Pkt. C.II., Rn. 12.

104 *Jarass*, GRCh, Art. 11, Rn. 15.

105 Eine detaillierte Bewertung der Abwägungskriterien erfolgt daher im Rahmen der Analyse der Zulässigkeitstatbestände selbst, vgl. etwa Kap. 3 Pkt. A.III.2.a.bb.iii, S. 120; Kap. 3 Pkt. A.III.2.c, S. 125.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kapitel 2: Territorial anwendbares Recht

A. Problemaufriss

> „As Rigaux quite rightly remarks, legislators have proceeded as if the entire phenomenon of automatic data processing was taking place within the borders. When they awoke to the fact that this was not so, they responded with a variety of measures which did not fill the gaps nor avoid clashes." (*Hondius*, 1983)[106]

Die Frage des territorial anwendbaren Rechts ist von besonderer Bedeutung für Konstellationen, denen typischerweise grenzüberschreitender Datenverkehr inhärent ist. Damit muss im Kontext von sozialen Netzwerken diese Frage beantwortet werden, noch bevor auf die materiell-rechtlichen Probleme eingegangen wird: Die sozialen Netzwerke mit den nach aktuellem Stand höchsten deutschen Nutzerzahlen sind vorwiegend US-amerikanische Unternehmen,[107] die nicht selten Niederlassungen in unterschiedlichen Mitgliedstaaten der EU unterhalten.[108]

Das Problem des territorial anwendbaren Rechts beschäftigt Literatur und Rechtsprechung gleichermaßen seit mehreren Jahrzehnten. So prangert etwa *Hondius* in seinem Text von 1983, bezugnehmend auf ein Zitat von *Rigaux* von 1980[109], das Fehlen klarer kollisionsrechtlicher Regelungen für das territorial anwendbare Recht in den „Leitlinien für den Schutz der Privatsphäre und des grenzüberschreitenden Datenverkehrs personenbezogener Daten"[110] der Organisation für wirtschaftliche Zusammenarbeit und

---

106 *Hondius*, NILR 1983, 103, 119.

107 Vgl. etwa *Facebook* und *Twitter* mit Hauptsitz in Kalifornien, *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017); *Twitter Inc.,* Twitter Nutzung / Fakten zum Unternehmen, abrufbar unter https://about.twitter.com/company (abgerufen am 13.10.2017).

108 Vgl. *Facebook* und *Twitter*, jeweils mit Büros u. a.in Berlin, Hamburg Amsterdam, Mailand, *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017); *Twitter Inc.*, Twitter Nutzung / Fakten zum Unternehmen, abrufbar unter https://about.twitter.com/company (abgerufen am 13.10.2017).

109 *Rigaux*, 60 Rev. crit. 1980, 443, 462.

110 *OECD*, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD-Dok, C(80)58/FINAL, abrufbar unter

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Entwicklung (OECD) an. Die Leitlinien der OECD waren das erste Regelwerk für den Schutz personenbezogener Daten über nationale Grenzen hinweg.[111] Mehr als ein Jahrzehnt später, im Jahr 1994, stellte *Korff* einleitend zu seiner Bewertung eines Entwurfs für die spätere DSRL fest: „Die zur Zeit geltenden nationalen Gesetze verursachen daher ernsthafte Gesetzeskonflikte: Bei grenzüberschreitenden oder internationalen Datenverarbeitungsvorgängen gelten häufig für nur einen Verarbeitungsvorgang oder einen Datensatz zwei (oder mehrere) Gesetze."[112] Im Jahr 2017 gibt es zwar mit Art. 4 Abs. 1 DSRL schon längst die erwünschte Kollisionsnorm, sie bereitet Rechtsprechung und Literatur jedoch nicht minder Kopfzerbrechen. So stellen *Kartheuser/Schmitt* zum *Weltimmo*-Urteil[113] des *EuGH* fest, dass das Urteil für Unternehmen bedeuten könne, dass sie potenziell mit der Anwendbarkeit mehrerer Datenschutzrechte rechnen müssten.[114] Es ist also festzustellen, dass trotz jahrzehntelanger Kritik an und Auseinandersetzung mit dem Problem des territorial anwendbaren Rechts nicht nur bislang noch keine endgültige Lösung gefunden wurde – die Kritik an der jeweils geltenden Rechtslage und die daraus resultierenden aufgezeigten Probleme für die Praxis gleichen sich damals wie heute in erstaunlichem Maße.

Das folgende Kapitel zeichnet die kollisionsrechtlichen Bestimmungen auf Unionsebene wie nationaler Ebene de lege lata nach und diskutiert ihre Auslegung durch Rechtsprechung und Literatur. Anschließend werden die Änderungen durch die ab dem 25. Mai 2018 geltende DSGVO[115] bewertet und beurteilt, ob mit ihr die nun jahrzehntelang bestehenden Unsicherheiten über das territorial anwendbare Recht im Datenschutz beseitigt werden.

---

http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&Lang=en&Book=False (abgerufen am 13.10.2017).

111 *OECD*, 2013 OECD Privacy Guidelines, abrufbar unter http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (abgerufen am 13.10.2017).

112 *Korff*, RDV 1994, 209.

113 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639 – Weltimmo; vgl. Kap. 2 Pkt. B.II, S. 59.

114 *Kartheuser/Schmitt*, ZD 2016, 155, 159.

115 Art. 99 Abs. 2 DSGVO.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

B. Datenschutzrechtliche Vorgaben der DSRL

Die Frage des territorial anwendbaren mitgliedstaatlichen Rechts ist in der DSRL in Art. 4 geregelt und wird zusätzlich in EG 18 bis 20 DSRL behandelt; im BDSG wurde die Norm in § 1 Abs. 5 umgesetzt[116]. Art. 4 DSRL verfolgt ausweislich der Begründung des Entwurfs zwei Ziele: Erstens sollen Datensubjekte davor geschützt werden, rechtsschutzlos zu stehen, indem der für die Verarbeitung Verantwortliche sich dem Recht entzieht. Zweitens soll für denselben Verarbeitungsvorgang nicht mehr als das Recht eines Mitgliedstaats Anwendung finden.[117] Im ursprünglichen von der Kommission im Jahr 1990 vorgelegten Entwurf für die Richtlinie stellte Art. 4 Abs. 1 lit. a noch auf den Standort der Daten ab.[118] Dieses Kriterium wurde jedoch rasch aufgegeben, da der Standort der Daten (damals wie heute) regelmäßig schwer zu bestimmen ist.[119] Stattdessen wurde das Niederlassungsprinzip gewählt, das schließlich auch in Art. 4 Abs. 1 lit. a DSRL Eingang gefunden hat: Die Norm bestimmt, dass das Recht des Mitgliedstaates auf alle Verarbeitungen (i. S. d. Art. 2 lit. b DSRL) personenbezogener Daten anwendbar ist, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wurden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaates besitzt. Selbiges gilt, wenn sich die Niederlassung zwar nicht im Hoheitsgebiet dieses Mitgliedstaates befindet, jedoch an einem Ort, in dem nach internationalem öffentlichen Recht das Recht dieses Mitgliedstaates anwendbar ist, Art. 4 Abs. 1 lit. b DSRL. Gem. Art. 4 Abs. 1 lit. c DSRL sind die Vorschriften des Mitgliedstaates auf alle Verarbeitungen anwendbar, die von einem für die Verarbeitung Verantwortlichen ausgeführt werden, der nicht im Gebiet der EU niedergelassen ist und zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese

116 *Dammann*, in: Simitis, BDSG, § 1, Rn. 198 und 217, dort mit Verweis auf Art. 4 Abs. 1 lit. c DSRL in Fn. 562.

117 Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM(90) 314 final – SYN 287, Abl.EG 1990 C 277, 3, S. 21 f.; Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 13.

118 COM(90) 314 final – SYN 287, Abl.EG 1990 C 277, 3.

119 COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 13.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Mittel nur zum Zweck der Durchfuhr durch das Gebiet der EU verwendet werden. Art. 4 Abs. 1 lit. c DSRL ist also nur dann anwendbar, wenn keine Niederlassung in dem Mitgliedstaat, dessen Recht angewendet werden soll, besteht. Die Auslegung des Niederlassungsbegriffs i. S. d. DSRL ist damit der zentrale Punkt zur Identifikation der einschlägigen Norm.[120]

Die Vorgaben des Art. 4 DSRL sind mit § 1 Abs. 5 BDSG in deutsches Recht umgesetzt worden. Dabei weicht der Wortlaut des § 1 Abs. 5 BDSG teilweise sinnverändernd von Art. 4 Abs. 1 DSRL ab. § 1 Abs. 5 S. 1 BDSG, der Art. 4 Abs. 1 lit. a DSRL umsetzt[121], sieht vor, dass das BDSG keine Anwendung findet, „[…] sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland.“ Nach Art. 4 Abs. 1 lit. a DSRL muss die Verarbeitung[122] jedoch nur „im Rahmen der Tätigkeiten einer Niederlassung“ und nicht „durch die Niederlassung“ geschehen, stellt also geringere Anforderungen an die Rolle der Niederlassung.[123] § 1 Abs. 5 S. 1 BDSG ist jedenfalls nicht zu entnehmen, dass allein die Existenz einer Niederlassung im Inland als Anknüpfungspunkt für die Anwendbarkeit deutschen Datenschutzrechts ausreicht.[124] Das ergibt sich aus dem Wort „dies“ in § 1 Abs. 5 S. 1 Hs. 2 BDSG, mit dem eine anaphorische Verbindung zur Erhebung, Verarbeitung und Nutzung aus § 1 Abs. 5 S. 1 Hs. 1 BDSG hergestellt wird.[125]

Ferner bestimmt § 1 Abs. 5 S. 2 BDSG, der Art. 4 Abs. 1 lit. c DSRL umsetzt,[126] dass das BDSG anwendbar ist, „[…] sofern eine verantwortliche

120 Vgl. sogleich, Kap. 2 Pkt. B.II.1, S. 60.
121 *Dammann*, in: Simitis, BDSG, § 1, Rn. 198.
122 Verarbeitung i. S. d. DSRL schließt die Erhebung und Nutzung ein, Art. 2 lit. b.
123 Vgl. zum Merkmal „im Rahmen der Tätigkeiten“ aus Art. 4 Abs. 1 lit. a DSRL Kap. 2 Pkt. B.II.1.c, S. 62.
124 *Dammann*, in: Simitis, BDSG, § 1, Rn. 201; a. A. wohl *VG Schleswig,* Beschl. v. 14.02.2013, Az. 8 B 60/12, ZD 2013, 245, 246, mit dem Verweis, dass § 1 Abs. 5 S. 1 BDSG richtlinienkonform dahingehend auszulegen sei, dass sich das „Vorhandensein einer Niederlassung […] *nur* [Hervorh. durch die Verf.] soweit erstreck[e], wie die Verarbeitung personenbezogener Daten durch die Niederlassung in Rede steh[e].“ Tatsächlich ist das BDSG sogar enger gefasst als Art. 4 Abs. 1 lit. a DSRL, der nur eine Verarbeitung „im Rahmen der Tätigkeiten“ und nicht „von“ der Niederlassung fordert, vgl. Kap. 2 Pkt. B.II.1.c, S. 62.
125 Vgl. *Bußmann,* Lexikon der Sprachwissenschaft, Punkt „Anapher”.
126 *Dammann*, in: Simitis, BDSG, § 1, Rn. 217 mit Verweis auf Art. 4 Abs. 1 lit. c DSRL in Fn. 562.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt." Statt von einem Rückgriff auf im entsprechenden Mitgliedstaat belegenen Mittel[127] spricht § 1 Abs. 5 S. 2 BDSG also von einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten „im Inland". Dieser Unterschied im Wortlaut wird meist zu keiner unterschiedlichen Bewertung führen, da die „Mittel" i. S. d. Art. 4 Abs. 1 lit. c DSRL gleichfalls im Mitgliedstaat – identisch mit dem Inlandsbegriff aus § 1 Abs. 5 S. 1 BDSG, sofern es sich um Deutschland handelt – belegen sein müssen. Andernfalls müsste im entsprechenden Fall § 1 Abs. 5 S. 2 BDSG richtlinienkonform ausgelegt werden.[128] Da das BDSG keine Definition des Niederlassungsbegriffs enthält, ist auf den Niederlassungsbegriff aus EG 19 DSRL zurückzugreifen.[129]

I. Für die Verarbeitung Verantwortlicher i. S. d. Art. 4 Abs. 1 DSRL

Sowohl Art. 4 Abs. 1 DSRL als auch § 1 Abs. 5 BDSG gehen auf den Begriff des für die Verarbeitung Verantwortlichen bzw. die verantwortliche Stelle[130] einerseits und auf den Begriff der Niederlassung andererseits ein. Für die Verarbeitung Verantwortlicher ist gem. Art. 2 lit. d DSRL „[…] die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. […]".[131] Gem. EG 19 S. 1 DSRL setzt „[e]ine Niederlassung im Hoheitsgebiet eines Mitgliedstaats […] die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus." Da die großen sozialen Netzwerke neben ihrem Hauptsitz auch Dependancen in der ganzen Welt und insbesondere auch in der EU unterhalten[132], stellt sich bei Art. 4 Abs. 1 lit. a

127 Vgl. Kap. 2 Pkt. B.III, S. 79.
128 So auch *Dammann*, in: Simitis, BDSG, § 1, Rn. 217.
129 Vgl. auch *Dammann*, in: Simitis, BDSG, § 1, Rn. 200; *Gabel*, in: Taeger/Gabel, BDSG, § 1, Rn. 55.
130 Zu den terminologischen Unterschieden zwischen DSRL und BDSG vgl. Kap. 1 Pkt. A, S. 31.
131 Vgl. korrespondierend hierzu § 3 Abs. 7 BDSG.
132 Vgl. etwa *Facebook* mit Dependancen in Amsterdam, Dublin, Hamburg, Warschau u. v. m., *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

DSRL zunächst die Frage, welche Auswirkungen diese konzernrechtlichen Verflechtungen auf die Bestimmung des territorial anwendbaren Rechts haben.

1. Verantwortlichkeit bei mehreren Niederlassungen

Sowohl Art. 4 Abs. 1 lit. a DSRL als auch § 1 Abs. 5 S. 1 BDSG differenzieren zwischen dem für die Verarbeitung Verantwortlichen bzw. der verantwortlichen Stelle einerseits und der Niederlassung andererseits. Daraus lässt sich ableiten, dass in den Fällen mehrerer Niederlassungen die Benennung des für die Verarbeitung Verantwortlichen lediglich in dem Zusammenhang relevant ist, ob er eine Niederlassung[133] im jeweiligen Mitgliedstaat unterhält. Denn aus den Normen lässt sich nicht herauslesen, dass die Niederlassung zugleich verantwortliche Stelle sein muss.[134] Entscheidendes Merkmal ist damit, *ob* und *wo* der für die Verarbeitung Verantwortliche Niederlassungen unterhält und deren Verbindung zur in Frage stehenden Verarbeitung[135]. Es kommt demnach in diesem Zusammenhang auch nicht darauf an, ob die in Frage stehende Niederlassung Auftragsdatenverarbeiter i. S. d. Art. 2 lit. e DSRL bzw. § 11 BDSG ist,[136] sondern lediglich, ob die Verarbeitung „im Rahmen der Tätigkeiten einer Niederlassung" i. S. d. Art. 4 Abs. 1 lit. a DSRL erfolgt. Datenschutzrechtlich denkbar ist auch eine gemeinsame Verantwortlichkeit von Niederlassung und Mutterkonzern, da es grundsätzlich auch mehr als einen für die Verarbeitung Verantwortlichen geben kann, wie die Formulierung „allein oder gemeinsam" in Art. 2 lit. d DSRL klarstellt.[137] Zwar macht der Wortlaut von Art. 4 Abs. 1 lit. a DSRL und § 1 Abs. 5 BDSG deutlich, dass zwischen Niederlassung und für die Verarbeitung Verantwortlichen zu unterscheiden ist. Daraus lässt sich jedoch nur herauslesen, dass die Niederlassung nicht zwingend

133 Zum Niederlassungsbegriff vgl. sogleich, Kap. 2 Pkt. B.II, S. 59.

134 So auch *VG Schleswig,* Beschl. v. 14.02.2013, Az. 8 B 60/12, ZD 2013, 245, 246; bestätigt in *OVG Schleswig,* Beschl. v. 22.04.2013, Az. 4 MB 11/13, ZD 2013, 364, 365 f.

135 Dazu sogleich unter Kap. 2 Pkt. B.II, S. 59.

136 *OVG Schleswig,* Beschl. v. 22.04.2013, Az. 4 MB 11/13, ZD 2013, 364, 365; a. A. *Dammann*, in: Simitis, BDSG, § 1, Rn. 201; *Gabel*, in: Taeger/Gabel, BDSG, § 1, Rn. 55.

137 *Dammann*, in: Simitis, BDSG, § 3, Rn. 226; *Schild*, in: BeckOK DatenschutzR, BDSG, § 3, Rn 112.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

auch für die Verarbeitung Verantwortlicher sein *muss*, nicht jedoch, dass sie es nicht sein *darf*.

2. Konsequenzen am Beispiel von *Facebook*

Damit kommt es bei solchen konzernrechtlichen Verflechtungen, z. B. bei Vorliegen verschiedener Niederlassungen neben dem Mutterkonzern, für die Bestimmung des territorial anwendbaren Rechts insbesondere auf die Klärung der Frage an, im Rahmen der Tätigkeiten *wessen* Niederlassung die Verarbeitung ausgeführt wird. Die datenschutzrechtliche Verantwortlichkeit ist von der gesellschaftsrechtlichen Struktur eines Konzerns unabhängig, womit auch unabhängige Niederlassungen für die Verarbeitung Verantwortliche sein können.[138] Dies wird etwa am Beispiel der Konzernstruktur des sozialen Netzwerks *Facebook* deutlich: Der Mutterkonzern *Facebook Inc.* hat seine Hauptniederlassung in den USA[139]. Gleichzeitig unterhält *Facebook Inc.* im gesellschaftsrechtlichen Sinne eine Niederlassung in Irland, *Facebook Ireland Ltd.*[140]. Diese Niederlassung ist gem. Punkt 18.1 in den AGB[141] offizieller Geschäftspartner aller Nutzer außerhalb der USA und Kanadas. Zugleich ist *Facebook Ireland Ltd.* nach einer konzerninternen Zuweisung für die Verarbeitung Verantwortliche.[142] Ob allein die vertragliche Zuweisung *Facebook Ireland Ltd.* auch datenschutzrechtlich zur für die Verarbeitung Verantwortlichen macht, ist bislang umstritten und liegt derzeit im Rahmen eines Vorabentscheidungsverfahrens dem *EuGH*

---

138 *Weichert*, in: DKWW, BDSG, § 3 Rn. 59.

139 Vgl. Eintragung im kalifornischen Handelsregister des California Secretary of State, abrufbar unter http://kepler.sos.ca.gov/ (abgerufen am 13.10.2017).

140 Vgl. Eintragung im irischen Handelsregister des Companies Registration Office, abrufbar unter https://search.cro.ie/company/CompanyDetails.aspx?id=462932&type=C (abgerufen am 13.10.2017).

141 *Facebook Inc.,* Erklärung der Rechte und Pflichten, abrufbar unter https://www.facebook.com/legal/terms (abgerufen am 13.10.2017).

142 Zuweisung nach einem „Data Processing Agreement" (Deutsch: Vereinbarung über Auftragsdatenverarbeitung) zwischen *Facebook Inc.* und *Facebook Ireland Ltd.* Das „Data Processing Agreement" war u. a. Gegenstand in dem Verfahren *OVG Schleswig,* Beschl. v. 22.04.2013, Az. 4 MB 11/13, ZD 2013, 364, 365 f. und wurde dem *EuGH* nun zur Klärung vorgelegt, *EuGH,* Vorabentscheidungsersuchen des BVerwG v. 14.04.2016, Rs. C-210/16, ABl.EU 2016 C 260, 18 – Wirtschaftsakademie Schleswig-Holstein; *BVerwG,* EuGH-Vorlage v. 25.02.2016, Az. 1 C 28/14, NVwZ 2016, 1737; hierauf verweisend *OVG Hamburg,* Beschl. v. 29.06.2016, Az. 5 Bs 40/16, CR 2016, 576.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

vor.[143] Aus datenschutzrechtlicher Hinsicht macht es jedoch keinen entscheidenden Unterschied, welche Dependance innerhalb des Konzerns für die Verarbeitung Verantwortliche ist. Denn wenn man *Facebook Inc.* als Verantwortliche ansieht, muss man davon ausgehen, dass *Facebook Inc.* auf dem Unionsgebiet mehrere Niederlassungen unterhält, u. a. *Facebook Ireland Ltd.* und *Facebook Germany GmbH*[144]. Sieht man jedoch *Facebook Ireland Ltd.* als für die Verarbeitung Verantwortliche an, muss man davon ausgehen, dass die *Facebook Germany GmbH* als Niederlassung der *Facebook Ireland Ltd.* zu werten ist. Auf die tatsächliche konzerninterne Stellung kommt es nämlich datenschutzrechtlich nicht an. Die *Facebook Germany GmbH* erfüllt auch alle Anforderungen an eine Niederlassung i. S. d. Art. 4 Abs. 1 i. V. m. EG 19 DSRL.[145] Denkbar wäre auch, dass die *Facebook Germany GmbH* als für die Verarbeitung Verantwortliche gilt. Dafür müsste sie über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Nach eigenen Angaben ist die *Facebook Germany GmbH* im Bereich der Anzeigenakquise und des Marketings tätig und nimmt keine Verarbeitung von personenbezogenen Daten vor.[146] Über die datenschutzrechtliche Verantwortlichkeit gibt Letzteres jedoch noch keinen Aufschluss, da es hierfür nicht auf den Ort der Datenverarbeitung ankommt.[147] Dies wird schon durch die Möglichkeit der Auftragsdatenverarbeitung klar, § 11 Abs. 1 BDSG bzw. Art. 2 lit. e DSRL, in deren Rahmen die Verarbeitung von einem anderen als dem für die Verarbeitung Verantwortlichen vorgenommen wird. Für die Bestimmung, ob deutsches Datenschutzrecht anwendbar ist, ist jedoch nur wichtig, ob die *Facebook Germany GmbH* mindestens eine Niederlassung darstellt, *in deren Rahmen* die Verarbeitung personenbezogener Daten ausgeführt wird,[148] Art. 4 Abs. 1 lit. a DSRL, oder ob *Facebook Inc.* überhaupt keine Niederlassungen auf

143 *EuGH,* Vorabentscheidungsersuchen des BVerwG v. 14.04.2016, Rs. C-210/16, ABl.EU 2016 C 260, 18 – Wirtschaftsakademie Schleswig-Holstein; *BVerwG,* EuGH-Vorlage v. 25.02.2016, Az. 1 C 28/14, NVwZ 2016, 1737; vgl. sogleich Kap. 2 Pkt. B.I.3, S. 58.

144 Vgl. Eintragung ins Handelsregister B des AG Hamburg, Abteilung B, Wiedergabe des aktuellen Registerinhalts, abrufbar unter https://www.unternehmensregister.de/ureg/ (abgerufen am 13.10.2017).

145 Vgl. Kap. 2 Pkt. B.II.1.c, S. 62.

146 Vgl. etwa Angaben im Verfahren *OVG Schleswig,* Beschl. v. 22.04.2013, Az. 4 MB 11/13, ZD 2013, 364, 365 f.

147 *Weichert*, in: DKWW, BDSG, § 3, Rn. 56; *Dammann*, in: Simitis, BDSG, § 3, Rn. 225.

148 Vgl. Kap. 2 Pkt. B.II.1.c, S. 62.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

dem Gebiet der EU i. S. d. Art. 4 Abs. 1 lit. c DSRL bzw. § 1 Abs. 5 S. 1 Hs. 2 BDSG hat.
Daraus ergeben sich folgende Möglichkeiten:

Für die Verarbeitung Verantwortliche	**Niederlassung**	**Konsequenz**
Facebook Inc.	*Facebook Ireland Ltd.* und *Facebook Germany GmbH*	Deutsches Datenschutzrecht anwendbar, wenn: • Relevante Verarbeitung „im Rahmen der Tätigkeiten" der *Facebook Germany GmbH*, Art. 4 Abs. 1 lit. a DSRL bzw. § 1 Abs. 5 S. 1 Hs. 2 BDSG. • Relevante Verarbeitung weder „im Rahmen der Tätigkeiten" der *Facebook Germany GmbH*, noch der *Facebook Ireland Ltd.*, aber Rückgriff auf Mittel in Deutschland, Art. 4 Abs. 1 lit. c DSRL bzw. § 1 Abs. 5 S. 2 BDSG.
Facebook Ireland Ltd.	*Facebook Germany GmbH*	• Deutsches Datenschutzrecht anwendbar, wenn relevante Verarbeitung „im Rahmen der Tätigkeiten" der *Facebook Germany GmbH*, Art. 4 Abs. 1 lit. a DSRL bzw. § 1 Abs. 5 S. 1 HS. 2 BDSG. • Irisches Recht anwendbar, wenn relevante Verarbeitung nicht im Rahmen der Tätigkeiten der *Facebook Germany GmbH*, Art. 4 Abs. 1 lit. a DSRL bzw. § 1 Abs. 5 S. 1 Hs. 1 BDSG.
Facebook Germany GmbH	-	Deutsches Datenschutzrecht anwendbar gem. Art. 4 Abs. 1 lit. a DSRL bzw. wegen Territorialprinzips des BDSG[149].

149 *Dammann*, in: Simitis, BDSG, § 3, Rn. 208.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Wie die Tabelle zeigt, kommt es bei konzernrechtlichen Verflechtungen zur Bestimmung des räumlichen Anwendungsbereichs der DSRL bzw. mitgliedstaatlicher Datenschutzbestimmungen nicht darauf an, wer für die Verarbeitung Verantwortlicher ist, sondern ob eine Niederlassung i. S. d. DSRL vorliegt und die Verarbeitung im Rahmen der Tätigkeiten dieser Niederlassung stattfindet. Dementsprechend wird im Folgenden auf den datenschutzrechtlichen Niederlassungsbegriff unter Einbeziehung der Rechtsprechung eingegangen.

3. Zulässigkeit einer rechtlichen Zuweisung der Verantwortlichkeit

Die Verantwortlichkeit kann im Übrigen nicht durch eine rein rechtliche Zuweisung übertragen werden. Die Frage stellt sich etwa bei *Facebook Inc.*, das im Rahmen eines „Data Processing Agreements" die rechtliche Verantwortlichkeit für bestimmte Datenkategorien an die *Facebook Ireland Ltd.* übertragen hat. Im Rahmen eines Verfahrens vor dem *OVG Schleswig* hatte das ULD argumentiert, dass sich nicht bereits aus dem „Data Processing Agreement" ergebe, dass *Facebook Ireland Ltd.* verantwortliche Stelle sei und damit irisches Datenschutzrecht zur Anwendung komme.[150] Wie bereits dargestellt, kommt es im Rahmen des territorial anwendbaren Rechts im Anwendungsbereich des Art. 4 Abs. 1 lit. a DSRL (Niederlassung des Unternehmens auf dem Gebiet der EU/des EWR) aber nicht darauf an, wer verantwortliche Stelle ist, sondern ob die Datenverarbeitung im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird.[151] Diese Frage kann nicht durch rechtliche Zuweisung der Verantwortlichkeit geklärt werden. Nach dem Wortlaut des Art. 4 Abs. 1 lit. a DSRL geht es hier um die tatsächliche Tätigkeit, nicht um rechtliche Zuweisungen. Auch teleologisch kann eine rechtliche Zuweisung der Verantwortlichkeit nicht als Anknüpfungspunkt für die Bestimmung des territorial anwendbaren Rechts dienen, da so die rechtlichen Bestimmungen des Art. 4 Abs. 1 DSRL ausgehebelt werden könnten.[152]

---

150 *OVG Schleswig,* Beschl. v. 22.04.2013, Az. 4 MB 11/13, ZD 2013, 364, 365 f.; vgl. auch *OVG Hamburg,* Beschl. v. 29.06.2016, Az. 5 Bs 40/16, CR 2016, 576, 576 f.

151 Vgl. ausführlich Kap. 2 Pkt. B.I., S. 53.

152 Die Frage, ob sich kontrollbehördliche Maßnahmen auch gegen die nicht konzernintern verantwortliche Niederlassung richten dürfen, liegt derzeit dem *EuGH* vor, *EuGH,* Vorabentscheidungsersuchen des BVerwG v. 14.04.2016,

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

II. Niederlassung i. S. d. Art. 4 Abs. 1 lit. a DSRL

Das Vorliegen einer Niederlassung in einem Mitgliedstaat ist ein zentraler Faktor für die territoriale Anwendbarkeit des Datenschutzrechts dieses Mitgliedstaats. Für die Bestimmung des territorial anwendbaren Rechts kommt es damit grundlegend auf die Auslegung des Niederlassungsbegriffs an. Dementsprechend war die Auslegung des Art. 4 Abs. 1 DSRL und insbesondere des Niederlassungsbegriffs jüngst Gegenstand von zwei Verfahren vor dem *EuGH*, den Entscheidungen *Google Spain und Google*[153] und *Weltimmo*[154]. Die Sachverhalte beider Fälle spielten sich im Internet ab und befassten sich mit Unternehmen, die zu dem entsprechenden Mitgliedstaat zwar Anknüpfungspunkte aufwiesen, welche jedoch nicht hauptsächlich in der Verarbeitung der personenbezogenen Daten bestanden: In dem Fall *Google Spain und Google* ging es um die Frage, ob spanisches Recht auch dann anwendbar ist, wenn der Suchmaschinenbetreiber Google in Spanien eine Dependance hat, die für die Förderung des Verkaufs der Werbeflächen zuständig ist.[155] Der Fall *Weltimmo* betraf ein Unternehmen, das seine offizielle Niederlassung zwar in der Slowakei unterhielt, jedoch eine ungarischsprachige Website betrieb, auf der die Nutzer Immobilien in Ungarn zur Veräußerung oder zur Miete anbieten konnten und die für die Eintreibung offener Forderungen einen Vertreter in Ungarn sowie ein Bankkonto in Ungarn hatte.[156]

Der Niederlassungsbegriff wird in der DSRL selbst nicht definiert, jedoch in EG 19 näher bestimmt. Nach EG 19 S. 1 der DSRL setzt „[e]ine Niederlassung […] die effektive und tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus." Nach EG 19 S. 2 der DSRL ist dabei die Rechtsform nicht von Bedeutung. Für das Vorliegen einer Niederlassung i. S. d. DSRL müssen kumulativ also zwei Dinge vorliegen: Eine feste Einrichtung (dazu 1.a.) und die effektive und tatsächliche Ausübung

---

Rs. C-210/16, ABl.EU 2016 C 260, 18 – Wirtschaftsakademie Schleswig-Holstein.

153 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google Spain und Google.

154 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639 – Weltimmo.

155 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 45 – Google Spain und Google.

156 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 16, 19 – Weltimmo.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

einer Tätigkeit (dazu 1.b.). Ferner muss die Verarbeitung personenbezogener Daten gem. Art. 4 Abs. 1 lit. a DSRL im Rahmen der Tätigkeiten dieser Niederlassung stattfinden (dazu 1.c.).

1. Merkmale des Niederlassungsbegriffs

a) Vorliegen einer festen Einrichtung

Fraglich ist, wann eine „feste Einrichtung" i. S. d. EG 19 S. 1 DSRL vorliegt. Im Fall *Google Spain und Google* stand das Bestehen einer festen Einrichtung nicht in Frage[157], da *Google Spain* eine Tochtergesellschaft mit eigener Rechtspersönlichkeit und Sitz in Madrid ist[158]. Im Fall *Weltimmo* hatte der *EuGH* hingegen über die Frage zu entscheiden, ob eine feste Einrichtung i. S. d. EG 19 DSRL vorliegt, wenn das Unternehmen keine Dependance in dem Mitgliedstaat, dessen Datenschutzrecht angewendet werden soll (in diesem Fall Ungarn), unterhält. Die Anknüpfungspunkte an den Mitgliedstaat bestanden im Fall *Weltimmo* in einem ungarischen Bankkonto zur Einziehung der Forderungen, einer Website in ungarischer Sprache, einem Postfach in Ungarn und einem Vertreter, der im slowakischen Handelsregister eingetragen war, jedoch unter ungarischer Adresse.[159] Der *EuGH* führte dazu in Anlehnung an die Schlussanträge von *GA Cruz Villalón* aus, dass die DSRL eine flexible Konzeption des Niederlassungsbegriffs vorsehe, die Abstand von einer formalistischen Sichtweise nehme, nach der ein Unternehmen ausschließlich an dem Ort niedergelassen sein könne, an dem es eingetragen sei. Daraus schloss der *EuGH*, dass der Grad der Beständigkeit der Einrichtung und die effektive Ausübung unter Beachtung des besonderen Charakters der angebotenen Dienstleistung ausgelegt werden müsse.[160] *GA Cruz Villalón* hatte zuvor in seinen Schlussanträgen außerdem den besonderen Charakter von Unternehmen, die ausschließlich über das Internet tätig werden, hervorgehoben: In diesen Fällen werde der

157 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 49 – Google Spain und Google.
158 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 43 – Google Spain und Google.
159 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639 – Weltimmo.
160 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 29; *GA Cruz Villalón,* Schlussanträge v. 25.06.2015, Rs. C-230/14, ECLI:EU:C:2015:426, Rn. 28, 32 – Weltimmo.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Begriff der ständigen körperlichen Einrichtung relativiert und die Intensität der personellen und sachlichen Mittel beeinflusst.[161]

Diese Auslegung ist zu begrüßen. Die DSRL stellt keine Anforderungen an die Qualität der „festen Einrichtung". In der englischen Fassung fordert EG 19 S. 1 DSRL „[…] the effective and real exercise of activity through *stable arrangements* [Hervorh. durch die Verf.] […]". "[S]table arrangements" lässt sich zwar durchaus als „feste Einrichtung" übersetzen, jedoch wäre ebenso eine Übersetzung als „beständige Regelung" möglich. Im Übrigen kann die Wendung „feste Einrichtung" zwar auch so ausgelegt werden, dass die Niederlassung eine festgelegte Örtlichkeit erfordert, dies ist jedoch keineswegs zwingend. Ebenso wenig ist dieses Erfordernis aus der englischen Wendung des „stable arrangement[ ]" oder des französischen Begriffs des „établissement" unbedingt herauszulesen. Die Auslegung durch *GA Cruz Villalón*, der von einer „körperlichen Einrichtung"[162] spricht, ist demnach keineswegs die einzig mögliche Deutungsweise. *GA Cruz Villalón* kommt über eine teleologische Auslegung schließlich zum selben Ergebnis, indem er auf die Relativierung des Begriffs der ständigen körperlichen Einrichtung durch das digitale Zeitalter[163] hinweist. Wie gezeigt hätte es dieses Hinweises aber gar nicht bedurft. Denn ein Bankkonto lässt sich als „stable arrangement[ ]" i. S. d. DSRL qualifizieren und lässt sich ebenso unter den Begriff der „festen Einrichtung" subsumieren. Damit genügt eine Ausganslage wie im Fall *Weltimmo* dem Kriterium der festen Einrichtung i. S. d. EG 19 S. 1 DSRL.[164]

b) Effektive und tatsächliche Ausübung einer Tätigkeit

Auch an das Merkmal der „effektive[n] und tatsächliche[n] Ausübung einer Tätigkeit" stellt die DSRL keiner weiteren Anforderungen. Somit reichen bereits geringfügige Tätigkeiten zur Erfüllung dieses Merkmals aus, solange sie nur „effektiv und tatsächlich" sind. Nicht zuzustimmen ist insoweit dem *KG Berlin*, das eine „[…] eigene und effektive Datenverarbeitung

161 *GA Cruz Villalón,* Schlussanträge v. 25.06.2015, Rs. C-230/14, ECLI:EU:C:2015:426, Rn. 34 – Weltimmo.
162 *GA Cruz Villalón,* Schlussanträge v. 25.06.2015, Rs. C-230/14, ECLI:EU:C:2015:426, Rn. 34 – Weltimmo.
163 *GA Cruz Villalón,* Schlussanträge v. 25.06.2015, Rs. C-230/14, ECLI:EU:C:2015:426, Rn. 34 – Weltimmo.
164 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 32 f. – Weltimmo.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

(mittels eigener Datenverarbeitungsanlagen und eigenem Personal) […]“ fordert.[165] Es ergeben sich aus dem Wortlaut des EG 19 S. 1 DSRL keine Anhaltspunkte dafür, dass die Tätigkeit die Datenverarbeitung selbst sein muss.[166] Dies stünde auch im Widerspruch zu Art. 4 Abs. 1 lit. a S. 1, der die Datenverarbeitung lediglich im „Rahmen der Tätigkeiten einer Niederlassung“ erfordert und gerade nicht „von“ der Niederlassung.[167] Das Merkmal der „effektive[n] und tatsächliche[n] Ausübung einer Tätigkeit“ ist damit bereits bei dem Betreiben einer oder mehrerer Websites erfüllt.[168]

c) Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung i. S. d. Art. 4 Abs. 1 lit. a DSRL

Art. 4 Abs. 1 lit. a DSRL verlangt neben dem Vorliegen einer Niederlassung in dem Hoheitsgebiet des Mitgliedstaates, dessen Recht angewendet werden soll, dass die Verarbeitung personenbezogener Daten „im Rahmen der Tätigkeiten“ einer Niederlassung ausgeführt werden muss. Dieses Merkmal ist ein zentrales Auslegungselement des Art. 4 Abs. 1 lit. a DSRL, da seine Interpretation entscheidend die Tragweite einer Niederlassung als Anknüpfungspunkt für das territorial anwendbare Recht mitbestimmt.

Zunächst wurde das Merkmal überwiegend derart ausgelegt, dass die Verarbeitung „von“ der Niederlassung ausgeführt werden müsse. So gingen etwa das *VG Schleswig* wie auch das *OVG Schleswig* davon aus, dass sich an die Existenz der *Facebook Germany GmbH* keine Anwendbarkeit deutschen Datenschutzrechts knüpfen lasse, da sie nur im Bereich der Anzeigenakquise und des Marketings tätig sei und eine Verarbeitung personenbezogener Daten dort nicht stattfinde.[169] Allerdings käme das Abstellen auf

---

165 *KG Berlin,* 24.01.2014, Az. 5 U 42/12, ZD 2014, 412, 415; dem *KG Berlin* wohl zustimmend *Maisch,* Informationelle Selbstbestimmung in Netzwerken, S. 183 f.

166 A. A. wohl *Kampert,* Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, S. 152, der eine Kontrolle oder Einbeziehung der Niederlassung in die konkrete Datenverarbeitung fordert.

167 Vgl. Kap. 2 Pkt. B.II.1.c, S. 62.

168 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 31 – Weltimmo.

169 *VG Schleswig,* Beschl. v. 14.02.2013, Az. 8 B 60/12, ZD 2013, 245, 246; bestätigt in *OVG Schleswig,* Beschl. v. 22.04.2013, Az. 4 MB 11/13, ZD 2013, 364,365 f.; fraglich ist, ob das *OVG Schleswig* als letztinstanzliche Gericht hier nicht seine Vorlagepflicht aus Art. 267 AUV verletzt hat. Zur Kritik an der Zurückhaltung deutscher Gerichte bei der Vorlage vgl. *Kühling*, EuZW 2013, 641.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

den Ort der Datenverarbeitung einem Abstellen auf den Ort der Daten gleich, einem Merkmal, das gerade keinen Eingang in die finale Fassung von Art. 4 DSRL gefunden hat.[170] Mit Blick auf die zahlreichen Serverfarmen von großen Unternehmen und der Möglichkeit, Daten je nach Speicherkapazität ständig zu verschieben,[171] wäre dies auch nicht zielführend.

Zudem lässt sich diese Auslegung nicht mit dem Wortlaut des Art. 4 Abs. 1 lit. a DSRL vereinen. Der Wortlaut spricht gerade nicht davon, dass die Verarbeitung personenbezogener Daten „von der Niederlassung", sondern „im Rahmen der Tätigkeiten einer Niederlassung" ausgeführt werde. Dieses Ergebnis hat auch der *EuGH* im Fall *Google Spain und Google* in seiner Wortlautanalyse des Art. 4 Abs. 1 lit. a DSRL zu Recht betont.[172] Nach der grammatikalischen Auslegung des Art. 4 Abs. 1 lit. a DSRL muss die Niederlassung die Verarbeitung personenbezogener Daten demnach nicht selbst vornehmen.

Nach Ansicht des *Gerichtshofs* liegt – entgegen der eingangs erwähnten Urteile – eine Verarbeitung „im Rahmen der Tätigkeiten einer Niederlassung" auch dann vor, wenn eine Dependance lediglich im Bereich des Verkaufs von Werbeflächen tätig ist; die Werbetätigkeit sei untrennbar mit der Tätigkeit einer Suchmaschine verbunden, da sie dadurch erst wirtschaftlich rentabel gemacht werde und daher die Verarbeitung auch „im Rahmen der Tätigkeiten" der Niederlassung ausgeführt werde.[173]

Dieser Auslegung ist zuzustimmen. Wie gezeigt finanzieren sich die meisten sozialen Netzwerke gerade durch Werbeeinnahmen. So gehen über 96 % des Jahresumsatzes von *Facebook* auf Werbeeinahmen zurück.[174] Die Verarbeitung personenbezogener Daten ist dahingehend gerade das Geschäftsmodell des Netzwerks. Dem *EuGH* ist damit zuzustimmen, dass entsprechende Werbetätigkeiten den Internetdienst erst wirtschaftlich rentabel

170 Vgl. Kap. 2 Pkt. B, S. 51.

171 *Nägele/Jacobs*, ZUM 2010, 281, 289 f.; *Klar,* Datenschutzrecht und die Visualisierung des öffentlichen Raums, S. 179.

172 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 50, 52 – Google Spain und Google; *Kühling*, EuZW 2014, 527, 528.

173 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 55 f. – Google Spain und Google.

174 *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 62; vgl. Kap. 1 Pkt. C.I, S. 38.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

machen und damit das Mittel sind, das die Durchführung des Dienstes ermöglicht.[175]

Der Anwendungsbereich des Art. 4 Abs. 1 lit. a DSRL ist weit umfangreicher, als er teilweise interpretiert wird. Eine Interpretation des Merkmals „im Rahmen der Tätigkeiten einer Niederlassung" dahingehend, dass es auf den Ort der Datenverarbeitung ankommt, die Verarbeitung also „von" der Niederlassung ausgeführt werden müsse, würde den Anwendungsbereich des Art. 4 Abs. 1 lit. a DSRL hingegen über seinen Wortlaut hinaus einschränken.

2. Territorial anwendbares Recht innerhalb der EU bei mehreren Niederlassungen

a) Abgrenzung mitgliedstaatlicher Datenschutzregimes als Folgefrage

Mit oben erzieltem Ergebnis[176] stellt sich jedoch die Folgefrage nach dem territorial anwendbaren Recht bei Sachverhalten, in denen in mehreren Mitgliedstaaten eine Niederlassung desselben Konzerns besteht. Denn es ist durchaus denkbar, dass ein Unternehmen nach den dargelegten Maßstäben mehrere Niederlassungen auf dem Gebiet der EU unterhält. Dies zeigt das Beispiel von *Facebook*, das in Deutschland mit der *Facebook Germany GmbH* vertreten ist. Nach den Merkmalen des *EuGH* stellt die *Facebook Germany GmbH* unzweifelhaft eine Niederlassung i. S. d. EG 19 der DSRL dar: Als im Handelsregister eingetragene Gesellschaft[177] ist sie zweifellos eine feste Einrichtung. Da auch geringfügige Tätigkeiten für eine effektive und tatsächliche Tätigkeit i. S. d. EG 19 S. 1 DSRL ausreichen,[178] wird diese Tätigkeit auch bei der *Facebook Germany GmbH* zu bejahen sein. Auch die *Facebook Germany GmbH* ist nach eigenen Angaben im Bereich der Anzeigenakquise und des Marketings tätig, die Verarbeitung personenbezogener Daten erfolgt also „im Rahmen [ihrer] […] Tätigkeiten". Damit sind ebenso wie bei *Google Spain* die Werbeakquise und das Marketing der *Facebook Germany GmbH* untrennbar verbunden mit den Tätigkeiten des

175 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 55 f. – Google Spain und Google.
176 Vgl. Kap. 2 Pkt. B.II.1.c, S. 62.
177 Eintragung ins Handelsregister B des AG Hamburg, Abteilung B, Wiedergabe des aktuellen Registerinhalts, abrufbar unter https://www.unternehmensregister.de/ureg/ (abgerufen am 13.10.2017).
178 Vgl. Kap. 2 Pkt. B.II.1.b, S. 61.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

sozialen Netzwerks selbst. Allerdings unterhält *Facebook* neben der *Facebook Germany GmbH* ähnliche Dependancen beispielsweise auch in Amsterdam oder Warschau.[179]

b) Übertragbarkeit der Auslegung des Art. 4 Abs. 1 lit. a DSRL auf rein innereuropäische Sachverhalte

Die Bestimmung der Anwendbarkeit der DSRL klärt freilich noch nicht die Frage, welches mitgliedstaatliche Datenschutzrecht zur Anwendung kommt. Teilweise wird vertreten, dass die Auslegung von Art. 4 Abs. 1 lit. a DSRL des *EuGH* im Fall *Google Spain und Google* nicht auf Sachverhalte übertragbar seien, die lediglich die Abgrenzung innereuropäischer Datenschutzrechte beträfen.[180] Im Fall *Google Spain und Google* hatte der *EuGH* das Merkmal „im Rahmen der Tätigkeiten" aus Art. 4 Abs. 1 lit. a DSRL präzise diskutiert und klargestellt, dass es gerade nicht auf eine Verarbeitung „von" der Niederlassung ankäme, sondern lediglich auf einer Verarbeitung „im Rahmen der Tätigkeiten einer Niederlassung".[181] Wo es jedoch lediglich um die Abgrenzung der harmonisierten Datenschutzrechte der Mitgliedstaaten gehe, sei eine derart weite Auslegung nicht anwendbar.[182] In der Konsequenz führt diese Ansicht also dazu, dass dasselbe Merkmal je nach Sachverhalt unterschiedlich ausgelegt werden soll.

---

179 *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017).

180 *Pauly/Ritzer/Geppert*, ZD 2013, 423, 425 f.; *VG Hamburg,* Beschl. v. 09.03.2016, Az. 15 E 4482/15, ZD 2016, 243, 245 f.; *GA Saugmandsgaard Øe,* Schlussanträge v. 02.06.2016, Rs. C-191/15, ECLI:EU:C:2016:388, Rn. 124 – Verein für Konsumenteninformation.

181 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 50, 52 – Google Spain und Google; *Kühling*, EuZW 2014, 527, 528; vgl. Kap. 2 Pkt. B.II.1.c, S. 62.

182 *Pauly/Ritzer/Geppert*, ZD 2013, 423, 425 f.; *GA Saugmandsgaard Øe,* Schlussanträge v. 02.06.2016, Rs. C-191/15, ECLI:EU:C:2016:388, Rn. 124 – Verein für Konsumenteninformation; *VG Hamburg,* Beschl. v. 09.03.2016, Az. 15 E 4482/15, ZD 2016, 243, 246; *v. Lewinski/Herrmann*, ZD 2016, 467, 470.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aa) Keine Beschränkung auf Drittlandsachverhalte durch den Wortlaut des Art. 4 Abs. 1 lit. a DSRL

Allerdings gibt der Wortlaut der DSRL keine Hinweise darauf, dass ihre Merkmale je nach Sachverhalt nach unterschiedlichen Maßstäben ausgelegt werden sollten. Insbesondere lässt sich Art. 4 Abs. 1 lit. a S. 2 und EG 19 S. 3 DSRL entnehmen, dass die DSRL davon ausgeht, dass ein für die Verarbeitung Verantwortlicher mit mehreren Niederlassungen im Unionsgebiet auch verschiedenen nationalen Datenschutzrechten unterworfen sein kann. Dies spricht gegen eine unterschiedliche Auslegung je nach Sachverhalt, da die DSRL gerade auch den Fall mehrerer anwendbarer nationaler Datenschutzrechte für denselben für die Verarbeitung Verantwortlichen im Blick hat.[183]

bb) Keine Beschränkung auf Drittlandsachverhalte durch die *EuGH*-Rechtsprechung

i) Keine Beschränkung durch *Google Spain* und *Weltimmo*

Überdies ist entgegen einer im Aufstreben befindlichen Ansicht auch der Rechtsprechung des *EuGH* nicht zu entnehmen, dass die weite Auslegung des Merkmals „im Rahmen der Tätigkeiten" nur für Sachverhalte mit Drittstaatenbezug Geltung beanspruchen soll. Allein mit der Tatsache, dass der *EuGH* die weite Auslegung auch mit dem Ziel der DSRL „bei der Verarbeitung personenbezogener Daten einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen […] zu gewährleisten" begründet hat und auf die Gefahr von Umgehungen der

183 Das *VG Hamburg* hingegen legt Art. 4 Abs. 1 lit. a S. 1 DSRL einschränkend dahin aus, dass die Niederlassungen inhaltlich identische Aufgaben wahrnehmen müssen, *VG Hamburg,* Beschl. v. 09.03.2016, Az. 15 E 4482/15, ZD 2016, 243, 246; richtigerweise verweist das *OVG Hamburg* jedoch darauf, dass sich hierfür im Wortlaut des Art. 4 Abs. 1 lit. a S. 2 DSRL keine Anhaltspunkte finden, *OVG Hamburg,* Beschl. v. 29.06.2016, Az. 5 Bs 40/16, CR 2016, 576. Die Norm erfordert nur das Vorliegen einer Niederlassung, nicht eine inhaltlich identische Tätigkeit aller Niederlassungen im Unionsgebiet. Kritisch zum Beschl. des *VG Hamburg Herbrich*, ZD 2016, 243, 249.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

DSRL hingewiesen hat[184], lässt sich dies jedenfalls nicht darlegen.[185] Im Gegenteil: Der *EuGH* gab bisher keine ausdrücklichen Hinweise darauf, dass das Merkmal bei innereuropäischen Sachverhalten anders ausgelegt werden soll. Vielmehr hat er diese weite Auslegung des Merkmals im Fall *Weltimmo*, bei dem lediglich die Abgrenzung von ungarischem zu slowakischem Datenschutzrecht in Frage stand, mit Verweis auf die *Google Spain und Google*-Entscheidung bestätigt.[186] Darüber hinaus hat der *EuGH* in beiden Fällen auf Art. 4 Abs. 1 lit. a DSRL abgestellt. Wäre es dem *Gerichtshof* lediglich darum gegangen, eine Anwendbarkeit der DSRL zu begründen, hätte dies auch über eine entsprechend enge Auslegung des Niederlassungsbegriffs und in Anwendung des Art. 4 Abs. 1 lit. c DSRL erreicht werden können, da Google mittels Cookies auf die Computer seiner Nutzer „zurückgreift".[187] Es ist demnach davon auszugehen, dass der *EuGH* bewusst eine weite Auslegung von Art. 4 Abs. 1 lit. a DSRL angelegt hat und dies auch nicht für bestimmte Sachverhalte einschränken wollte. Eine je nach Sachverhalt variierende Auslegung derselben Norm ist daher abzulehnen.

ii) Keine Beschränkung durch Verein für Konsumenteninformation

Diese Argumentation bestätigt auch die Entscheidung *Verein für Konsumenteninformation* des *EuGH*.[188] In dem Fall ging es um einen innereuropäischen Sachverhalt und das anwendbare Datenschutzrecht, wenn ein Unternehmen mit Sitz in der EU weder eine Niederlassung noch seinen Sitz in dem entsprechenden Mitgliedstaat hat, seine Geschäftstätigkeit jedoch auf

184 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 53 f. – Google Spain und Google.

185 So hingegen *GA Saugmandsgaard Øe,* Schlussanträge v. 02.06.2016, Rs. C-191/15, ECLI:EU:C:2016:388, Rn. 124 – Verein für Konsumenteninformation mit Fußnotenverweis auf *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 54 – Google Spain und Google; *VG Hamburg,* Beschl. v. 09.03.2016, Az. 15 E 4482/15, ZD 2016, 243, 246.

186 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 35 – Weltimmo.

187 Zur Auslegung von Art. 4 Abs. 1 lit. c DSRL vgl. Kap. 2 Pkt. B.III, S. 79.

188 *EuGH,* Urt. v. 28.07.2016, Rs. C-191/15, ECLI:EU:C:2016:612 – Verein für Konsumenteninformation.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

einen bestimmten Mitgliedstaat ausrichtet.[189] In durchgängiger Bezugnahme auf seine Rechtsprechung im Urteil *Weltimmo* fasst der *EuGH* die von ihm bereits aufgestellten Kriterien zur Auslegung des Art. 4 Abs. 1 lit. a DSRL nochmals zusammen: So stellt er erneut klar, dass auch nur geringfügige tatsächliche und effektive Tätigkeiten mittels einer festen Einrichtung ausreichten und daher zwar weder das Bestehen einer Zweigniederlassung noch einer Tochtergesellschaft Voraussetzung des Art. 4 Abs. 1 lit. a DSRL seien.[190] Allein die Zugriffsmöglichkeit auf eine Website von einem Mitgliedstaat genügten den Erfordernissen des Art. 4 Abs. 1 lit. a DSRL jedoch nicht.[191] Vielmehr seien sowohl der Grad der Beständigkeit als auch die effektive Ausübung der wirtschaftlichen Tätigkeiten im fraglichen Mitgliedstaat zu bewerten.[192] Schließlich weist der *EuGH* ausdrücklich und ganz auf einer Linie mit seinen Urteilen *Google Spain und Google* sowie *Weltimmo* darauf hin, dass die Verarbeitung personenbezogener Daten i. S. d. Art. 4 Abs. 1 lit. a DSRL nicht *von*, sondern *im Rahmen der Tätigkeiten* einer Niederlassung ausgeführt werden müsse.[193] Mit diesen Ausführungen verweist der *EuGH* die Entscheidung zurück an das vorlegende Gericht, das unter Berücksichtigung der genannten Rechtsprechung und aller relevanten Umstände die Frage des territorial anwendbaren Rechts beantworten soll.[194]

Teilweise wird vertreten, dass es besonders auffällig sei, dass der *EuGH* sich in *Verein für Konsumenteninformation* allein auf *Weltimmo* berufe und nicht auf seine Rechtsprechung in *Google Spain und Google*. Daraus sei zu schließen, dass der *EuGH* sich den Stimmen, die eine unterschiedliche Auslegung des Merkmals „im Rahmen der Tätigkeiten" je nach Sachverhalt – rein innereuropäisch oder mit Drittstaatenbezug – befürworten, anschließe.[195] Dies ist jedoch abzulehnen, da der *EuGH* diese Aussage gerade

189 *EuGH,* Urt. v. 28.07.2016, Rs. C-191/15, ECLI:EU:C:2016:612, Rn. 29, 72 – Verein für Konsumenteninformation.

190 *EuGH,* Urt. v. 28.07.2016, Rs. C-191/15, ECLI:EU:C:2016:612, Rn. 75 f. – Verein für Konsumenteninformation.

191 *EuGH,* Urt. v. 28.07.2016, Rs. C-191/15, ECLI:EU:C:2016:612, Rn. 76 – Verein für Konsumenteninformation.

192 *EuGH,* Urt. v. 28.07.2016, Rs. C-191/15, ECLI:EU:C:2016:612, Rn. 77 – Verein für Konsumenteninformation.

193 *EuGH,* Urt. v. 28.07.2016, Rs. C-191/15, ECLI:EU:C:2016:612, Rn. 78 – Verein für Konsumenteninformation.

194 *EuGH,* Urt. v. 28.07.2016, Rs. C-191/15, ECLI:EU:C:2016:612, Rn. 79 – Verein für Konsumenteninformation.

195 *Piltz,* Anwendbares Datenschutzrecht: Europäischer Gerichtshof schafft ein wenig mehr Klarheit, abrufbar unter

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

nicht trifft. Diese Feststellung erlangt umso mehr Gewicht, wenn man bedenkt, dass der *EuGH* auf die Ausführungen des GA *Saugmandsgaard Øe*, der gerade dieses Argument noch angeführt hatte,[196] nicht eingeht. Ferner zitiert der *EuGH* zwar insbesondere zum Merkmal „im Rahmen der Tätigkeiten" ausschließlich sein Urteil *Weltimmo*. Die zitierte Rn. 35 des Urteils verweist jedoch seinerseits auf die Rechtsprechung im Fall *Google Spain und Google*.[197] Ein Abstandnehmen von seiner Rechtsprechung im *Google Spain und Google*-Urteil ist daher nicht erkennbar.

cc) Zwischenergebnis

Die dargestellte Auslegung des Art. 4 Abs. 1 lit. a DSRL ist durchaus auf rein innerunionale Sachverhalte übertragbar. Auch die dargestellte Rechtsprechung des *EuGH* enthält keine Hinweise auf eine Einschränkung der Interpretation auf Sachverhalte mit Drittstaatenbezug.

c) Abgrenzung mitgliedstaatlicher Datenschutzregimes bei innereuropäischen Sachverhalten

Die dargestellte Auslegung des Art. 4 Abs. 1 lit. a DSRL steht in der Kritik, die Bestimmung des anwendbaren mitgliedstaatlichen Rechts zu erschweren. Dabei führen die Kritiker an, dass aufgrund der ausgeweiteten Auslegung des Niederlassungsbegriffs für denselben Verarbeitungsvorgang verschiedene nationale Datenschutzrechte anwendbar sein könnten.[198] Die Anwendung mehrerer nationaler Datenschutzrechte auf denselben Verarbeitungsvorgang widerspreche dem Sinn des Art. 4 DSRL als Kollisionsnorm

---

https://www.delegedata.de/2016/07/anwendbares-datenschutzrecht-europaeischer-gerichtshof-schafft-ein-wenig-mehr-klarheit/ (abgerufen am 13.10.2017).

196 *GA Saugmandsgaard Øe,* Schlussanträge v. 02.06.2016, Rs. C-191/15, ECLI:EU:C:2016:388, Rn. 124 – Verein für Konsumenteninformation.

197 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 35 – Weltimmo mit Verweis auf *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 52 – Google Spain und Google.

198 *Beyvers*, EuZW 2015, 912, 917; *Kartheuser/Schmitt*, ZD 2016, 155, 157 f.; so schon zu den Schlussanträgen von *GA Jääskinen Pauly/Ritzer/Geppert*, ZD 2013, 423, 426; dem *EuGH* zustimmend jedoch *Karg*, ZD 2015, 580, 584.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

zur Abgrenzung der nationalen Datenschutzrechte.[199] Im Folgenden werden die Auswirkungen der dargestellten Auslegung des Art. 4 Abs. 1 lit. a DSRL bei innereuropäischen Sachverhalten unter Auseinandersetzung mit der Kritik in Literatur und Rechtsprechung diskutiert. Im Zuge dessen werden auch Lösungsansätze zur Abgrenzung mitgliedstaatlicher Datenschutzregimes dargestellt und ihre Funktionalität bewertet. Dabei wird insbesondere zwischen der Unterwerfung desselben Datenverarbeiters unter mehrere nationale Datenschutzregimes und der Anwendbarkeit von Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben Verarbeitungsvorgang zu unterscheiden sein: Denn die DSRL sollte nur die Anwendung von Datenschutzregimen mehrerer Mitgliedstaaten auf denselben Verarbeitungs*vorgang*, nicht jedoch grundsätzlich auch die Unterwerfung desselben *Verantwortlichen* unter die Datenschutzregimes mehrerer Mitgliedstaaten verhindern.[200] Der folgende Abschnitt zeigt die Notwendigkeit dieser Trennung auf.

aa) Anwendbarkeit nationaler Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben Verantwortlichen

Während die DSRL laut Entwurfsbegründung die Anwendbarkeit nationaler Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben Verarbeitungsvorgang verhindern sollte,[201] gilt dasselbe nicht auch für die Anwendbarkeit nationaler Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben für die Verarbeitung Verantwortlichen. So sieht Art. 4 Abs. 1 lit. a S. 2, EG 19 S. 3 DSRL vor, dass ein für die Verarbeitung Verantwortlicher mit mehreren Niederlassungen im Unionsgebiet sicherstellen soll, dass jede seiner Niederlassungen die Bestimmungen des *jeweils anwendbaren* einzelstaatlichen Rechts einhält. Aus der Entwurfsbegründung lässt sich lediglich schließen, dass Art. 4 DSRL Rechtsunsicherheiten hinsichtlich des anwendbaren Rechts auf *denselben Verarbeitungsvorgang* vermeiden will – aus ihr lässt sich jedoch nicht ebenso schließen, dass die

199 *Pauly/Ritzer/Geppert*, ZD 2013, 423, 425; *GA Saugmandsgaard Øe,* Schlussanträge v. 02.06.2016, Rs. C-191/15, ECLI:EU:C:2016:388, Rn. 110 – Verein für Konsumenteninformation; *VG Hamburg,* Beschl. v. 09.03.2016, Az. 15 E 4482/15, ZD 2016, 243, 245.

200 COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 13; dazu ausführlich Kap. 2 Pkt. B.II.2.c.bb, S. 72.

201 COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 13; dazu ausführlich Kap. 2 Pkt. B.II.2.c.bb, S. 72.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Richtlinie vermeiden will, dass *derselbe für die Verarbeitung Verantwortliche* mehreren Datenschutzregimen unterworfen wird. Gerade diese Unterscheidung trifft die Kritik an der dargestellten Auslegung des Art. 4 Abs. 1 lit. a DSRL und damit an den Urteilen *Google Spain und Google* und *Weltimmo* jedoch nicht hinreichend: So sind Argumente, die kritisieren, dass die *EuGH*-Rechtsprechung dazu führe, „[…] dass […] [Unternehmen] potenziell mit der Anwendbarkeit mehrerer Datenschutzrechte rechnen müssen, was zu einem erhöhten Prüfungsaufwand führen kann […]“[202] zwar zutreffend – sie können sich aber nicht darauf stützen[203], dass dies dem Normzweck von Art. 4 DSRL zuwiderliefe. Soweit die Kritik dahingeht, dass „Datenverarbeiter […] sich nicht mehr darauf verlassen [können], nur das Datenschutzrecht des Mitgliedstaats ihrer Hauptniederlassung in der Union anwenden zu können […]“[204] kann dem entgegengehalten werden, dass die DSRL nie vorsah, dass Datenverarbeiter sich nur dem Datenschutzrecht ihrer *Hauptniederlassung* unterwerfen mussten. Vielmehr sieht die DSRL gerade vor, dass Datenverarbeiter mit der Anwendbarkeit mehrerer mitgliedstaatlicher Datenschutzrechte rechnen müssen.

Diese Kritik an der vorliegend vertretenen Auslegung des Art. 4 Abs. 1 lit. a DSRL bemängelt also vorwiegend, dass Datenverarbeiter nun mit erschwerten Bedingungen zu kämpfen hätten, indem sie dem Regime mehrerer Datenschutzrechte unterworfen würden. Das überrascht, da im selben Zuge angeführt wird, dass eine höchstrichterliche Ausweitung des Niederlassungsbegriffs zum Schutze der personenbezogenen Daten mit Blick auf die Harmonisierung des Datenschutzrechts durch die DSRL nicht nötig sei.[205] Im Umkehrschluss dürften Unternehmen von der Unterwerfung unter die Datenschutzregimes mehrerer Mitgliedstaaten dann aber nicht allzu hart getroffen werden. Zwar gehen mit der Pflicht zur Beachtung mehrerer nationaler Datenschutzregimes erhöhte Kosten einher. Fortgedacht führt diese Kritik aber dazu, dass der Mehraufwand und die erhöhten Kosten von den für die Verarbeitung Verantwortlichen auf die Betroffenen umgelegt würden. So wird etwa argumentiert, dass es zwar „[…] unter Umständen die Rechtsdurchsetzung für einzelne Betroffene [erleichtere], wenn auf die sie

202 *Kartheuser/Schmitt*, ZD 2016, 155, 159.
203 So führen etwa *Kartheuser/Schmitt* die Kritik gerade im Rahmen der historischen Auslegung von Art. 4 DSRL mit Verweis auf die Begründung zu Art. 4 DSRL aus, ZD 2016, 155, 158 f.
204 *Beyvers*, EuZW 2015, 912, 917.
205 *Beyvers*, EuZW 2015, 912, 917; *Kartheuser/Schmitt*, ZD 2016, 155, 158.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

betreffenden Datenverarbeitungen das Datenschutzrecht ihres Mitgliedstaats anwendbar ist.“[206] Es sei jedoch zweifelhaft, ob diese Begründung ein starkes Abweichen vom dem in Art. 4 der Richtlinie angelegten Grundgedanken des Niederlassungsprinzips rechtfertige.[207] Der finanzielle wie logistische Mehraufwand der Rechtsdurchsetzung in einem anderen Land wird für die Betroffenen jedoch regelmäßig eine sehr hohe Hürde darstellen, die dazu führen kann, dass die Schutzwirkung von Datenschutzgesetzen leerläuft. Zudem befinden sich die Datenverarbeiter oftmals in einer stärkeren Ausgangsposition als die Betroffenen. Letztlich ist es zumindest den Datenverarbeitern, die personenbezogene Daten ihrer Nutzer monetisieren, zuzumuten, die Verpflichtungen, die im jeweiligen einzelstaatlichen Recht vorgesehen sind, einzuhalten. Dies entspricht dem in Art. 4 Abs. 1 lit. a S. 2, EG 19 S. 3 DSRL angelegten System.

Es ist also festzuhalten, dass die Bestimmungen der DSRL einer Anwendbarkeit mehrerer nationaler Datenschutzbestimmungen auf denselben Datenverarbeiter nicht entgegenstehen.

bb) Anwendbarkeit nationaler Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben Verarbeitungsvorgang

Weiterhin stellt sich die Frage, ob Art. 4 Abs. 1 lit. a DSRL der Anwendbarkeit nationaler Datenschutzbestimmungen mehrerer Mitgliedstaaten auf denselben Verarbeitungsvorgang entgegensteht. In den Begründungen für die Vorschläge einer Datenschutzrichtlinie aus den Jahren 1990 und 1992 wird zu Art. 4 der Vorschläge ausgeführt, dass damit die Anwendbarkeit mehrerer nationaler Datenschutzrechte auf denselben Verarbeitungsvorgang verhindert werden soll.[208] Dabei ist zunächst zu klären, was als *derselbe* Verarbeitungsvorgang gilt.

206 *Beyvers*, EuZW 2015, 912, 917.
207 *Beyvers*, EuZW 2015, 912, 917.
208 COM(90) 314 final – SYN 287, Abl.EG 1990 C 277, 3, S. 21 f.; COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 13.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

i) Definition „desselben“ Verarbeitungsvorgangs

Bei der Definition dessen, was als „derselbe“ Verarbeitungsvorgang gilt, ist sowohl eine streng technische Betrachtung, nach der jeder technische Verarbeitungsvorgang für sich betrachtet wird, denkbar, als auch eine einheitliche Betrachtungsweise, bei der sämtliche technischen Verarbeitungsvorgänge, die mit derselben Tätigkeit in Verbindung stehen, als *derselbe* Verarbeitungsvorgang zählen.

Beispielhaft aufgeführt sei nur die Kommunikation des Nutzer-PCs mit einer besuchten Website. Schon beim Aufrufen einer Website findet bei strikt technischer Betrachtung eine Vielzahl technischer Verarbeitungsvorgänge statt. Auch bei dem Platzieren eines HTTP-Cookies finden zahlreiche Verarbeitungsvorgänge statt, die etwa in der Kommunikation des Browsers mit dem Nutzer-PC liegen, aber auch in dem tatsächlichen Platzieren des HTTP-Cookies auf dem Nutzer-PC sowie in dem erneuten Ablegen von Informationen in der Datei bei jedem Website-Besuch.[209] Man könnte diese Vorgänge entweder als Einheit betrachten, oder auf jeden einzelnen technischen Verarbeitungsschritt abstellen.

Juristisch trennschärfer erscheint auf den ersten Blick eine streng nach technischen Gesichtspunkten getrennte Betrachtungsweise: In der Begründung zu Art. 4 im Richtlinienvorschlag von 1992 wird zwar nicht näher erläutert, wie ein Verarbeitungsvorgang zu definieren ist, dies ergibt sich jedoch aus der DSRL selbst: Art. 2 lit. b DSRL, der den Verarbeitungsbegriff definiert, verdeutlicht, dass die Richtlinie zwischen den einzelnen Vorgängen unterscheidet und eine technische Betrachtungsweise annimmt, indem sie das Erheben, das Speichern, die Organisation, und andere Verarbeitungsvorgänge aufzählt und somit voneinander unterscheidet. Zudem wird der Vorschlag zu Art. 2 lit. b in dem Dokument von 1990[210] damit begründet, dass in der Definition des Verarbeitungsbegriffs die wesentlichen Verarbeitungsvorgänge gelistet werden, um eine weitere Anwendbarkeit der Richtlinie zu erzielen.[211] Auch der Richtlinienvorschlag von 1992 verwendet in der Begründung zu Art. 4 den Begriff „processing operation“, der zu unterscheiden ist vom Oberbegriff „processing“[212]. Dieses Zusammenspiel aus den Vorschlagsbegründungen von 1990, 1992 und der endgültigen

209 Vgl. Kap. 1 Pkt. C.II.1, S. 41.
210 Die Verarbeitungsdefinition ist dort noch in Art. 2 lit. d zu finden, COM(90) 314 final – SYN 287, Abl.EG 1990 C 277, 3, S. 20.
211 COM(90) 314 final – SYN 287, Abl.EG 1990 C 277, 3, S. 20.
212 COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 13.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

DSRL lässt darauf schließen, dass in der Begründung zu Art. 4 des Richtlinienvorschlags von 1992 keine einheitliche Betrachtungsweise, sondern eine technische Betrachtungsweise intendiert war. Im Übrigen entspricht diese Betrachtungsweise auch der üblichen datenschutzrechtlichen Betrachtungsweise, bei der stets jeder Verarbeitungsvorgang für sich genommen dem Verbot mit Erlaubnisvorbehalt unterliegt und damit einer Rechtfertigung bedarf.[213]

Dennoch ist die nach Verarbeitungsvorgängen getrennte Betrachtungsweise nicht hinreichend praktikabel. Die einzelnen internen Datenverarbeitungsvorgänge sind schwer nachvollziehbar und stellen sich überdies für den Nutzer als Einheit dar. Daher ist eine einheitliche Betrachtungsweise zur Beurteilung des territorial anwendbaren Rechts sinnvoll.

ii) Abgrenzung anhand des Merkmals der „engsten Verknüpfung"

Da die DSRL die Anwendung mehrerer Datenschutzrechte auf denselben Verarbeitungsvorgang verhindern wollte, muss in einem nächsten Schritt geprüft werden, wie die Abgrenzung mitgliedstaatlicher Datenschutzregimes bei Sachverhalten, die Berührungspunkte zu verschiedenen Mitgliedstaaten aufweisen, erfolgen kann.

Von den Befürwortern der Ansicht, dass Art. 4 Abs. 1 lit. a DSRL bei innereuropäischen Sachverhalten eng auszulegen sei, wird teilweise vertreten, dass die Abgrenzung der mitgliedstaatlichen Datenschutzbestimmungen anhand des Kriteriums „im Rahmen der Tätigkeiten" danach erfolgen soll, welche Niederlassung die engste Verknüpfung zur Verarbeitung aufweist.[214] Unklar bleibt allerdings, wie die engste Verknüpfung bestimmt werden soll. So verweist das *VG Hamburg* darauf, dass die *Facebook Ireland Ltd.* eine engere Verknüpfung zur Verarbeitung aufweise als die *FB Germany GmbH*, da die *Facebook Ireland Ltd.* die offizielle Vertragspartnerin der Nutzer in Deutschland sei sowie aufgrund eines „Data Transfer and Processing Agreements",[215] das *Facebook Ireland Ltd.* die Verantwortlichkeit für bestimmte Kategorien von Datenverarbeitungen zuweist. Auch

213 Vgl. Art. 7 DSRL / § 4 Abs. 1 BDSG / Art. 6 Abs. 1 DSGVO.

214 *VG Hamburg,* Beschl. v. 09.03.2016, Az. 15 E 4482/15, ZD 2016, 243, 246; *GA Saugmandsgaard Øe,* Schlussanträge v. 02.06.2016, Rs. C-191/15, ECLI:EU:C:2016:388, Rn. 125 – Verein für Konsumenteninformation.

215 *VG Hamburg,* Beschl. v. 09.03.2016, Az. 15 E 4482/15, ZD 2016, 243, 248; vgl. aber auch *VG Hamburg,* Beschl. v. 24.04.2017, Az. 13 E 5912/16, abrufbar unter

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

GA Saugmandsgaard Øe nennt die Klausel in den AGB von *Amazon EU*, dass „Amazon.de" die entsprechende Datenverarbeitung vornehme, als Indiz für die Bestimmung der engsten Verknüpfung.[216] Allerdings ist gem. Art. 4 Abs. 1 DSRL nicht die rechtliche Zuweisung des Vertragspartners und der Verantwortlichkeit entscheidend, sondern die tatsächliche Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung.[217] Überdies bestünde bei konsequenter Anwendung dieser Ansicht die engste Verbindung zur Verarbeitung der personenbezogenen Daten *aller* Nutzer außerhalb der USA und Kanadas zu *Facebook Ireland Ltd.* als deren Vertragspartner.[218] Der Wortlaut des Art. 4 Abs. 1 lit. a DSRL, der wie dargestellt keine Verarbeitung „von" der Niederlassung fordert, spricht auch gegen eine „engste Verknüpfung" der *Facebook Ireland Ltd.* zur Datenverarbeitung von Nutzern innerhalb der europäischen Union alleine auf Grundlage dessen, dass dort *Facebooks* Datenzentren beheimatet sind.

Legt man der „engsten Verknüpfung" nicht rein rechtliche Zuweisungen, sondern die Argumentation des *EuGH* zugrunde, dass die Tätigkeit einer Suchmaschine „untrennbar […] verbunden"[219] mit der Werbeschaltung ist, da sie durch diese erst wirtschaftlich rentabel wird[220], kommt man zu dem Schluss, dass für deutsche Nutzer die *Facebook Germany GmbH* die engste Verknüpfung zur relevanten Datenverarbeitung aufweist. *Facebook* generiert über 96 % seines Umsatzes durch Werbeeinnahmen.[221] Die *Facebook Germany GmbH* ist indes für die Werbeakquise in Deutschland zuständig[222]

---

http://justiz.hamburg.de/contentblob/8628058/8d1290fe1e894141c634755236d8394d/data/13e5912-16.pdf (abgerufen am 13.10.2017), S. 23 f., das Zweifel an der „engsten Verbindung" der *Facebook Ireland Ltd.* äußert für Fälle, in denen ausschließlich deutsche Nutzer betroffen sind.

216 *GA Saugmandsgaard Øe*, Schlussanträge v. 02.06.2016, Rs. C-191/15, ECLI:EU:C:2016:388, Rn. 125 – Verein für Konsumenteninformation.

217 Vgl. Kap. 2 Pkt. B.I.3, S. 58.

218 Vgl. Punkt 18 der Allgemeinen Geschäftsbedingungen von *Facebook, Facebook Inc.,* Erklärung der Rechte und Pflichten, abrufbar unter https://www.facebook.com/legal/terms (abgerufen am 13.10.2017).

219 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 56 – Google Spain und Google.

220 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 56 – Google Spain und Google.

221 *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 62; vgl. hierzu Kap. 1 Pkt. C.I, S. 38.

222 Eintragung ins Handelsregister B des AG Hamburg, Abteilung B, Wiedergabe des aktuellen Registerinhalts, abrufbar unter

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

und ist damit zentrales Element für die Rentabilität des Unternehmens auf dem deutschen Markt. Die Interpretation dieses Abgrenzungskriteriums für sich ist jedoch nicht hinreichend geeignet, um die Anwendbarkeit des mitgliedstaatlichen Datenschutzregimes zutreffend zu analysieren. Denn *Facebook* unterhält in zahlreichen weiteren Mitgliedstaaten Dependancen.[223] Es müssen also zusätzliche Kriterien gefunden werden, um im Verhältnis zwischen Anbieter und Nutzer das anwendbare mitgliedstaatliche Datenschutzregime zu bestimmen.

iii) Die Ausrichtung auf den Mitgliedstaat als weiterer Anknüpfungspunkt

Die Idee der „engste[n] Verknüpfung" kann dann zu trennscharfen Ergebnissen kommen, wenn man zusätzlich zu dem dargestellten Kriterium der untrennbaren Verbindung der Verarbeitung mit dem Geschäftskonzept[224] die engste Verknüpfung zu der Niederlassung des Mitgliedstaates anerkennt, auf den das Angebot des Plattformbetreibers ausgerichtet ist. Denn nach dargelegter Auslegung des Niederlassungsbegriffs stellt EG 19 S. 1 DSRL weder an die effektive und tatsächliche Ausübung einer Tätigkeit noch an die feste Einrichtung allzu hohe Anforderungen. Damit kann das Bestehen einer Niederlassung unter anderem an die Sprache der Website, die Ausrichtung auf einen Mitgliedstaat und die Bestellung eines ständigen Vertreters geknüpft werden.[225]

Diese Auslegung ist im Wortlaut des Art. 4 Abs. 1 lit. a DSRL angelegt. Denn Art. 4 Abs. 1 lit. a DSRL fordert wie gezeigt gerade keine Verarbeitung „von" der Niederlassung, ebenso wenig wie die DSRL weitere Anforderungen an die Qualität der „effektive[n] und tatsächliche[n] Ausübung einer Tätigkeit" i. S. d. EG 19 DSRL stellt. Die Hinwendung zu diesem Konzept, dem Marktortprinzip[226], erweist sich in Verbindung mit den weiteren dargestellten Kriterien als praktikable Lösung zur Abgrenzung der mitgliedstaatlichen Datenschutzregimes.

---

https://www.unternehmensregister.de/ureg/ (abgerufen am 13.10.2017).

223 *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017).

224 Vgl. Kap. 2 Pkt. B.II.2.c.bb.ii, S. 74.

225 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 41 – Weltimmo.

226 So bereits *Kühling*, EuZW 2014, 527 zu *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google und Google Spain.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Denn damit muss zwar der Datenverarbeiter mehrere mitgliedstaatliche Datenschutzregimes beachten, es kommen damit jedoch nicht mehrere mitgliedstaatliche Datenschutzregimes auf denselben Datenverarbeitungsvorgang zur Anwendung. Die Unterwerfung desselben für die Verarbeitung Verantwortlichen unter mehrere Datenschutzregimes entspricht ausdrücklich dem System der DSRL.[227] Schon vor der Rechtsprechung des *EuGH* bestand also für die Datenverarbeiter bei Unterhaltung mehrerer Dependancen im Unionsgebiet das Risiko, mehrere mitgliedstaatliche Datenschutzrechtregimes befolgen zu müssen. Die Auslegung des Art. 4 Abs. 1 lit. a DSRL trifft große Datenverarbeiter mit Dependancen in mehreren Mitgliedstaaten demzufolge nicht allzu schwer.

iv) Konfligierende Datenschutzregimes

Dieser Lösung wohnt auch keine Belastung über Gebühr inne, sollten sich die mitgliedstaatlichen Datenschutzregimes trotz Harmonisierung durch die DSRL unterscheiden. Denn diese Lösung zielt zunächst darauf ab, dass der Betreiber im Verhältnis mit dem jeweiligen Nutzer die Vorgaben des entsprechenden Datenschutzregimes – eine Niederlassung im entsprechenden Mitgliedstaat und die Ausrichtung des Angebots vorausgesetzt – zu wahren hat. Probleme könnten jedoch dann auftreten, wenn zwei Nutzer unterschiedlicher Mitgliedstaaten miteinander agieren, d. h., wenn etwa ein Nutzer in Deutschland ein Foto von sich und einem Freund in Polen hochlädt. Für diese Verarbeitung ist zunächst der hochladende Nutzer verantwortlich.[228] Sollte *Facebook* dieses Foto für eigene Zwecke verwerten wollen, müsste es in diesem Fall das Recht des Mitgliedstaates mit den stärkeren Regeln befolgen. In diesem Sinne ist ein gewisser Übertragungseffekt des strengeren Datenschutzregimes auf das großzügigere nicht von der Hand zu weisen. In der Praxis wird diese Verwertung aber ohnehin über eine Einwilligung erreicht.[229]

Der entscheidende Unterschied dieser Lösung zu der engeren Auslegung des Art. 4 Abs. 1 lit. a DSRL ist jedoch, dass soziale Netzwerkbetreiber ihre

227 Vgl. Kap. 2 Pkt. B.II.2.c, S. 69.
228 Vgl. Kap. 3 Pkt. A.II, S. 97.
229 Vgl. etwa *Facebook Inc.,* Datenrichtlinie, abrufbar unter https://www.facebook.com/about/privacy (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Nutzer nicht trotz einer Niederlassung in und Ausrichtung auf einen bestimmten Mitgliedstaat auf ein ganz anderes Datenschutzregime verweisen können. Das jedoch entspricht gerade dem System der DSRL.

Nicht zuletzt ist es auch in anderen Rechtsgebieten üblich, dass die Tätigkeiten in verschiedenen Ländern auch die Pflicht zur Befolgung rechtlicher Bestimmungen all dieser Länder zur Folge haben.[230] So hatten etwa vor Umsetzung der damaligen Haustürrechterichtlinie[231] in Spanien Händler bei auf deutsche Kunden ausgerichteten Werbefahrten deutsches Widerrufsrecht zu befolgen.[232] Für Verbraucherverträge trifft Art. 6 Abs. 1 lit. b Rom I-VO[233] eine ähnliche Regelung.

d) Zwischenergebnis

Sofern es sich um rein innereuropäische Sachverhalte handelt, wird die Übertragbarkeit der dargestellten Auslegung des Art. 4 Abs. 1 lit. a DSRL durch den *EuGH* auf diese Sachverhalte teilweise in Frage gestellt, da die DSRL die Anwendbarkeit von Datenschutzregimen mehrerer Mitgliedstaaten auf denselben Verarbeitungsvorgang verhindern wollte. Diese Frage ist jedoch von der Unterwerfung desselben für die Verarbeitung Verantwortlichen unter die Anwendbarkeit mehrerer mitgliedstaatlicher Datenschutzregimes zu unterscheiden. Art. 4 Abs. 1 lit. a S. 2 DSRL zeigt, dass die DSRL für die Verarbeitung Verantwortliche nicht per se vor der Pflicht schützt, das Recht verschiedener Mitgliedstaaten einzuhalten.

Der *EuGH* hat mit seiner Rechtsprechung nicht etwa die Anwendbarkeit mehrerer Datenschutzrechte auf denselben für die Verarbeitung Verantwortlichen originär ermöglicht, sondern vielmehr ein vom Wortlaut nicht

---

230 So auch *Art. 29-Datenschutzgruppe*, Update of Opinion 8/2010 on applicable law in light of CJEU judgement in Google Spain. WP 179 update (16.12.2015), S. 6 f.

231 Richtlinie 85/577/EWG des Rates vom 20. Dezember 1985 betreffend den Verbraucherschutz im Falle von außerhalb von Geschäftsräumen geschlossenen Verträgen, ABl.EG 1985 L 372, 31, aufgehoben m. W. v. 13.06.2014.

232 Sog. „Gran Canaria"-Fälle, vgl. *Hoffmann/Thorn/Firsching,* IPR, § 10 Pkt. E.I.4, Rn. 73; *BGH,* Urt. v. 19.09.1990, Az. VIII ZR 239/89, BGHZ 112, 204 - Empfehlen und Verwenden von Allgemeinen Geschäftsbedingungen; vgl. Art. 6 Abs. 1 lit. b Rom I-VO.

233 Verordnung (EG) Nr. 593/2008 des Europäischen Parlaments und des Rates vom 17. Juni 2008 über das auf vertragliche Schuldverhältnisse anzuwendende Recht (Rom I), ABl.EU 2008 L 177, 6.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

gedecktes sehr enges Verständnis des Anwendungsbereichs des Art. 4 Abs. 1 lit. a DSRL überzeugend widerlegt.

III. Rückgriff auf Mittel i. S. d. Art. 4 Abs. 1 lit. c DSRL

Ist der für die Verarbeitung Verantwortliche auch nach Zugrundelegung des weiten Auslegungsmaßstabes des *EuGH* nicht in dem entsprechenden Mitgliedstaat niedergelassen, ist das Recht des Mitgliedstaates nach Art. 4 Abs. 1 lit. c DSRL dann anwendbar, wenn der für die Verarbeitung Verantwortliche zum Zwecke der Verarbeitung auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, außer diese Mittel werden nur zum Zweck der Durchfuhr durch das Gebiet der EU verwendet.

1. Keine Niederlassung in der EU

Art. 4 Abs. 1 lit. c DSRL kommt nur dann zur Anwendung, wenn der für die Verarbeitung Verantwortliche keine Niederlassung im Mitgliedstaat besitzt, oder eine Niederlassung besitzt, die jedoch keine Relevanz für die Tätigkeit hat.[234] Dies ergibt sich im Umkehrschluss aus dem Wortlaut des Art. 4 Abs. 1 lit. a DSRL, nachdem die Verarbeitung personenbezogener Daten „im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden" muss. Das bedeutet, dass Art. 4 Abs. 1 lit. c DSRL selbst dann zur Anwendung gelangt, wenn der für die Verarbeitung Verantwortliche zwar eine Niederlassung im entsprechenden Mitgliedstaat hat, diese jedoch keine Berührungspunkte mit der Verarbeitung personenbezogener Daten aufweist.[235]

234 So auch *Art. 29-Datenschutzgruppe,* Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), S. 23 f.

235 *Art. 29-Datenschutzgruppe*, Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), S. 24 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

2. Rückgriff auf im Mitgliedstaat belegene Mittel

Für eine Anwendung von Art. 4 Abs. 1 lit. c DSRL muss ein Rückgriff auf im Hoheitsgebiet des entsprechenden Mitgliedstaats belegene Mittel vorliegen.

Fraglich ist zunächst, was „Mittel" i. S. d. Art. 4 Abs. 1 lit. c DSRL sind. Die Auslegung des Merkmals gestaltet sich aufgrund von sprachlichen Differenzen in den unterschiedlichen Entwürfen der (späteren) DSRL und der Übersetzungen der DSRL schwierig. So heißt es in der deutschen Fassung des Art. 4 Abs. 1 lit. c DSRL, dass der für die Verarbeitung Verantwortliche auf „Mittel" zurückgreifen muss, während in der englischen Sprachfassung von „equipment" die Rede ist. Gem. Art. 2 lit. d DSRL ist der für die Verarbeitung Verantwortliche derjenige, der über die „Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Das Merkmal „Mittel" in Art. 2 lit. d DSRL könnte also gleichbedeutend mit dem Merkmal „Mittel" aus Art. 4 Abs. 1 lit. c DSRL sein. Anders als in der deutschen Sprachfassung unterscheidet die englische Fassung jedoch zwischen Mittel i. S. d. Art. 2 lit. d DSRL – englisch „means" – und Mittel i. S. d. Art. 4 Abs. 1 lit. c DSRL – englisch „equipment".[236] Indes wurde der Begriff „equipment" erst später eingefügt: Im geänderten Kommissionsentwurf von 1992, der den ersten Entwurf zum jetzigen Art. 4 Abs. 1 lit. c DSRL beinhaltete, ist in Art. 4 Abs. 1 lit. b (Art. 4 Abs. 1 lit. c in der DSRL) noch von „means" die Rede.[237] Diese nachträgliche Änderung deutet daraufhin, dass das Wort „means" ganz gezielt nicht mehr verwendet wurde, also eine Unterscheidung zwischen dem Merkmal des „Mittels" bzw. „means" in Art. 2 lit. d DSRL und dem Merkmal des „Mittels" bzw. „equipment" in Art. 4 Abs. 1 lit. c DSRL beabsichtigt ist. [238] Das Wort „means" ist dabei weitergehend auszulegen als das Wort „equipment", das technisch belegt ist.[239]

---

236 So auch *Art. 29-Datenschutzgruppe*, Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), S. 25 f.

237 COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, S. 40 f., Art. 4 Abs. 1 lit. b.

238 A. A. *Art. 29-Datenschutzgruppe*, Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), S. 25 f., die für eine Gleichstellung der Begriffe „equipment" aus Art. 4 Abs. 1 lit. c DSRL und „means" aus Art. 2 Abs. 1 lit. d DSRL plädiert.

239 So wohl *Art. 29-Datenschutzgruppe*, Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), S. 25 f.; *Brühann*, in: Grabitz/Hilf/Nettesheim, DSRL, Art. 2, Rn. 19.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Übersetzt bedeutet „equipment" nämlich technisch „Ausrüstung", „Ausstattung", „Anlage".[240] Für den Begriff „means" wurden in der Begründung zur Änderung des Art. 4 in dem geänderten Kommissionsentwurf von 1992 beispielhaft Fragebögen und Terminals – also mit einem Großrechner verbundene Endgeräte zur Eingabe von Daten – angeführt. Damit nennt die Entwurfsbegründung je ein Beispiel für nicht-automatisierte und für automatisierte Mittel. Nutzer-PCs[241] lassen sich auch unter den engeren Begriff des „equipment" subsumieren, da Nutzer-Computer eine (technische) „Anlage" im Sinne der Wortbedeutung „equipment" darstellen. Auf die unterschiedliche Bedeutung der beiden Worte kommt es im Rahmen der Fragestellung dieser Arbeit daher nicht an.

Der für die Verarbeitung Verantwortliche müsste auch auf diese Mittel zurückgreifen. In der englischen Version von Art. 4 Abs. 1 lit. c DSRL heißt es hierzu: „[…] the controller […] makes use of equipment […] situated on the territory of the said Member State […]". In der englischen Version ist also nicht von einem Rückgriff, sondern von „Gebrauch machen" die Rede. Die Art. 29-Datenschutzgruppe stellte hierzu klar, dass „make use" sowohl ein Tätigkeitwerden des für die Verarbeitung Verantwortlichen als auch die klare Absicht des für die Verarbeitung Verantwortlichen zur Verarbeitung der personenbezogenen Daten voraussetzt.[242] Sie kommt daher richtigerweise zu dem Schluss, dass es für die Anwendbarkeit von Art. 4 Abs. 1 lit. c DSRL weder auf die Eigentumsverhältnisse ankommt, noch darauf, dass der für die Verarbeitung Verantwortliche die volle Kontrolle über die im Mitgliedstaat belegenen Mittel hat.[243] Das Mittel müsse hinsichtlich

240 *Willmann/Messinger/Langenscheidt-Redaktion,* Langenscheidts Großwörterbuch der englischen und deutschen Sprache, Eintrag „equipment".

241 Vgl. etwa Beispiele der *Art. 29-Datenschutzgruppe*, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU. WP 56 (30.05.2002), S. 10 ff.

242 *Art. 29-Datenschutzgruppe*, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU. WP 56 (30.05.2002), S. 9; *Art. 29-Datenschutzgruppe*, Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), S. 25; in der deutschen Version wird „make use" ohne Bezug auf den deutschen Wortlaut des Art. 4 Abs. 1 lit. c DSRL als „verwenden" übersetzt.

243 *Art. 29-Datenschutzgruppe*, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU. WP 56 (30.05.2002), S. 9; *Art. 29-Datenschutzgruppe*, Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), S. 25.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

der Verarbeitung von personenbezogenen Daten zu seiner Disposition stehen.[244] Dies wäre etwa der Fall, wenn eine Website mit dem Browser des Nutzers kommuniziert und dabei beispielsweise einen HTTP-Cookie auf der Festplatte des Nutzer-Computers hinterlegt[245].[246] Diese Auslegung ist zu begrüßen. Art. 4 Abs. 1 lit. c DSRL verfolgt gerade das Ziel, Datensubjekte davor zu schützen, dass für die Verarbeitung Verantwortliche sich dem Anwendungsbereich der DSRL entziehen könnten. In der starken technologischen Entwicklung seit Inkrafttreten der DSRL droht diese Gefahr heute umso stärker als vor über zwei Jahrzehnten. Auch der Hinweis in der Entwurfsbegründung auf Terminals lässt auf nichts Anderes schließen: Die Nutzer-PCs interagieren mit den Servern und sind damit zu den damaligen Terminals äquivalent.

Sollte ein für die Verarbeitung Verantwortlicher also keine Niederlassung in der EU haben, ist der Anwendungsbereich der DSRL dennoch eröffnet, sobald der für die Verarbeitung Verantwortliche auf Nutzer-PCs zugreift.[247] Dies geschieht im Internet durch verschiedene technische Hilfsmittel, wie etwa HTTP-Cookies und ähnliche Mechanismen, bei jedem Website-Aufruf. Aufgrund der durch die Rechtsprechung des *EuGH* stark ausgeweiteten Definition des Niederlassungsbegriffs ist der Anwendungsbereich des Art. 4 Abs. 1 lit. c DSRL jedoch geschrumpft: So haben Anbieter der großen sozialen Netzwerke meist eine oder mehrere Dependancen auf dem Gebiet der EU,[248] die der Dependance aus dem Fall *Google Spain*

---

244 *Art. 29-Datenschutzgruppe*, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU. WP 56 (30.05.2002), S. 9.

245 Vgl. Kap. 1 Pkt. C.II.1, S. 41.

246 Vgl. Beispiele der *Art. 29-Datenschutzgruppe*, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU. WP 56 (30.05.2002), S. 10 ff.; *Dammann*, in: Simitis, BDSG, § 1, Rn. 227; *Weichert*, in: DKWW, BDSG, § 1, Rn. 17a; *Gabel*, in: Taeger/Gabel, BDSG, § 1, Rn. 59; *Gusy*, in: BeckOK DatenschutzR, Rn. 104.

247 Nicht ausreichend wäre demgegenüber allein der Aufruf einer Website durch den Nutzer ohne einen Rückgriff auf den Nutzer-PC durch den Verantwortlichen, *Klar*, ZD 2013, 109, 111 f. Durch die starke Verbreitung von Tracking Tools, insbesondere HTTP-Cookies, ist dieser Anwendungsfall als selten zu bewerten.

248 Vgl. beispielsweise *Facebook* und *Twitter*, jeweils mit Büros u. a. in Berlin, Hamburg Amsterdam, Mailand, *Facebook Inc.,* Company Info, abrufbar unter

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

und Google sehr ähnlich sind. Vor allem für Drittparteien, sofern sie für die Verarbeitung Verantwortliche sind, könnte die Norm jedoch weiterhin von Bedeutung sein. Dies wäre etwa der Fall, wenn Werbedienstleister mittels HTTP-Cookies oder ähnlicher Technologien auf den Nutzer-PC „zurückgreifen".

C. Änderungen durch die DSGVO

Die DSGVO, die gem. Art. 99 Abs. 2 DSGVO zwei Jahre nach Inkrafttreten, also ab dem 25. Mai 2018, gelten wird, regelt das territorial anwendbare Recht in Art. 3 DSGVO.

I. Verarbeitung personenbezogener Daten nach Vorgabe der DSGVO

Wie bereits Art. 4 Abs. 1 DSRL, trennt auch Art. 3 DSGVO zwischen Unternehmen mit Niederlassung im Unionsgebiet (Art. 3 Abs. 1 DSGVO, bislang Art. 4 Abs. 1 lit. a DSRL) und solchen ohne Niederlassung im Unionsgebiet (Art. 3 Abs. 2 DSGVO, bislang Art. 4 Abs. 1 lit. c DSRL). Art. 3 Abs. 1 DSGVO bestimmt, dass die DSGVO auf Verarbeitungen anwendbar ist, die im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet. Damit entspricht Art. 3 Abs. 1 DSGVO dem noch geltenden Art. 4 Abs. 1 lit. a DSRL. Der Passus, dass die Anwendbarkeit unabhängig von dem Ort der Verarbeitung gelten soll, war im Entwurf der Kommission nicht vorgesehen und wurde vom Europäischen Parlament eingefügt.[249] Spätestens durch die Auslegung des Niederlassungsbegriffs durch den *EuGH* und die Klarstellung, dass die Ver-

---

http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017); *Twitter Inc.,* Twitter Nutzung / Fakten zum Unternehmen, abrufbar unter https://about.twitter.com/company (abgerufen am 13.10.2017).

249 Vgl. Art. 3 Abs. 1 DSGVO des DSGVO-Entwurfes der Kommission, KOM(2012) 11 endgültig; vgl. Art. 3 Abs. 1 des Parlamentsentwurfs der DSGVO, Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), P7_TA(2014)0212.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

arbeitung nicht „von" der Niederlassung vorgenommen werden muss, enthält dieser Passus jedoch keine Neuerung im Vergleich zum Recht der DSRL.[250]

Für nicht in der Union niedergelassene Unternehmen oder Auftragsdatenverarbeiter findet die DSGVO gem. Art. 3 Abs. 2 DSGVO Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten (lit. a) oder das Verhalten betroffener Personen zu beobachten (lit. b). In Art. 3 Abs. 2 lit. a DSGVO wird damit das Marktortprinzip eingeführt.[251]

Auch bei Art. 3 Abs. 1 DSGVO ist also, wie bereits bei Art. 4 Abs. 1 DSRL, zentraler Anknüpfungspunkt die Niederlassung eines Unternehmens. Nur wenn das Unternehmen keine Niederlassung im Unionsgebiet unterhält, kommt Art. 3 Abs. 2 DSGVO zur Anwendung. Die Rechtsprechung des *EuGH* zum Niederlassungsbegriff ist damit auch ab dem 25. Mai 2018 weiterhin von Bedeutung, insbesondere, weil die Definition einer Niederlassung aus EG 22 S. 2 DSGVO dem EG 19 S. 1 DSRL entspricht. Der räumliche Anwendungsbereich der Verordnung wird zudem durch Art. 3 Abs. 2 DSGVO sehr weit gefasst. Art. 3 Abs. 2 DSGVO ersetzt den komplizierten Art. 4 Abs. 1 lit. c DSRL und erledigt damit die Diskussion darüber, wann ein „Rückgriff auf Mittel" i. S. d. Norm vorliegt. Wichtig wird Art. 3 Abs. 2 DSGVO also dann, wenn ein Unternehmen keine Niederlassung im Unionsgebiet hat, im Unionsgebiet befindlichen Personen jedoch Waren oder Dienstleistungen anbietet oder deren Verhalten beobachtet. Für Anbieter sozialer Netzwerke ist Art. 3 Abs. 2 lit. a DSGVO die einschlägige Norm, sofern sie keine Niederlassung im Unionsgebiet unterhalten. Art. 3 Abs. 2 lit. a DSGVO stellt klar, dass die Norm auch einschlägig ist, wenn von den betroffenen Personen keine monetäre Gegenleistung für die Ware oder Dienstleistung erbracht wird.[252] Für Drittparteien, die den Nutzern keine Waren oder Dienstleistungen anbieten, ist Art. 3 Abs. 2 lit. b DSGVO einschlägig. Dies gilt etwa für Dritte, die mittels Tracking Tools wie HTTP-Cookies das Surfverhalten der Nutzer beobachten.[253] Unternehmen mit Sitz

250 Vgl. Kap. 2 Pkt. B.II.1.c, S. 62.
251 Vgl. auch *Kühling/Martini*, EuZW 2016, 448, 450.
252 Vgl. auch *Kühling/Martini*, EuZW 2016, 448, 450.
253 Vgl. Kap. 3 Pkt. C, S. 199; kritisch zur Reichweite der Regelung des Art. 3 Abs. 2 lit. b DSGVO *Klar*, DuD 2017, 533, 536.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

in Drittländern werden sich dem Anwendungsbereich der DSGVO somit nur schwerlich entziehen können.

II. Keine spezifische Kollisionsnorm bei der Aktivierung von Öffnungsklauseln

Fraglich ist jedoch, auf welche Kollisionsnorm unter dem Regime der DSGVO zurückzugreifen ist, wenn die territoriale Anwendbarkeit nationaler Datenschutzbestimmungen in Frage steht. Die DSGVO trifft keine Aussage über die territoriale Anwendbarkeit nationaler datenschutzrechtlicher Regelungen. Entscheidend wäre eine solche Regelung dort, wo die unmittelbare Wirkung der DSGVO durch Öffnungsklauseln durchbrochen wird. Auch wenn dies auf den ersten Blick vor allem für die Verarbeitung durch öffentliche Stellen der Fall ist – vgl. etwa Art. 6 Abs. 1 lit. e i. V. m. Abs. 2, 3 DSGVO – bietet die DSGVO den Mitgliedstaaten auch hinsichtlich der Verarbeitung durch nicht-öffentliche Stellen Möglichkeiten, nationale Regelungen zu erlassen: So bietet Art. 6 Abs. 4 DSGVO i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 DSGVO etwa eine Öffnungsklausel, mittels derer die Mitgliedstaaten nationale Regelungen „für andere Zwecke" zum Schutz der Freiheiten anderer Personen erlassen können.[254]

Die Abgrenzung der nationalen Datenschutzbestimmungen bei Aktivierung der Öffnungsklauseln kann nicht von Art. 3 DSGVO getroffen werden.[255] Fraglich ist also, auf welche Kollisionsnormen künftig bei diesen Fällen zurückzugreifen sein wird. Zunächst scheint es naheliegend, die Abgrenzung über die nationalen Kollisionsnormen vorzunehmen, die de lege lata noch Art. 4 Abs. 1 DSRL umsetzen.[256] Mit der Ablösung der DSRL durch die DSGVO sind die Mitgliedstaaten jedoch nicht mehr an die Vorgaben des Art. 4 DSRL gebunden. Zugleich sind sie allerdings auch nicht daran gebunden, ihre nationalen Datenschutzbestimmungen an Art. 3 DSGVO anzupassen, da dieser nur den Anwendungsbereich der Verordnung regelt. Auch lassen sich den Öffnungsklauseln nicht mit hinreichender Deutlichkeit selbst Kollisionsnormen entnehmen. Teilweise werden diese

254 Vgl. ausführlich *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 428 ff.

255 A. A. *Karg*, in: BeckOK DatenschutzR, DSGVO, Art. 8, Rn. 21 f., der die Abgrenzung der nationalen Regelungen im Rahmen der Öffnungsklausel des Art. 8 Abs. 1 DSGVO anhand des Art. 3 DSGVO vornimmt.

256 So wohl *Kartheuser/Schmitt*, ZD 2016, 155, 159.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

jedoch aus Formulierungen wie in Art. 6 Abs. 3 lit. b DSGVO herausgelesen, nach dem „[d]ie Rechtsgrundlage für Verarbeitungen gemäß [Art. 6] Absatz 1 Buchstaben c und e […] festgelegt [wird] durch […] das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt."[257] Allerdings kann man Art. 6 Abs. 3 S. 1 DSGVO hier keine Kollisionsregelung entnehmen. Die Norm regelt inhaltlich nicht das territorial anwendbare Rechtsregime, sondern stellt das Erfordernis einer im Unionsrecht (lit. a) oder im Recht des Mitgliedstaates (lit. b) verankerten Rechtsgrundlage für die Fälle des Art. 6 Abs. 1 lit. c und e DSGVO auf.[258] Der Zusatz „dem der Verantwortliche unterliegt" stellt vielmehr eine Präzisierung dar, hat inhaltlich als Kollisionsnorm jedoch keinen weiterführenden Aussagegehalt.[259] In der Konsequenz besteht im Fall der Aktivierung von Öffnungsklauseln kein spezifisches Kollisionsrecht.[260] Solange die Mitgliedstaaten sich nicht auf eine neue Kollisionsnorm für diese Fälle oder auf die verbindliche Beibehaltung der bislang jeweils bestehenden Umsetzung von Art. 4 Abs. 1 DSRL in nationales Recht einigen, ist stattdessen auf allgemeines Kollisionsrecht, etwa aus der Rom I-VO, zurückzugreifen. Da die Rechtsbeziehung zwischen sozialen Netzwerkbetreiber und Nutzer üblicherweise auf Vertragsbasis gegründet ist, wird oftmals die Rom I-VO einschlägig sein,[261] und damit insbesondere der für Verbraucherverträge anwendbare Art. 6 Rom I-VO. Nach Art. 6 Abs. 1 Rom I-VO ist das Recht des gewöhnlichen

257 Vgl. *Laue*, ZD 2016, 463, 464.

258 Vgl. detailliert zu den Öffnungsklauseln des Art. 6 Abs. 1 lit. c, e i. V. m. Abs. 2, 3 DSGVO *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 27 ff.

259 A. A. *Laue*, ZD 2016, 463, 464 f., der aus dieser Formulierung schließt, dass zur Bestimmung des territorial anwendbaren Rechts für Verantwortliche und Auftragsverarbeiter in der Union auf den Sitz der Hauptverwaltung eines Unternehmens abzustellen sei, während für Verantwortliche und Auftragsverarbeiter außerhalb der Union der – bei der Aktivierung der Öffnungsklausel nicht mehr sachlich anwendbare – Art. 3 DSGVO heranzuziehen sei.

260 So sah der Referentenentwurf des BMI v. 05.08.2016 in § 2 Abs. 4 vor, dass das Nachfolgegesetz zum BDSG nur Anwendung finden sollte, soweit eine Verarbeitung im Rahmen der Tätigkeiten einer inländischen Niederlassung stattfindet und blieb damit sowohl hinter § 1 Abs. 5 BDSG bzw. Art. 4 Abs. 1 DSRL als auch hinter Art. 3 DSGVO zurück, abrufbar unter https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/09/Entwurf-ABDSG-E-08.2016.pdf (abgerufen am 13.10.2017). Das BDSG-neu knüpft demgegenüber in § 1 Abs. 4 an die Verarbeitung personenbezogener Daten im Inland, eine inländische Niederlassung oder den Anwendungsbereich der DSGVO an (§ 1 Abs. 4 Nr. 3), vgl. Art. 1 § 1 Abs. 4 DSAnpUG-EU, BGBl. 2017 I, 2097.

261 Vgl. *Herbrich/Beyvers*, RDV 2016, 3, 6.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Aufenthalts des Verbrauchers anzuwenden, sofern der Unternehmer seine berufliche oder gewerbliche Tätigkeit in dem Staat ausübt (lit. a) oder das Recht des Staates oder der Staaten, auf den der Unternehmer seine Tätigkeit ausrichtet (lit. b). Damit korrespondiert Art. 6 Abs. 1 lit. b Rom I-VO mit Art. 3 Abs. 2 lit. a DSGVO.

Dies führt aber zu einer Reihe von Folgefragen. So ist schon unklar, ob eine Rechtswahl, die etwa Art. 6 Abs. 2 Rom I-VO ausdrücklich zulässt[262], in Ermangelung einer Eingriffsnorm i. S. d. Art. 9 Rom I-VO[263] dann möglich ist oder nicht.[264] Zudem kann die genaue Kollisionsnorm nur je nach Einzelfall bestimmt werden.[265] So ist schon nicht jede datenschutzrechtlich relevante Handlung zugleich Verbraucherrecht, wie die hochfrequente Nutzung von sozialen Netzwerken durch gewerbliche Nutzer, etwa mittels sog. Fanpages, verdeutlicht. Dies führt dazu, dass für verschiedene Situationen unterschiedliches Recht anwendbar sein kann. Eine Beurteilung des territorialen Rechts nach unterschiedlichen Maßstäben für Sachverhalte, in denen die DSGVO Öffnungsklauseln bereithält und die Mitgliedstaaten von diesen Gebrauch gemacht haben und für Sachverhalte, in denen die DSGVO zur Anwendung gelangt, ist für Nutzer zudem intransparent und reißt einen einheitlichen Nutzungsvorgang rechtlich auseinander. Es bleibt daher zu hoffen, dass diese Regelungslücke rasch mit spezifischem Kollisionsrecht geschlossen wird.

---

262 Vgl. aber zu den Einschränkungen bei Art. 6 Abs. 2 Rom I-VO *Piltz*, K&R 2012, 640, 642; *Solmecke/Dam*, MMR 2012, 71; für die Voraussetzungen vgl. *Kaufhold*, EuZW 2016, 247, 248 ff.

263 Die Einordnung des § 1 Abs. 5 BDSG als Eingriffsnorm i. S. d. Art. 9 Rom I-VO ist umstritten. Vgl. bejahend *Piltz*, K&R 2012, 640; *Dammann*, in: Simitis, BDSG, § 1, Rn. 197b; *Kremer*, RDV 2014, 73, 77 f; generell die Rom I-VO für das BDSG unbeachtlich erklärend *Gabel*, in: Taeger/Gabel, BDSG, § 1, Rn. 50; zweifelnd *Herbrich/Beyvers*, RDV 2016, 3, 7; ablehnend *Steinrötter*, MMR 2013, 691, 693 f.

264 Für die Zulässigkeit einer Rechtswahlregelung zwischen Privaten *LG Berlin,* Urt. v. 06.03.2010, Az. 16 O 551/10, ZD 2012, 276, 278; *KG Berlin,* 24.01.2014, Az. 5 U 42/12, ZD 2014, 412, 416; *Polenz*, VuR 2012, 207, 208 f.; a. A. *VG Schleswig,* Beschl. v. 14.02.2013, Az. 8 B 60/12, ZD 2013, 245, 245 f.; *Piltz*, K&R 2012, 640; *Piltz*, K&R 2013, 292, 296; *Kremer*, RDV 2014, 73, 78 f.; *Hornung/Müller-Terpitz,* Rechtshandbuch Social Media, S. 88.

265 Für einen Überblick vgl. etwa *Herbrich/Beyvers*, RDV 2016, 3.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

D. Territorial anwendbares Recht im Nutzer-Nutzer-Verhältnis

Fraglich ist zudem, welches Recht territorial im Nutzer-Nutzer-Verhältnis zur Anwendung kommen soll. Insofern ist zunächst festzustellen, dass dieser Fall nicht explizit in der DSRL und auch nicht im BDSG geregelt ist. Art. 4 Abs. 1 DSRL setzt das Vorliegen einer Niederlassung voraus und ist nicht auf natürliche Personen zugeschnitten. Allerdings könnte die Vorschrift analog anzuwenden sein, sofern ein vergleichbarer Sachverhalt und eine Regelungslücke vorliegen.[266] Die Sachverhalte sind hier durchaus vergleichbar, da es sich um die Bestimmung der territorialen Anwendbarkeit datenschutzrechtlicher Regelungen auf für die Verarbeitung Verantwortliche handelt. Auch sieht die DSRL keine andere, passende Regelung vor. Zudem bietet sonstiges Unionsrecht keine passende Kollisionsregelung. Insbesondere ein Rückgriff auf die Regelungen der Rom II-VO[267] scheidet in diesem Fall wegen Art. 1 Abs. 2 lit. g ROM II-VO aus, der Verletzungen der Privatsphäre und des Persönlichkeitsrechts ausdrücklich vom sachlichen Anwendungsbereich ausnimmt. Aus der Überprüfungsklausel des Art. 30 Abs. 2 ROM II-VO kann entnommen werden, dass dies auch Verstöße gegen Datenschutzbestimmungen einschließt.[268] Damit ist Art. 4 Abs. 1 lit. a DSRL analog auf natürliche Personen anwendbar. Statt auf die Niederlassung könnte bei natürlichen Personen etwa auf deren Wohnsitz[269] oder den gewöhnlichen Aufenthaltsort[270] abzustellen sein. Allerdings bedeutet dies im Umkehrschluss auch, dass die DSRL auf für die Verarbeitung Verantwortliche ohne Wohnsitz oder gewöhnlichen Aufenthaltsort in der EU bzw. dem EWR nicht anwendbar ist: ein Rückgriff auf im Mitgliedstaat

---

266 *EuGH,* Urt. v. 12.12.1985, Rs. 165/84, ECLI:EU:C:1985:507, Rn. 14 – Krohn; *EuGH,* Urt. v. 11.11.2010, Rs. C-152/09, ECLI:EU:C:2010:671, Rn. 41 – Groote.

267 Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates über das auf außervertragliche Schuldverhältnisse anzuwendende Recht ("Rom II"), ABl.EU 2007 L 199, 40.

268 *Weller/Nordmeier*, in: Spindler/Schuster, Recht der elektronischen Medien, ROM II-VO, Art. 1, Rn. 11.

269 Vgl. etwa Wohnsitz als Anknüpfungspunkt in der EuGVVO, Verordnung (EU) Nr. 1215/2012 des Europäischen Parlaments und des Rates vom 12. Dezember 2012 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (Neufassung), ABl.EU 2012 L 351, 1.

270 Vgl. etwa Begriff des gewöhnlichen Aufenthalts in Art. 5 ROM II-VO; zum Begriff des Aufenthaltsorts in der DSGVO vgl. Kap. 3 Pkt. D.II.4.c, S. 234.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

belegene Mittel durch den Verantwortlichen i. S. d. Art. 4 Abs. 1 lit. c DSRL liegt im Nutzer-Nutzer-Verhältnis nicht vor.[271]

Zum selben Ergebnis kommt man mithin bei Art. 3 DSGVO. Art. 3 Abs. 1 DSGVO ist dem Art. 4 Abs. 1 lit. a DSRL ähnlich konzipiert und damit nicht auf natürliche Personen ohne weiteres anwendbar. Auch hier ist jedoch eine analoge Anwendung denkbar, beispielsweise mit einer Anknüpfung an den Aufenthaltsort des Verantwortlichen in Anlehnung an diese Anknüpfung aus Art. 79 DSGVO[272]. Allerdings bedeutet dies, dass die DSGVO auf natürliche Personen, die personenbezogene Daten von Betroffenen in der Union verarbeiten, nicht anwendbar ist, sofern diese weder Waren noch Dienstleistungen anbieten noch das Verhalten der Betroffenen beobachten i. S. d. Art. 3 Abs. 2 DSGVO.

Verarbeitet also ein Verantwortlicher, der natürliche Person ist, personenbezogene Daten, so ist unter dem Regime der DSRL in entsprechender Anwendung des Art. 4 Abs. 1 lit. a DSRL das Recht des Mitgliedstaates seines Wohnsitzes oder gewöhnlichen Aufenthalts anwendbar, unter dem Regime der DSGVO die DSGVO selbst. Hat dieser Verantwortliche jedoch seinen Wohnsitz bzw. gewöhnlichen Aufenthaltsort nicht in der EU bzw. dem EWR, so sind weder DSRL noch DSGVO territorial anwendbar.

E. Fazit

Vor allem die jüngste Rechtsprechung des *EuGH* läutet einen Paradigmenwechsel in der Bestimmung des territorialen Rechts ein, von einer zuvor überwiegend restriktiven und nicht im Wortlaut angelegten Auslegung des Niederlassungsbegriffs in Art. 4 Abs. 1 DSRL zu einer nun zutreffend weiten Auslegung desselben. Während zuvor Einrichtungen mit ausschließlicher Marketingfunktion wie etwa die *Facebook Germany GmbH* meist nicht als Niederlassung anerkannt wurden, muss der Niederlassungsbegriff richtigerweise dergestalt ausgelegt werden, dass schon die von einer im Inland vorgenommenen Anzeigenakquise und Marktforschung als Anknüpfungspunkt für das deutsche Datenschutzrecht ausreichen können. Dies ist dann der Fall, wenn die Verarbeitung personenbezogener Daten von Nutzern in Deutschland „im Rahmen der Tätigkeiten" der *Facebook Germany GmbH* stattfindet. Zur Abgrenzung mitgliedstaatlicher Datenschutzregimes

271 Vgl. Kap. 2 Pkt. B.III, S. 79; vgl. aber auch Art. 40 EGBGB bei unerlaubten Handlungen, *Spickhoff*, in: BeckOK BGB, ROM II-VO, Art. 1, Rn. 18.

272 Vgl. Kap. 3 Pkt. D.II.4.c, S. 234.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

bei innereuropäischen Sachverhalten, in denen derselbe Konzern mehrere Niederlassungen unterhält, kann das Kriterium der „engsten Verknüpfung" einer Niederlassung zum Sachverhalt herangezogen werden. Dies führt jedoch nur dann zu einer hinreichend scharfen Abgrenzung der mitgliedstaatlichen Datenschutzregimes voneinander, wenn man als zusätzliches Kriterium für die „engste Verknüpfung" zu der Niederlassung desjenigen Mitgliedstaates die Ausrichtung auf einen bestimmten Mitgliedstaat heranzieht. Für die von Teilen der deutschsprachigen Literatur vertretene unterschiedliche Auslegung des Merkmals „im Rahmen der Tätigkeiten einer Niederlassung" in Art. 4 Abs. 1 lit. a DSRL je nach Sachverhalt finden sich demgegenüber keine rechtlichen Anhaltspunkte.

Mit der DSGVO steht ein Wechsel zum Marktortprinzip bevor. Die weite Auslegung des Niederlassungsbegriffs in der DSRL zeigt, dass dieses Marktortprinzip bereits dort angelegt war; sie schlägt zudem eine Brücke zu dem ab Mitte des Jahres 2018 geltenden Recht. Denn die Verarbeiter sind dem räumlichen Anwendungsbereich der DSGVO unterworfen, wenn sie eine Niederlassung im Unionsgebiet unterhalten oder im Unionsgebiet befindlichen Betroffenen Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten. Der räumliche Anwendungsbereich der DSGVO umfasst damit alle typischen Geschäftsmodelle von sozialen Netzwerken.

Allerdings greift das Marktortprinzip auch mit Geltung der DSGVO nicht absolut und die Frage nach dem territorial anwendbaren Recht wird somit auch mit Geltung der DSGVO weiterhin in Teilbereichen für schwierige Abgrenzungsfragen sorgen. Denn die DSGVO regelt in Art. 3 Abs. 1 die Anwendbarkeit der DSGVO nur für die Bereiche, in denen das Datenschutzrecht durch die DSGVO einheitlich geregelt sein wird und nicht durch Öffnungsklauseln der individuellen Regelung der Mitgliedstaaten vorbehalten bleibt. Für Fälle, in denen eine Öffnungsklausel aktiviert wird, besteht nach derzeitigem Stand noch kein spezifisches Kollisionsrecht. Sollte bis zur Anwendbarkeit der DSGVO auch kein spezifisches Kollisionsrecht erlassen werden, wird sich das territorial anwendbare Recht in diesen Fällen nach allgemeinem Kollisionsrecht richten. Ob diese durch die DSGVO gerissene Lücke im datenschutzrechtlichen Kollisionsrecht noch geschlossen wird, ist eine spannende Frage mit nicht unbeträchtlichen Auswirkungen für die Bestimmung des territorial anwendbaren Datenschutzrechtes im Bereich der von Öffnungsklauseln markierten Regelungsspielräumen.

Mit Art. 3 DSGVO wurde demnach eine wichtige Regelung geschaffen, die viele Fragen hinsichtlich des territorial anwendbaren Rechts klärt und den technologischen Gegebenheiten der heutigen Zeit angepasst ist. Eine

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

vollständige Klärung des territorial anwendbaren Datenschutzrechtes ist jedoch noch nicht erreicht.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kapitel 3: Datenschutzrechtliche Bewertung der Verarbeitung personenbezogener Daten in sozialen Netzwerken

Im Folgenden wird zunächst die Zulässigkeit der Verarbeitung personenbezogener Daten in sozialen Netzwerken sowohl nach dem BDSG bzw. der DSRL als auch nach der DSGVO sowie weiteren, gegebenenfalls anwendbaren bereichsspezifischen Regelungen bewertet. Dabei ist zwischen dem Nutzer-Nutzer-Verhältnis (dazu A.), dem Anbieter-Nutzer-Verhältnis (dazu B.) und der Verarbeitung durch Dritte (dazu C.) zu unterscheiden. Anschließend werden Betroffenenrechte und die Durchsetzbarkeit des Datenschutzrechts analysiert (dazu D.).

A. Zulässigkeit der Verarbeitung personenbezogener Daten im Nutzer-Nutzer-Verhältnis

Zunächst wird die Zulässigkeit der Verarbeitung personenbezogener Daten durch andere Nutzer näher betrachtet. Angesichts der großen Mengen an hochgeladenen Fotos von Nutzern anderer Nutzer oder „geteilten" Nutzerbeiträgen ist dabei durchaus überraschend, dass das Nutzer-Nutzer-Verhältnis in der Diskussion bislang eine untergeordnete Rolle spielt. Dabei lässt sich im Nutzer-Nutzer-Verhältnis ein Auseinanderfallen von Realität und Rechtslage erkennen: In der Nutzerrealität werden oftmals Fotos und Informationen über andere Personen in sozialen Netzwerken zugänglich gemacht. Das folgende Kapitel wird aufzeigen, dass für den überwiegenden Teil dieser Verarbeitung nach dem Regime des BDSG kein Erlaubnistatbestand zur Verfügung steht. Gleichzeitig sind jedoch die formellen Anforderungen an die Einwilligung durch das BDSG sehr hoch. In der Konsequenz ist nach dem BDSG-Regime – jedenfalls bei strenger Auslegung seiner Voraussetzungen – der Großteil der Interaktion der Nutzer miteinander datenschutzrechtlich unzulässig.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

I. Datenverarbeitung ausschließlich zu persönlichen oder familiären Tätigkeiten

Vor einer datenschutzrechtlichen Prüfung muss jedoch zunächst eruiert werden, ob die Datenverarbeitung in sozialen Netzwerken im Nutzer-Nutzer-Verhältnis überhaupt datenschutzrechtliche Relevanz besitzt, oder wegen der Ausnahme in § 1 Abs. 2 Nr. 3 a. E. BDSG bzw. Art. 3 Abs. 2 2. Spiegelstr. DSRL sowie Art. 2 Abs. 2 lit. c DSGVO vom sachlichen Anwendungsbereich dieser Regelwerke ausgenommen ist. Dies wäre der Fall, wenn das Teilen eines Beitrags eines anderen Nutzers auf der eigenen Pinnwand als „ausschließlich persönliche[ ] oder familiäre[ ] Tätigkeit[ ]" i. S. d. Normen zu qualifizieren wäre.

Dabei ist zu bedenken, dass nicht jede Datenverarbeitung im Nutzer-Nutzer-Verhältnis nach demselben Muster erfolgt; vielmehr sind die unterschiedlich in Betracht kommenden Nutzungsweisen sozialer Netzwerke für sich zu beleuchten. In Betracht kommen hierbei folgende Fallgruppen: Das Erstellen oder „Teilen" von Inhalten, die für jeden Internetnutzer zugänglich sind (dazu 1.); das Erstellen oder „Teilen" von Inhalten nur für einen bestimmten Personenkreis (dazu 2.); und die Kommunikation über netzwerkintern private Nachrichtenfunktionen, wie etwa dem *Facebook Messenger* (dazu 3.).

1. Öffentliche Inhalte

a) BDSG bzw. DSRL

Die Schwelle von dem privaten, gem. § 1 Abs. 2 Nr. 3 BDSG nicht dem sachlichen Anwendungsbereich des BDSG unterfallenden, Datenumgang zu dem datenschutzrechtlich relevanten Datenumgang ist niedrig anzusetzen und die in § 1 Abs. 2 Nr. 3 BDSG normierte Ausnahme sehr eng auszulegen.[273] Bei einer extensiven Auslegung dieser Ausnahme vom sachlichen Anwendungsbereich bestünde die Gefahr, dass eine Vielzahl von Handlungen nicht dem Datenschutzrecht unterfallen und ein datenschutzrechtliches Vakuum entstünde. Daher kann die Ausnahme nur dann greifen, wenn der Umgang mit personenbezogenen Daten i. S. d. § 1 Abs. 2 Nr. 3

273 *Damann*, in: Simitis, BDSG, § 1, Rn. 148; *Kühling/Raab*, in: Kühling/Buchner, DSGVO, Art. 1, Rn. 23.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

a. E. BDSG „ausschließlich" der persönlichen Sphäre des für die Verarbeitung Verantwortlichen unterfällt, nicht jedoch, wenn, wie in solchen Fällen, der private Bereich verlassen wird und der Verarbeitung damit „Außenbezug"[274] zukommt.

Unter dem datenschutzrechtlichen Regime der DSRL bzw. des BDSG war damit klar, dass bereits solche Beiträge nicht unter die Ausnahme fallen, die für jeden Internetnutzer einsehbar, also öffentlich, sind.[275] Dieser Außenbezug ist anzunehmen, wenn der ursprüngliche Beitrag allen Nutzern zugänglich ist und erst recht, wenn ein Beitrag durch das sog. Teilen auf dem eigenen Profil allen Nutzern zugänglich gemacht wird.[276]

b) DSGVO

Unter dem DSGVO-Regime bereitet die Auslegung dieser Ausnahme vom sachlichen Anwendungsbereich gerade mit Blick auf soziale Netzwerke aufgrund von EG 18 DSGVO Schwierigkeiten. EG 18 S. 2 Var. 3 DSGVO nennt explizit die Nutzung sozialer Netze als möglichen Teil einer familiären oder persönlichen Tätigkeit. Davon sind jedoch die Anbieter sozialer Netzwerke ausgenommen, EG 18 S. 3 DSGVO. Dies legt zunächst nahe, dass im Umkehrschluss Nutzer von der Ausnahme umfasst sind. Wie der Wortlaut („können") deutlich macht, gilt dies jedoch nicht uneingeschränkt.[277] Auch würde sich eine generelle Ausnahme für jegliche Datenverarbeitung durch die Nutzer in sozialen Netzwerken nicht in die Reihe der weiteren Beispiele aus EG 18 S. 2 DSGVO, wie das Führen eines Schriftverkehrs, eingliedern. Schließlich kann EG 18 S. 2 Var. 3, 4 DSGVO schon deswegen nicht als unbeschränkte Ausnahme vom sachlichen Anwendungsbereich gelten, weil nach EG 18 S. 1 DSGVO nur solche Tätigkeiten von Art. 2 Abs. 2 lit. c DSGVO umfasst sind, die „[…] ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen […] [werden]." Allerdings werden soziale Netzwerke wie Twitter oder Facebook auch von zahlreichen Nutzern zu wirtschaftlichen und beruflichen Zwecken genutzt. Damit ist bereits klar, dass nicht jegliche Nutzeraktivität

274 *Klar*, NJW 2015, 463, 465.
275 *EuGH,* Urt. v. 06.11.2003, Rs. C-101/01, ECLI:EU:C:2003:596, Rn. 47 – Lindqvist; *EuGH,* Urt. v. 16.12.2008, Rs. C-73/07, ECLI:EU:C:2008:727, Rn. 44 – Satakunnan Markkinapörssi und Satamedia.
276 Vgl. dazu Kap.3 Pkt. A.III., S. 110.
277 Ebenso *Albrecht/Jotzo,* Das neue Dateschutzrecht der EU, S. 67.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

in sozialen Netzwerken vom Anwendungsbereich der DSGVO ausgeschlossen sein kann.

Es finden sich auch keine Anhaltspunkte dafür, dass die DSGVO in so starker Weise von der bisherigen Auslegung des Haushalts- und Familienprivilegs abweichen wollte.[278] So war in EG 15 des Kommissionsentwurfs – jetzt EG 18 DSGVO – das Beispiel sozialer Netzwerke noch gar nicht genannt. Zudem ist der Wortlaut von Art. 2 Abs. 2 lit. c DSGVO mit dem seines Vorgängers, Art. 3 Abs. 2 2. Spiegelstr. DSRL, abgesehen von kleinen Veränderungen im Satzbau identisch. Damit ist davon auszugehen, dass im Internet veröffentlichte Beiträge nicht vom Anwendungsbereich der DSGVO ausgenommen sind.[279]

2. Beschränkung auf bestimmte Personengruppen

a) BDSG bzw. DSRL

Weiterhin stellt sich die Frage, ob solche erstellten oder „geteilten" Inhalte unter die Ausnahme fallen, die von Nutzern nur mit bestimmten Gruppen – etwa ihren Kontakten im jeweiligen Netzwerk – auf ihrem Profil geteilt werden. Problematisch daran ist, dass es nicht unüblich ist, mehrere hundert oder gar mehrere tausend Kontakte in sozialen Netzwerken zu haben. Die Standardeinstellungen der meisten sozialen Netzwerke sehen zudem vor, dass entweder alle Internetnutzer oder jedenfalls alle Kontakte des jeweiligen Nutzers und u. U. auch die Kontakte der Kontakte Zugriff auf die Beiträge haben, die ein Nutzer auf seinem Profil bereitstellt. Zusätzlich verstärkt wird das Problem durch die Möglichkeit, Beiträge anderer Nutzer auf dem eigenen Nutzerprofil zu „teilen".[280] So kommt es sehr schnell zur Zugriffsmöglichkeit von einer unüberschaubaren Anzahl von Personen auf die personenbezogenen Daten. Diese Gruppen aus dem sachlichen Anwendungsbereich der DSRL oder der DSGVO auszuschließen, liefe diametral zum erklärten Ziel der DSRL und der DSGVO, Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere hinsichtlich des Rechts auf

278 So auch *Schantz*, NJW 2016, 1841, 1843; *Kühling/Raab*, in: Kühling/Buchner, DSGVO, Art. 2, Rn. 25.

279 A. A. wohl *Schaffland/Holthaus*, in: Schaffland/Wiltfang, DSGVO, Art. 2, Rn. 23, die beispielhaft die Nutzung von *Facebook* als pauschal vom Anwendungsbereich der DSGVO ausgenommenen Fall nennen.

280 *Kühling/Raab*, in: Kühling/Buchner, DSGVO, Art. 2, Rn. 25; *Gola/Lepperhoff*, ZD 2016, 9, 11.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Schutz personenbezogener Daten zu schützen, Art. 1 Abs. 1 DSRL bzw. Art. 1 Abs. 2 DSGVO.

Auch die Entstehungsgeschichte der Ausnahme der Datenverarbeitung zu *ausschließlich* persönlichen oder familiären Zwecken spricht gegen den Ausschluss dieser Nutzungsformen von jeglichem datenschutzrechtlichem Schutz: In der Entwurfsbegründung zur DSRL aus dem Jahr 1990 wird zu der Ausnahme angeführt, dass sie aufgenommen wurde, weil im privaten bzw. persönlichen Bereich Eingriffe in das Persönlichkeitsrecht unwahrscheinlich wären: Als Beispiel nennt die Entwurfsbegründung persönliche elektronische Tagebücher.[281] In der Entwurfsbegründung zu 1992 wird ferner darauf hingewiesen, dass zu extensive Ausnahmen dazu führen könnten, dass die Rechte der Betroffenen nicht ausreichend gewahrt würden.[282] Die Ausnahme entspringt also dem Gedanken, dass im ausschließlich privaten Bereich – wie etwa in Tagebüchern – keine Datenschutzverletzungen drohen. Mit sozialen Online-Netzwerken, in denen auf vermeintlich „privaten" Nutzerprofilen personenbezogene Daten innerhalb kürzester Zeit einem tausendfachen Publikum zugänglich gemacht werden können, sind elektronische Tagebücher nicht vergleichbar. Von Art. 3 Abs. 2 2. Spiegelstr. DSRL sind Inhalte, die bestimmten Personengruppen zugänglich gemacht werden, daher nicht umfasst.[283]

b) DSGVO

Dies muss auch für Art. 2 Abs. 2 lit. c DSGVO gelten. Wie bereits ausgeführt, sind die beiden Normen im Wortlaut nahezu identisch. Zwar hatte das Parlament EG 15 des Parlamentsentwurfs[284] (jetzt EG 18 DSGVO) noch dahingehend ergänzen wollen, dass das Haushalts- und Familienprivileg auch dann greifen solle, wenn „[…] davon auszugehen ist, dass [die Daten] […] nur einer begrenzten Anzahl von Personen zugänglich sein werden."

---

281 COM(90) 314 final – SYN 287, Abl.EG 1990 C 277, 3, Discussion of the Provisions, S. 21.

282 COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 13.

283 A.A. *Piltz,* Soziale Netzwerke im Internet, Pkt. 4.2.4.2.1, S. 94 f., der grundsätzlich Nutzerprofile vom sachlichen Anwendungsbereich der DSRL ausnehmen möchte und auf die konkrete Verarbeitungssituation abstellt; a. A. *Kampert,* Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, S. 83 f., der für eine einzelfallbezogene Betrachtungsweise abhängig vom konkreten Nutzerverhalten plädiert.

284 Art. 2 Abs. 2 lit. d des Parlamentsentwurfs der DSGVO, P7_TA(2014)0212.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Dies könnte so ausgelegt werden, dass gerade „private" Nutzerprofile sozialer Netzwerke auch vom Schutz personenbezogener Daten nach der DSGVO ausgeschlossen sind. Allerdings lässt sich bereits daran zweifeln, ob im Falle sozialer Netzwerke die Zahl der Personen, die auf die personenbezogenen Daten zugreifen könnten, tatsächlich begrenzt wäre, da gerade durch netzwerkinterne Möglichkeiten wie etwa das Teilen von Beiträgen rasch eine unbegrenzte Anzahl von Personen Zugriff auf die Daten erhalten könnte. Zudem wurde diese Ergänzung nicht in den endgültigen Text aufgenommen. Dies spricht gegen eine Auslegung des Art. 2 Abs. 2 lit. c DSGVO in diesem Sinne.

3. Datenverarbeitung mittels der Nutzung von Nachrichtenfunktionen

Lediglich die dritte Fallgruppe, die Datenverarbeitung im Rahmen von Nachrichten, wird vom Anwendungsbereich der DSRL bzw. BDSG sowie der DSGVO ausgenommen. Der private Austausch von Nachrichten fällt unter das in EG 12 DSRL bzw. EG 18 DSGVO genannte Beispiel des „Schriftverkehr[s]". Die Fallgruppe unterscheidet sich von den anderen beiden Fallgruppen insoweit, als die Datenverarbeitung dort tatsächlich eng beschränkt zwischen bestimmten Personen stattfindet und eine Gefährdung für Persönlichkeitsrechte minimiert ist. Freilich ließe sich auch hier einwenden, dass mit einfachen Klicks die Daten anderen Personen zugänglich gemacht werden können; dieses Problem stellt sich faktisch jedoch auch mit Briefen. Tatsächlich werden Nachrichten jedoch in einem viel stärker begrenzten Empfängerkreis ausgetauscht als Inhalte auf Profilen. Ferner unterfiele das Zugänglichmachen der Daten an einen unbestimmten Personenkreis seinerseits wieder den entsprechenden datenschutzrechtlichen Bestimmungen. Der Austausch privater Nachrichten innerhalb eines sozialen Netzwerks ist daher von der Ausnahme vom sachlichen Anwendungsbereich der DSRL bzw. des BDSG sowie der DSGVO umfasst, sofern sie ausschließlich zu persönlichen oder familiären Zwecken erfolgt.

II. Nutzer als Verantwortlicher

Wer „[…] personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt […]" (§ 3 Abs. 7 BDSG) bzw. „[…] allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet […]" (Art. 2 lit. d DSRL bzw. Art. 4 Nr. 7 DSGVO) ist

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

der (für die Verarbeitung) Verantwortliche i. S. d. der DSRL und der DSGVO bzw. in der Terminologie des BDSG die verantwortliche Stelle.[285] Dabei ist der *Zweck* das „erwartete Ergebnis, das beabsichtigt ist oder die geplante Aktion leitet“[286] und das *Mittel* die „Art und Weise, wie ein Ergebnis oder Ziel erreicht wird“[287]. Der Verantwortliche steuert also das „Warum“ und „Wie“ der Verarbeitung.[288] Seine eigenständige Entscheidungsbefugnis über Zweck und Mittel der Verarbeitung ist dabei zentraler Faktor zur Bestimmung der Verantwortlichkeit.[289]

Die Bestimmung des Verantwortlichen ist Voraussetzung für das Eingreifen des materiell-rechtlichen Datenschutzrechts, da die Folgen bei Verstößen gegen das Datenschutzrecht stets an den Verantwortlichen geknüpft sind. Allerdings ist die Bestimmung des Verantwortlichen nicht immer zweifellos möglich. Auf Ebene der Nutzer ist zu unterscheiden zwischen Nutzern mit privaten Profilen (dazu 1.) und Betreibern öffentlicher Profile, die sich die Infrastruktur eines bestimmten sozialen Netzwerks zunutze machen, etwa um ihr Unternehmen zu bewerben (dazu 2.). Der folgende Abschnitt beleuchtet die verschiedenen Akteure in sozialen Netzwerken näher und bewertet ihre mögliche Einordnung als datenschutzrechtliche Verantwortliche.

1. Betreiber privater Profile

In der Gruppe der Nutzer ist zu unterscheiden zwischen Nutzern mit Profil als Privatperson und Nutzern mit öffentlichem Profil, etwa für die Bewerbung eines Unternehmens. Nutzer privater Profile haben in sozialen Netzwerken die Möglichkeit, nicht nur Informationen über sich selbst preis zu

---

285 Zur verwendeten Terminologie vgl. Kap. 1 Pkt. A, S. 31.

286 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsdatenverarbeiter". WP 169 (16.02.2010), S. 16.

287 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsdatenverarbeiter". WP 169 (16.02.2010), S. 16.

288 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsdatenverarbeiter". WP 169 (16.02.2010), S. 16; *Martini*, in: Paal/Pauly, DSGVO, Art. 26, Rn. 19.

289 Vgl. *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsdatenverarbeiter". WP 169 (16.02.2010), S. 10 f.; *BVerwG,* EuGH-Vorlage v. 25.02.2016, Az. 1 C 28/14, NVwZ 2016, 1737, Rn. 27.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

geben, sondern auch Informationen oder Bildnisse anderer Personen. Dabei erlauben soziale Netzwerke es ihren Nutzern üblicherweise, den Empfängerkreis hierfür auszuwählen: Die Inhalte können bestimmten Personen, allen mit dem Nutzer verbundenen Kontakten oder gar jedem Internetnutzer zugänglich gemacht werden. Für diese Informationen, die der Nutzer selbst auf seinem Profil einstellt, ist er der datenschutzrechtlich Verantwortliche i. S. d. Art. 2 lit. d DSRL bzw. Art. 4 Nr. 7 DSGVO. Er entscheidet allein über die Zwecke und Mittel dieser Verarbeitung, indem er bestimmt, ob, warum und in welcher Form er diese Informationen mit anderen Nutzern teilt.[290]

An der datenschutzrechtlichen Verantwortlichkeit der Nutzer für von ihnen selbst generierte Inhalte ändert nichts, dass die Daten zugleich dem Anbieter des sozialen Netzwerks zuwachsen. Es handelt sich hierbei gerade nicht um unterschiedliche „Phasen" der Datenverarbeitung[291], sondern um voneinander getrennte, in sich abgeschlossene Datenverarbeitungsvorgänge mit unterschiedlichen Verantwortlichen. Was der Nutzer wann und zu welchem Zeitpunkt einstellt, entzieht sich dem Einfluss des Anbieters des sozialen Netzwerks. Umgekehrt hat der Nutzer keinen Einfluss auf eine daran anschließende, andere Verarbeitung der Informationen durch den Plattformbetreiber.

Somit ist der Nutzer für von ihm generierte Inhalte in sozialen Netzwerken der datenschutzrechtlich Verantwortliche.

2. Betreiber öffentlicher Profile

Soziale Netzwerke bieten Nutzern neben der Möglichkeit, private Profile für sich selbst zu erstellen, auch die Möglichkeit, öffentliche Profile zu erstellen. Diese öffentlichen Seiten können zu verschiedensten Zwecken erstellt werden, etwa zur Bewerbung des eigenen Unternehmens, zur Diskussion gemeinsamer Ziele und Ideen, zur Information der Bürger durch Behörden, oder als „Fanclub" für Personen des öffentlichen Lebens. Dementsprechend vielschichtig ist die Gruppe der Betreiber dieser öffentlichen Profile. Die Beispiele für Betreiber öffentlicher Profile reichen von Nutzern, die für ihren „Star" eine Plattform für Fans eröffnen, über Einzelunternehmer, wie etwa die Betreiberin einer Pizzeria, bis hin zu bekannten Politikern

290 Ebenso *Jandt/Roßnagel*, ZD 2011, 160, 161.

291 So aber *Jandt/Roßnagel*, ZD 2011, 160, 161, die von einer „kollektiven" Verantwortlichkeit sprechen, aber zum selben Ergebnis kommen.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

und Persönlichkeiten, wie etwa dem Präsidenten der Vereinigten Staaten oder Popstars.

a) Funktionsweise von öffentlichen Profilen am Beispiel von *Facebook*

Sobald ein Nutzer eine solche Fanpage erstellt, stellt *Facebook* ihm kostenlos und unaufgefordert eine Reihe von Statistiken über die Besucher der Seite zur Verfügung. Diese Statistiken umfassen zunächst in anonymisierter Form die Anzahl der Seitenaufrufe, die Anzahl der Nutzer, die mittels eines Klicks auf den Link „gefällt mir" der Seite entweder von sich aus oder über andere Kontakte („organisch") oder durch bezahlte Werbeanzeigen („bezahlt") gefolgt sind, die Reichweite der Seite, d. h. die Anzahl der Nutzer, die „organisch" oder „bezahlt" erreicht wurden, sowie Interaktionen mit von der Fanpage erstellten Beiträgen, d. h. Reaktionen oder Klicks auf Beiträge. Ferner erhält der Fanpage-Betreiber Informationen über die Namen der Nutzer der Fanpage, wobei er dauerhafte Einsicht in die Liste derjenigen Kontakte, die mit seinem privaten Nutzerprofil verbunden sind, erhält. Wenn ein Nutzer, mit dem der Fanpage-Betreiber auf seinem privaten Nutzerprofil nicht vernetzt ist, Beiträge seiner Fanpage mittels des „Like-Buttons" verfolgt, bekommt der Fanpage-Betreiber für einen kurzen Zeitraum dessen Namen zur Verfügung gestellt; der Nutzer taucht mit seinem Namen aber nicht dauerhaft auf der Liste der Nutzer auf, die die Fanpage mit „gefällt mir" markiert haben.

Der Fanpage-Betreiber hat keine Möglichkeit, auf die Bereitstellung dieser Statistiken zu verzichten, noch wird er vor Erstellung der Fanpage, die mittels weniger Klicks möglich ist, explizit auf diesen Dienst hingewiesen.

Zugleich verwertet auch *Facebook* diese Daten für sich. Insbesondere werden dabei nicht nur Daten, die Besucher der Fanpage durch aktives Tun erbringen, verarbeitet. So werden bei dem Besuch einer Fanpage auch die

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

IP-Adresse[292] des Besuchers an *Facebook* übertragen und Cookies auf dessen Endgerät gesetzt und zwar sowohl bei *Facebook*-Nutzern als auch Besuchern ohne Profil bei *Facebook*.[293]

b) Verantwortlichkeit der Fanpage-Betreiber

Besonders in die Diskussion geraten ist in diesem Zusammenhang der von *Facebook* angebotene Dienst zur Erstellung sog. „Fanpages" durch eine Anordnung des ULD an ein Unternehmen, die Fanpage auf *Facebook* zu deaktivieren. Gegen diese Anordnung wendete sich das Unternehmen vor dem *VG Schleswig*[294]. Das ULD hatte argumentiert, dass die Fanpage-Betreiber verantwortliche Stelle i. S. d. § 12 Abs. 3 TMG i. V. m. § 3 Abs. 7 BDSG für die Erhebung, Verarbeitung und Nutzung der Nutzungsdaten i. S. d. § 15 TMG durch *Facebook* seien. Durch die Errichtung der Fanpage leisteten die Fanpage-Betreiber einen „aktiven und willentlichen Beitrag zur Erhebung"[295]. Zudem initiierten die Betreiber durch die Fanpage die Nutzung und machten sie gezielt möglich.[296] Dadurch steuerten die Fanpage-Betreiber die Zuführung der Daten an *Facebook* und entschieden nicht nur über den Zweck der Erhebung, Verarbeitung und Nutzung, sondern

---

292 Zur Frage der IP-Adresse als personenbezogenes Datum vgl. *Meyerdierks*, MMR 2009, 8; *Kirchberg-Lennartz/Weber*, DuD 2010, 479; *Eckhardt*, CR 2011, 339; *Gerlach*, CR 2013, 478; *Kühling/Klar*, NJW 2013, 3611; *Karg*, MMR-Aktuell 2011, 315811; *Lundevall Unger/Tranvik*, ZD-Aktuell 2012, 03004; *Breyer*, ZD 2014, 400; *Nink/Pohle*, MMR 2015, 563; *Weinhold*, ZD-Aktuell 2016, 5366; *Richter*, EuZW 2016, 909; *Kühling/Klar*, ZD 2017, 24; *Wulf*, DB 2017, 111; *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, E-CLI:EU:C:2016:779 – Breyer; *BGH*, Urt. v. 16.05.2017, Az. VI ZR 135/13, ZD 2017, 424.

293 *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 9.

294 *VG Schleswig,* Urt. v. 09.10.2013, Az. 8 A 218/11, abrufbar unter https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf (abgerufen am 13.10.2017).

295 *VG Schleswig,* Urt. v. 09.10.2013, Az. 8 A 218/11, abrufbar unter https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf (abgerufen am 13.10.2017), S. 4.

296 *VG Schleswig,* Urt. v. 09.10.2013, Az. 8 A 218/11, abrufbar unter https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf (abgerufen am 13.10.2017), S. 4.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

auch über das wesentliche Mittel.[297] Nach Ansicht des ULD soll dies sogar gelten, wenn die Fanpage-Betreiber die Daten selbst nur in anonymisierter Form erhalten.

aa) Datenschutzrechtliche Verantwortlichkeit

Die Argumentation des ULD ist vergleichbar mit der Strafbarkeit des Gehilfen i. S. d. § 27 StGB.[298] Die Unterstützung „durch Rat und Tat"[299] zur vorsätzlichen, rechtswidrigen Haupttat löst die eigene Strafbarkeit des Gehilfen aus. Genauso soll nach Ansicht des ULD bereits die Hilfeleistung zur Datenverarbeitung durch *Facebook* durch die bloße Inanspruchnahme eines Services die datenschutzrechtliche Verantwortlichkeit der Fanpage-Betreiber auslösen. Allerdings sieht das deutsche und europäische Datenschutzrecht eine solche Verantwortung des „Gehilfen", im Gegensatz zum deutschen Strafrecht, gerade nicht vor. Im Gegenteil muss für die Aktivierung der Verantwortlichkeit eine eigene *Entscheidung* über das „Warum" und „Wie" des Verarbeitungsvorgangs vorliegen. Ausnahmen hiervon sind, abgesehen von der Auftragsdatenverarbeitung (dazu d.), nicht vorgesehen. Der Fanpage-Betreiber hat aber keinen Einfluss auf die Verarbeitung von Nutzungsdaten durch *Facebook*. Weder steuert er den Zweck, den *Facebook* mit der Datenverarbeitung verfolgt; noch hat der Fanpage-Betreiber Einfluss, oder auch nur Einblick, auf die Mittel dieser Datenverarbeitung. Aus diesen Gründen scheiterte das ULD sowohl vor dem *VG* als auch dem *OVG Schleswig*.[300] Das *OVG Schleswig* legte zutreffend dar, dass die Fanpage-Betreiber weder rechtlichen noch tatsächlichen Einfluss auf die Art der Verarbeitung personenbezogener Daten durch *Facebook* haben.[301]

Dieses Ergebnis gilt sowohl für eine eigene Verantwortlichkeit als auch für eine Mitverantwortlichkeit von Fanpage-Betreibern. Sowohl die DSRL als auch die DSGVO sehen dem Wortlaut nach die Möglichkeit vor, dass die Entscheidungsgewalt nicht nur alleine, sondern auch „gemeinsam mit anderen" (Art. 2 lit. d DSRL, Art. 4 Nr. 7 DSGVO sowie Art. 26 DSGVO) ausgeübt werden kann. Obwohl der Wortlaut des BDSG hiervon abweicht

297 *VG Schleswig,* Urt. v. 09.10.2013, Az. 8 A 218/11, abrufbar unter https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf (abgerufen am 13.10.2017), S. 4.
298 So auch *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 8.
299 *Joecks*, in: MüKo-StGB, § 27, Rn. 5.
300 *OVG Schleswig,* Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, 643, 644.
301 *OVG Schleswig,* Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, 643, 644.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

– gem. § 3 Abs. 7 BDSG ist verantwortliche Stelle, wer Daten „[…] für sich selbst erhebt, verarbeitet oder nutzt […]" – ist anerkannt, dass auch unter dem BDSG-Regime eine solche Mitverantwortlichkeit in richtlinienkonformer Auslegung möglich sein muss.[302] Gleichwohl setzt auch diese Mitverantwortung eine Entscheidungsbefugnis aller Verantwortlichen voraus. Im vorliegenden Fall hat der Fanpage-Betreiber jedoch keinerlei Entscheidungsgewalt über den Verarbeitungsprozess. Seine Entscheidungsbefugnis erschöpft sich darin, ob er den Betrieb einer Fanpage aufnimmt bzw. aufrechterhält, oder nicht. Diese Entscheidung ist jedoch losgelöst von jeglichen durch *Facebook* vorgenommenen Verarbeitungsprozessen zu betrachten und kann daher nicht als Anhaltspunkt für die Verantwortlichkeit für die Datenverarbeitung von Fanpage-Betreibern herangezogen werden.[303]

bb) Verantwortlichkeit i. S. d. TMG

Klarzustellen ist insoweit auch, dass sich aus den Regelungen des TMG kein anderes Ergebnis ergibt. Fanpage-Betreiber können zwar als Diensteanbieter i. S. d. § 2 S. 1 Nr. 1 TMG zu qualifizieren sein. Hierfür reicht es bereits aus, wenn eine „[…] natürliche oder juristische Person eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt […]". Auch wenn Fanpage-Betreiber selbst Nutzer eines sozialen Netzwerks sind, können sie also zugleich Diensteanbieter sein.[304] Als solche trifft sie eine Verantwortlichkeit gem. §§ 7 ff. TMG für die Inhalte ihrer Fanpage. §§ 7 ff. TMG regelt jedoch nur die inhaltliche Verantwortlichkeit,

302 *Eßer*, in: Auernhammer, BDSG, § 3, Rn. 76; *Monreal*, ZD 2014, 611, 614; *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 5; a. A. *Dammann,* in: Simitis, BDSG, § 3, Rn. 226, nach dem die Auslegung der gemeinsamen Verantwortlichkeit bereits vom Wortlaut des § 3 Abs. 7 BDSG gedeckt ist.

303 An diesem Ergebnis wird sich auch mit Art. 26 DSGVO, der eine Ausgestaltung für die bereits bestehende Regelung schafft, dass es gemeinsam für die Verarbeitung Verantwortliche geben kann, nichts ändern. Denn auch gem. Art. 26 DSGVO kommt es auf die tatsächliche Steuerungsmöglichkeit auf die Verarbeitung an, vgl. *Martini*, in: Paal/Pauly, DSGVO, Art. 26, Rn. 18.

304 *Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages*, "Facebook-Kampagne" des ULD, abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017), S. 12; *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 4; *OVG Schleswig,* Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, 643, 644.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

über die vorliegend in Frage stehende datenschutzrechtliche Verantwortlichkeit sagt der Abschnitt nichts aus. Datenschutzrechtliche Regelungen finden sich in §§ 11 – 15a TMG. Allerdings gelten die dortigen Bestimmungen alleine für eine eigene Erhebung und Verwendung der Daten des Diensteanbieters. Im vorliegenden Fall geht es jedoch um eine Verarbeitung personenbezogener Daten durch *Facebook*, die dem Fanpage-Betreiber zuteil wird.[305] Eine eigenständige Regelung darüber, wer Verantwortlicher ist, enthält das TMG hingegen nicht. Es sind gem. § 12 Abs. 3 TMG die allgemeinen Vorschriften über personenbezogene Daten heranzuziehen,[306] also die bereits diskutierten Normen des BDSG bzw. der DSRL, die im Mai 2018 von der DSGVO abgelöst werden.

c) Fanpages als Form der Auftragsverarbeitung

Das *VG* und *OVG Schleswig* befassten sich auch mit der Frage, ob *Facebook* möglicherweise die Daten im Auftrag der Fanpage-Betreiber verarbeitet, mithin also ein Fall der Auftragsverarbeitung[307] vorliegt. Die Auftragsverarbeitung ist einer der gesetzlich vorgesehenen Fälle, in denen die Verantwortlichkeit und die Verarbeitung auseinanderfallen können, vgl. § 11 BDSG, Art. 2 lit. e DSRL, Art. 4 Nr. 8, Art. 28 DSGVO. Wesentliches Merkmal ist dabei, dass, obschon die Verarbeitung nicht vom Verantwortlichen selbst ausgeführt wird, dieser über die Zwecke und Mittel der Verarbeitung bestimmt und die Verarbeitung durch den Auftragsverarbeiter auf Weisung des Verantwortlichen ausgeführt wird, der Auftragsverarbeiter also als „verlängerter Arm“ des Verantwortlichen agiert.[308]

---

305 *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 4; *OVG Schleswig,* Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, 643, 644.

306 *Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages*, "Facebook-Kampagne" des ULD, abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017), S. 14; *Piltz*, K&R 2014, 80, 82; *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 4; *OVG Schleswig,* Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, 643, 644; *Hoffmann/Schulz/Brackmann*, ZD 2013, 122, 123 f.; *Schröder/Hawxwell/Münzing*, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins, abrufbar unter https://www.datenschutzzentrum.de/uploads/facebook/WissDienst-BT-Facebook-ULD.pdf (abgerufen am 13.10.2017), S. 8.

307 Vorliegend wird der Terminologie der DSGVO gefolgt.

308 *Martini*, in: Paal/Pauly, DSGVO, Art. 28, Rn. 2; *Petri*, in: Simitis, BDSG, § 11, Rn. 20.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Bei einem Fanpage-Betreiber und *Facebook* liegt so eine Auftragsbeziehung jedoch gerade nicht vor. Wie bereits ausgeführt, nimmt *Facebook* die Datenverarbeitung automatisch und ungefragt vor. Der Fanpage-Betreiber hat keine Möglichkeit, sich gegen die Verarbeitung von Nutzungsdaten von Besuchern seiner Fanpage auszusprechen. Ferner hat er keinen Einfluss auf die Zwecke und Mittel der Verarbeitung, s.o. Erst recht ist ein Fanpage-Betreiber gegenüber *Facebook* nicht weisungsbefugt.[309] Dem Fanpage-Betreiber wachsen die Daten vielmehr ungefragt zu. Dabei erhält der Fanpage-Betreiber den Großteil der Daten lediglich in anonymisierter Form. Eine Auftragsverarbeitung durch *Facebook* im Auftrag der Fanpage-Betreiber ist somit ausgeschlossen.

d) Fanpagebetreiber als Auswahlverantwortliche

Fraglich ist jedoch, ob Fanpage-Betreibern eine Verantwortung für die sorgfältige Auswahl des Plattform-Betreibers, auf dessen Plattform sie ein an die Öffentlichkeit gerichtetes Profil betreiben, zukommt.

aa) Auswahlverantwortlichkeit als Teil der Auftragsverarbeitung

Diese Auswahlverantwortlichkeit könnte sich aus § 11 Abs. 2 S. 1 und § 4 BDSG[310] bzw. Art. 17 Abs. 2 DSRL[311] und in der DSGVO aus Art. 28 Abs. 1 DSGVO ergeben. Diese Normen sehen für die *Auftragsverarbeitung* vor, dass der Verantwortliche den Auftragsverarbeiter sorgfältig hinsichtlich der von diesem getroffenen technischen und organisatorischen Maßnahmen auszuwählen hat. Wie dargestellt,[312] liegt bei dem Betrieb von Fanpages jedoch keine Auftragsverarbeitung vor. Die Übertragung der Auswahlverantwortlichkeit von der Auftragsverarbeitung auf die Fallgruppe

309 So auch *VG Schleswig,* Urt. v. 09.10.2013, Az. 8 A 218/11, abrufbar unter https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf (abgerufen am 13.10.2017), S. 10; *OVG Schleswig,* Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, 643, 644; *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 6.

310 *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 12 ff.

311 *BVerwG,* EuGH-Vorlage v. 25.02.2016, Az. 1 C 28/14, NVwZ 2016, 1737, Rn. 35 ff.

312 Dazu Kap. 3 Pkt. A.II.2.c, S. 104.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

der Betreiber öffentlicher Profile wird mit einem Erst-Recht-Schluss begründet: Da *Facebook* kein Auftragnehmer im Auftragsverarbeitungsverhältnis ist, stehen *Facebook* bei der Datenverarbeitung größere Freiheiten zu als dem Auftragnehmer. Wenn Fanpage-Betreiber der Plattform, auf der sie ihr öffentliches Profil betreiben, aber größere Freiheiten zugestehen, als sie einem Auftragnehmer zugestehen würden, rechtfertigt dies erst recht, dass ihnen bei der Auswahl des Plattform-Betreibers ebenso eine Auswahlverantwortung zukommt wie bei der Auswahl eines Auftragnehmers.[313]

Allerdings knüpft diese Argumentation an die Annahme an, dass der Fanpage-Betreiber dem Plattform-Betreiber etwas *zugestehen* würde, es also in seiner Macht stünde, dem Plattform-Betreiber Rechte und Pflichten einzuräumen und zu entziehen. Genau diese Verhandlungsmacht gegenüber dem Plattform-Betreiber hat der Fanpage-Betreiber aber gerade nicht. Läge es in der Hand des Fanpage-Betreibers über die Verarbeitungsparameter zu verhandeln, müsste man wohl von dem Vorliegen einer Auftragsverarbeitung ausgehen. Das Vorliegen eines Auftragsverhältnisses wird aber gerade abgelehnt, weil Absprachen zur Verarbeitung zwischen dem Fanpage-Betreiber und *Facebook* völlig fehlen.

Überdies ist die Annahme einer Auswahlverantwortlichkeit nur dann gerechtfertigt, wenn Fanpage-Betreiber tatsächlich eine *Wahl* hinsichtlich der Plattform-Betreiber haben. Ob angesichts der Größe von *Facebook* insbesondere kleinere Unternehmen auf die Repräsentation ihres Unternehmens verzichten können, mag bezweifelt werden. Aufgrund der hohen Nutzeranzahl des sozialen Netzwerks kann eine Vielzahl von Menschen erreicht werden. Insbesondere für junge Menschen stellen soziale Netzwerke eine wichtige Informationsquelle dar. Würden Fanpage-Betreiber gezwungen, auf ihre öffentlichen Profile zu verzichten, müssten sie also auf einen wichtigen Publikumskanal verzichten.

Schließlich müsste diese Auswahlverantwortung, konsequent fortgedacht, nicht nur für Betreiber öffentlicher Profile, sondern auch für Nutzer privater Profile gelten. Denn ebenso wie *Facebook* den Fanpage-Betreibern Statistiken zur Verfügung stellt, werden in anderen sozialen Netzwerken auch privaten Nutzern Statistiken, etwa über Besucherzahlen des eigenen Profils und sogar der Profile anderer Nutzer, zur Verfügung gestellt.[314]

---

313 *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 12.

314 So stellt etwa *LinkedIn* jedem Nutzer die Anzahl der Seitenbesuche in den letzten 90 Tagen sowie ein „Ranking" des eigenen Profils im Vergleich zu den eigenen Kontakten sowie zu anderen Nutzern, die bei demselben Arbeitgeber arbeiten, zur Verfügung; bei „Premium"-Accounts stellt das Netzwerk sogar die Klarnamen der Seitenbesucher zur Verfügung.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Diese Ausstrahlwirkung der Annahme einer Auswahlverantwortung käme damit einem faktischen Verbot der Nutzung führender sozialer Netzwerke gleich.

bb) Grundrechtliche Implikationen der Auswahlverantwortlichkeit

Zudem sind die grundrechtlichen Implikationen der Annahme einer Auswahlverantwortlichkeit zu bedenken. Soweit sich ein hoheitliches Nutzungsverbot, etwa in Form einer Anordnung durch die zuständige Datenschutzaufsichtsbehörde, wie es im eingangs erwähnten Fall durch das ULD der Fall war[315], gegen private, also nicht staatliche, Nutzer richtet, müssen die einander gegenüberstehenden Grundrechtspositionen sorgfältig abgewogen werden. In Betracht kommen insoweit ein Eingriff in Art. 12 und ggf. 14 GG[316] bzw. Art. 15 und 16 GRCh bei Profilen mit beruflichem Bezug und Fanpages von Unternehmen einerseits und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bzw. Art. 8 GRCh andererseits. Betroffen sein könnten zudem die Rechte aus Art. 5 Abs. 1 GG bzw. Art. 11 Abs. 1 GRCh der Fanpage-Nutzer selbst, also auch der Personen, deren Grundrechte durch ein Nutzungsverbot eigentlich geschützt werden sollten. So ist für Fanpage-Betreiber, die das öffentliche Profil zum Meinungsaustausch über bestimmte Ansichten nutzen, die Argumentation unter dem Gesichtspunkt der Meinungsfreiheit nicht unkritisch, insbesondere, da andere Kanäle zum Meinungsaustausch oft nicht dieselbe Reichweite aufweisen werden.

Zumindest in den Fällen, in denen *Facebook* die Nutzungsdaten anderer Nutzer des Netzwerks verarbeitet, darf bei der Abwägung nicht außer Acht gelassen werden, dass sich diese Nutzer aus eigener Entscheidung auf die Verarbeitung ihrer Daten durch *Facebook* eingelassen haben und diese Entscheidung Ausdruck ihres Rechts auf informationelle Selbstbestimmung ist.

315 Vgl. *VG Schleswig,* Urt. v. 09.10.2013, Az. 8 A 218/11, abrufbar unter https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf (abgerufen am 13.10.2017); *OVG Schleswig,* Urt. v. 04.09.2014, Az. 4 LB 20/13, ZD 2014, 643; *BVerwG,* EuGH-Vorlage v. 25.02.2016, Az. 1 C 28/14, NVwZ 2016, 1737.

316 Vgl. *VG Schleswig,* Urt. v. 09.10.2013, Az. 8 A 218/11, abrufbar unter https://www.datenschutzzentrum.de/facebook/20131009-vg-urteil-fanpages.pdf (abgerufen am 13.10.2017), S. 8.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Dieser Umstand führt freilich nicht automatisch zur Zulässigkeit der Datenverarbeitung durch *Facebook*[317], kann aber für ein Überwiegen der Grundrechte der Fanpage-Betreiber und Nutzer der Fanpage sprechen.[318] Teilweise wird jedoch argumentiert, dass Besuchern von Fanpages gar nicht bewusst ist, dass sie sich auf einer *Facebook*-internen Seite befinden, sondern das Interesse zuvorderst der Fanpage selbst gilt.[319] Dabei machen jedoch gute sichtbare Logos und nicht zuletzt die URL kenntlich, dass es sich um ein Angebot von *Facebook* handelt, was für versierte Internetnutzer durchaus erkennbar ist. Natürlich schützt dies insbesondere Internetnutzer, die keine registrierten Nutzer des sozialen Netzwerks sind, nicht davor, versehentlich die Internetseite zu besuchen. Abgesehen von derartigen Zufallsbesuchen ist jedoch davon auszugehen, dass sich das Gros der Besucher der Fanpages durchaus bewusst ist, dass sie sich gerade auf einer Seite des sozialen Netzwerks befinden.

cc) Zumutbarkeit der Auswahlverantwortlichkeit

Schließlich sehen Befürworter der Auswahlverantwortlichkeit ihre Grenze in der Zumutbarkeit für den Fanpage-Betreiber; diese sei nur gegeben, wenn der Verstoß gegen Datenschutzrecht durch *Facebook* für den Fanpage-Betreiber offensichtlich sei.[320] Dabei muss sich allerdings vor Augen geführt werden, dass Fanpages gerade nicht nur von großen Unternehmen genutzt werden, sondern auch von Einzelunternehmern und Nutzern, die die Seiten zum Meinungsaustausch nutzen. Insbesondere in diesen Fallgruppen ist nicht nachvollziehbar, weshalb dem „Durchschnittsnutzer" einerseits nicht zugesprochen wird, dass er in der Lage ist zu erkennen, wenn er sich auf *Facebook* befindet; sobald sich ein Angehöriger derselben Gruppe aber mittels weniger Klicks entscheidet, eine Fanpage zu eröffnen, ihm damit zugleich üblicherweise klar sein wird, dass seine Fanpage von *Facebook* verwendet wird, um personenbezogene Daten zu verarbeiten. Sollte man eine Auswahlverantwortlichkeit von Fanpage-Betreibern befürworten, muss die

317 Vgl. hierzu Kap. 3 Pkt. B, S. 154.
318 Strenger können hingegen öffentliche Stellen in die Pflicht genommen werden; vgl. dazu ausführlich *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 13; vgl. zum Betrieb von Facebook-Fanpages durch öffentliche Stellen auch *Hoffmann/Schulz/Brackmann*, ZD 2013, 122, 125 f
319 So aber *Weichert*, ZD 2014, 1, 2.
320 *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 12.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Zumutbarkeit im Einzelfall entschieden werden; zumindest bei durchschnittlichen Nutzern – also gerade keinen Unternehmen mit starker Wirtschaftsmacht – ist jedoch fraglich, ob ihnen die Hilfsfunktion, die ihre Fanpage für die Datenverarbeitung durch *Facebook* darstellt, in vollem Ausmaß bekannt ist.

e) Zusammenfassung

Fanpage-Betreiber sind weder Verantwortliche für die Datenverarbeitung durch *Facebook* noch ist *Facebook* Auftragsverarbeiter für die Fanpage-Betreiber; ihm fehlen hierzu jeweils bereits die Einflussmöglichkeiten auf Zweck und Mittel, also das „Ob", „Warum" und „Wie" der Datenverarbeitung.

Auch über das Konstrukt der sog. „Auswahlverantwortlichkeit" kann privaten Fanpage-Betreibern nicht die Pflicht zur sorgfältigen Auswahl der Plattform, auf der die Fanpage betrieben wird, auferlegt werden. Einfachgesetzlich trifft diese Verpflichtung nämlich nur den Verantwortlichen, der sich eines Auftragsverarbeiters bedient; dies liegt, wie dargelegt, hier gerade nicht vor. Zudem müsste in konsequenter Fortschreibung des Gedankens der „Auswahlverantwortlichkeit" diese nicht nur Fanpage-Betreiber, sondern auch Nutzer privater Profile treffen: Schließlich sind auch sie, je nach sozialem Netzwerk, in nicht gerade geringem Umfang Profiteur anonymer Nutzerstatistiken und ein entscheidender Faktor für das Geschäftsmodell sozialer Netzwerke. Zudem dürfen bei einem Verbot von Fanpages mittels Deaktivierungs-Anordnungen durch die Datenschutzbehörden die grundrechtlichen Implikationen nicht außer Acht gelassen werden. In einer Abwägung widerstreitender Interessen muss auch einbezogen werden, dass Nutzer von Fanpages das Risiko der Datenverarbeitung als Ausdruck ihres Rechts auf informationelle Selbstbestimmung wissentlich hinnehmen. Zudem würde die Auswahlverantwortlichkeit regelmäßig an der Grenze der Zumutbarkeit scheitern. Hierzu müsste es für den Fanpage-Betreiber offensichtlich sein, dass seine Fanpage ein Hilfsmittel zur Datenverarbeitung durch *Facebook* ist.[321] Diese Offensichtlichkeit wird oftmals nicht gegeben sein.

321 *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 12.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Die Frage, ob Fanpage-Betreibern eine Auswahlverantwortlichkeit zukommt, hat das *BVerwG* nunmehr dem *EuGH* vorgelegt.[322] Auch wenn der *EuGH* in der Vergangenheit dem Schutz personenbezogener Daten den Vorrang gegeben hat und andere Grundrechte in multipolaren Rechtsverhältnissen nicht immer hinreichend bei seiner Abwägung berücksichtigt hat,[323] bleibt zu hoffen, dass der *EuGH* in dem hier vorliegenden Fall des Nutzer-Nutzer-Verhältnisses eine sorgfältige Abwägung der gegenläufigen Interessen vornimmt und dabei auch berücksichtigt, dass eine Auswahlverantwortlichkeit nur für den Fall der Auftragsverarbeitung vorgesehen ist.

III. Zulässigkeit der Verarbeitung von Informationen Anderer

Soziale Netzwerke stellen ihren Nutzern eine Reihe von Funktionen zur Verfügung, mittels derer sie personenbezogene Daten Anderer, und zwar sowohl von Nutzern als auch Nicht-Nutzern des Netzwerks, verarbeiten können. Unterschieden werden kann dabei insbesondere das Hochladen von Inhalten vom Teilen von Inhalten. Beim Hochladen generiert der Nutzer selbst den Inhalt im sozialen Netzwerk, indem er beispielsweise auf seinem Profil Inhalte postet. So ist es durchaus nicht unüblich, dass Nutzer auf ihrem Profil nicht nur mitteilen, was sie gerade tun, sondern auch mit wem. In diesem Beispiel wäre der (Klar-)Name der anderen Person das in Frage stehende personenbezogene Datum.

„Teilen" bzw. „Sharing" ist eine Funktion, die von vielen sozialen Netzwerken bereitgestellt wird und den Nutzern ermöglicht, mittels eines Klicks auf einen Link die von anderen Nutzern entweder originär hochgeladenen oder selbst geteilten Inhalte weiterzuverbreiten. Hierbei erscheint der geteilte Inhalt auf dem eigenen Nutzerprofil, meist unter Angabe des Nutzers, von dessen Profil der Inhalt geteilt wurde (und damit nicht notwendigerweise unter Angabe des originär hochladenden Nutzers). Mit dieser Methode finden bestimmte Zitate, Bildnisse oder Videos massenhafte Verbreitung im Netz. Das folgende Kapitel bewertet die Zulässigkeit des Hochladens und Teilens von Informationen unter datenschutzrechtlichen Gesichtspunkten.

---

322 *EuGH,* Vorabentscheidungsersuchen des BVerwG v. 14.04.2016, Rs. C-210/16, ABl.EU 2016 C 260, 18 – Wirtschaftsakademie Schleswig-Holstein; *BVerwG,* EuGH-Vorlage v. 25.02.2016, Az. 1 C 28/14, NVwZ 2016, 1737.

323 Vgl. etwa *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650; kritisch hierzu *Kühling/Heberlein*, NVwZ 2016, 7, 12.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

1. Rechtliche Einordnung

Für die Bewertung der Zulässigkeit des Hochladens und Teilens von Informationen Anderer muss das Handeln zunächst in den rechtlichen Kontext eingeordnet werden. Soweit mit den Informationen personenbezogene Daten hochgeladen oder geteilt werden, handelt es sich um eine Verarbeitung i. S. d. Art. 2 lit. b DSRL bzw. Art. 4 Nr. 2 DSGVO. Fraglich ist jedoch, in welcher Form die Verarbeitung stattfindet, insbesondere auch, weil hiervon die Bestimmung der einschlägigen BDSG-Normen abhängt.

In Betracht kommt jeweils zunächst eine Weitergabe durch Übermittlung bzw. Verbreitung i. S. d. Art. 2 lit. b Alt. 2 Var. 9 DSRL bzw. eine Offenlegung durch Übermittlung bzw. Verbreitung i. S. d. Art. 4 Nr. 2 Alt. 2 Var. 10 DSGVO. Dies gilt sowohl für das Hochladen als auch das Teilen der Informationen. Denn in beiden Fällen werden die Informationen Dritten mitgeteilt. Dies gilt selbst, wenn ein Nutzer personenbezogene Daten Anderer in einem sozialen Netzwerk, beispielsweise auf seinem Profil, hochlädt, diese aber mittels entsprechender Funktionen im sozialen Netzwerk anderen Nutzern nicht zugänglich macht. Denn selbst dann hätte zumindest der Betreiber des sozialen Netzwerks Zugriff auf diese Daten. Die sprachliche Unterscheidung zwischen „Weitergabe“ und „Offenlegung“ in den deutschen Sprachfassungen der DSRL bzw. DSGVO hat keine materiellrechtliche Bedeutung, wie die Begriffsgleichheit in den englischen Fassungen sowohl der DSRL als auch der DSGVO mit „disclosure by transmission“ zeigt. Die Verbreitung ist eine Form der gelisteten Weitergabe- bzw. Offenlegungsmechanismen, die in Art. 2 lit. b DSRL sowie Art. 4 Nr. 2 DSGVO genannt wurden. Dies zeigt auch der ursprüngliche Vorschlag der Kommission für die Definition des Verarbeitungsbegriffs. Dort war die Verarbeitung als „die mit oder ohne Hilfe automatisierter Verfahren vorgenommenen Vorgänge: […] Weitergabe, insbesondere die Übermittlung, Verbreitung, Erstellung von Auszügen sowie das Sperren und Löschen […]“ definiert.[324]

Die Unterschiede in den Sprachfassungen und den Regelwerken zeigen, dass die Weitergabe und Verbreitung zwar nicht gänzlich synonym sind, eine Abgrenzung jedoch vom Gesetzgeber nicht klar getroffen wurde und wegen der gemeinsamen Regelung in Art. 2 lit. b DSRL bzw. Art. 4 Nr. 2 DSGVO auch nicht getroffen werden muss. Laut Duden können die Be-

324 Art. 2 lit. d des Kommissionsvorschlags, KOM(90) 314 endg. – SYN 287, ABl.EG 1990 C 277, 3.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

griffe synonym verwendet werden, wobei Verbreitung auch die Veröffentlichung von Daten beinhalten kann, wohingegen die Weitergabe auch im kleineren Kreis erfolgen kann.[325] Im Falle des Hochladens oder Teilens eines Beitrags eines anderen Nutzers auf der eigenen Pinnwand wird es sich wohl sowohl um eine Weitergabe (in der Terminologie des BDSG um eine Übermittlung) als auch eine Verbreitung handeln. Aus rechtlicher Sicht zieht die Unterscheidung jedoch keine unterschiedlichen Konsequenzen nach sich.

Im BDSG ist mit § 3 Abs. 4 S. 2 Nr. 3 nicht die Weitergabe bzw. Offenlegung, sondern nur die Übermittlung geregelt. Diese wird jedoch als „[…] Bekanntgeben […] personenbezogener Daten […]" definiert, womit klar wird, dass auch dem Übermittlungsbegriff des BDSG der Offenlegungsgedanke innewohnt.

Ferner handelt es sich regelmäßig um eine Erhebung von Daten durch den hochladenden bzw. teilenden Nutzer. Das Erheben ist gem. § 3 Abs. 3 BDSG „[…] das Beschaffen von Daten über den Betroffenen […]" und enthält eine aktive sowie subjektive Komponente. Die aktive Komponente bedeutet, dass das bloße Heraussuchen aus bereits vorhandenen Daten keine Erhebung darstellt. Ferner muss die Erhebung subjektiv von einem Erhebungswillen getragen sein.[326] Beide Voraussetzungen treffen bei dem Hochladen sowie Teilen eines Beitrags auf der eigenen Pinnwand zu: Das Hochladen sowie Teilen geht über das bloße Heraussuchen von Daten heraus. Bei beiden Tätigkeiten liegt eine aktive, willentliche Komponente vor, durch die die Grenze zur Erhebung von Daten überschritten wird.

Bei dem Hochladen und Teilen handelt es sich somit um eine Verarbeitung i. S. d. Art. 2 lit. b DSRL bzw. Art. 4 Nr. 2 DSGVO in Form der Erhebung sowie in Form der Weitergabe und Verbreitung. In der Terminologie des BDSG mit der Trennung der Verarbeitungsschritte handelt es sich um eine Erhebung i. S. d. § 3 Abs. 3 BDSG sowie um eine Verarbeitung in Form der Übermittlung i. S. d. § 3 Abs. 4 S. 2 Nr. 3 BDSG.

---

325 Vgl. *Dudenredaktion,* Duden. Deutsches Universalwörterbuch, Beiträge zu „Weitergabe" und „Verbreitung".

326 Vgl. hierzu ausführlich *Dammann*, in: Simitis, BDSG, § 3, Rn. 102 ff.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

2. Zulässigkeit des Hochladens bzw. Teilens von Informationen Anderer durch Erlaubnistatbestände

a) Zulässigkeit nach dem BDSG

aa) Abgrenzung zwischen § 28 und § 29 BDSG

i) Übermittlung als Zweck der Verarbeitung

Im BDSG kommen die §§ 28, 29 BDSG als Erlaubnisnormen in Betracht. § 28 BDSG kommt zur Anwendung, wenn der Umgang mit personenbezogenen Daten i. S. d. § 28 Abs. 1 S. 1 BDSG „als Mittel für die Erfüllung eigener Geschäftszwecke" erfolgt, bei § 29 BDSG muss der Umgang mit personenbezogenen Daten gem. § 29 Abs. 1 S. 1 BDSG geschäftsmäßig und „[…] zum Zweck der Übermittlung […]" erfolgen. [327] Abgrenzungsmerkmal ist also, ob als Verarbeitungszweck eigene Geschäftszwecke oder die Übermittlung im Vordergrund stehen. Für letzteres müsste die Übermittlung selbst Zweck der Verarbeitung sein.[328] Dies ist etwa bei Bewertungsportalen im Internet der Fall, auf denen Nutzer etwa Ärzte[329] oder Lehrer[330] bewerten können. Der Zweck beim Hochladen und Teilen eines Beitrags liegt eindeutig in der Übermittlung von Daten an Andere. Somit ist auch dieses Merkmal erfüllt und § 29 BDSG ist die richtige Erlaubnisnorm.[331]

Da es sich bei dem Hochladen und Teilen nicht nur um eine Erhebung, sondern insbesondere um eine Übermittlung handelt, kommt § 29 Abs. 2 BDSG als Zulässigkeitstatbestand in Betracht, und zwar entweder i. V. m. § 29 Abs. 1 S. 1 Nr. 2 BDSG oder § 29 Abs. 1 S. 1 Nr. 1 BDSG.

---

327 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 336, Rn. 24 – spickmich.de; *BGH,* Urt. v. 23.09.2014, Az. VI ZR 358/13, BGHZ 202, 242, 246 f., Rn. 14 ff. – Ärztebewertung II.

328 *BGH,* Urt. v. 23.09.2014, Az. VI ZR 358/13, BGHZ 202, 242, 246 f., Rn. 15 – Ärztebewertung II; *Buchner*, in: BeckOK DatenschutzR, BDSG, § 29, Rn. 2; *Ehmann*, in: Simitis, BDSG, § 29, Rn. 20; *Weichert*, in: DKWW, BDSG, § 29, Rn. 5.

329 Vgl. *BGH,* Urt. v. 23.09.2014, Az. VI ZR 358/13, BGHZ 202, 242 – Ärztebewertung II.

330 Vgl. *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328 – spickmich.de.

331 Ebenso *Kampert,* Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, S. 114; zweifelnd *Krügel/Pfeiffenbring/Pieper*, K&R 2014, 699, 701, Fn. 22.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ii) Geschäftsmäßigkeit des Hochladens und Teilens

Allerdings müsste das Hochladen und Teilen auch „geschäftsmäßig" i. S. d. § 29 Abs. 1 S. 1 BDSG sein. Ein geschäftsmäßiges Handeln ist dabei eine auf Wiederholung und gewisse Dauer ausgerichtete Tätigkeit.[332] § 29 Abs. 1 S. 1 BDSG fordert dabei ausdrücklich keine Gewerbsmäßigkeit, d. h. es kommt gerade nicht auf eine Gewinnerzielungsabsicht bzw. ein kommerzielles Handeln an.[333] Vielmehr fällt ein Handeln bereits bei Fortsetzungsabsicht darunter.[334]

Nach dieser weiten Definition könnte das Hochladen und Teilen von Beiträgen anderer Nutzer bereits unter § 29 Abs. 1 BDSG fallen. Denn mit Ausnahme von Nutzern, die nur einmalig oder jedenfalls sehr selten etwas hochladen oder die Beiträge anderer Nutzer auf ihrem eigenen Profil teilen, ist eine Vielzahl von Nutzern mit einer gewissen Regelmäßigkeit in sozialen Netzwerken aktiv.

Gleichwohl ist dem Begriff der Geschäftsmäßigkeit eine gewisse kommerzielle Ausrichtung immanent, wie die nicht abschließend aufgezählten Handlungen in § 29 Abs. 1 S. 1 BDSG („Werbung, […] Tätigkeit von Auskunfteien oder […] Adresshandel") verdeutlichen.[335] Teilweise wird daher eine kommerzielle Tätigkeit für die Erfüllung der Geschäftsmäßigkeit gefordert.[336] Begründet wird dies damit, dass die Geschäftsmäßigkeit als Abgrenzung zur rein[337] privaten Datenverarbeitung zu sehen sei. Dies kann jedoch nicht überzeugen, da die Schwelle von dem privaten, gem. § 1 Abs. 2 Nr. 3 BDSG nicht dem sachlichen Anwendungsbereich des BDSG unterfallenden, Datenumgang zu dem datenschutzrechtlich relevanten Datenumgang sehr niedrig ist.[338] Allein mit der Abgrenzung zu privaten Tätigkeiten kann diese Auslegung daher nicht begründet werden, da dann im

---

332 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 336, Rn. 24 – spickmich.de; *Kramer*, in: Auernhammer, BDSG, § 29, Rn. 13; *Weichert*, in: DKWW, BDSG, § 29, Rn. 3; *Ehmann*, in: Simitis, BDSG, § 29, Rn. 60; *Taeger*, in: Taeger/Gabel, BDSG, § 29, Rn. 16.

333 *Kramer*, in: Auernhammer, BDSG, § 29, Rn. 13; *Weichert*, in: DKWW, BDSG, § 29, Rn. 3; *Ehmann*, in: Simitis, BDSG, § 29, Rn. 61.

334 *Weichert*, in: DKWW, BDSG, § 29, Rn. 3; *Ehmann*, in: Simitis, BDSG, § 29, Rn. 60.

335 *Taeger*, in: Taeger/Gabel, BDSG, § 29, Rn. 15.

336 *Schaffland/Wiltfang,* BDSG, § 29, Rn. 4.

337 Vgl. etwa *EuGH,* Urt. v. 06.11.2003, Rs. C-101/01, ECLI:EU:C:2003:596, Rn. 46 f. – Lindqvist; *EuGH,* Urt. v. 11.12.2014, Rs. C-212/13, ECLI:EU:C:2014:2428, Rn. 29 – Ryneš.

338 Vgl. Kap. 3 Pkt. A.I, S. 93.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Umkehrschluss jede den rein privaten Datenumgang überschreitende Tätigkeit einen kommerziellen Bezug aufweisen müsste, um auf die Erlaubnisnormen der §§ 28 f. BDSG[339] zurückgreifen zu können. Überdies zeigt der Wortlaut des § 29 Abs. 1 S. 1 BDSG („insbesondere"), dass es sich um eine nicht abschließende Aufzählung handelt. Eine Beschränkung auf kommerzielle Tätigkeiten ist grammatikalisch daher keinesfalls zwingend.

Auch wenn demnach eine Beschränkung des Anwendungsbereichs des § 29 BDSG auf rein kommerzielle Tätigkeiten abzulehnen ist, ist dennoch zu überlegen, ob durch das Hochladen und Teilen von Beiträgen anderer Nutzer die Schwelle zur Geschäftsmäßigkeit bereits überschritten ist. Dafür spricht in Abgrenzung zu § 28 BDSG, dass dort von einem „Geschäftszweck" die Rede ist und die Norm damit, anders als § 29 BDSG, explizit auf eine *Geschäfts*tätigkeit Bezug nimmt. Dafür spricht auch § 28 Abs. 1 S. 1 Nr. 1 BDSG, der, anders als § 29 BDSG, von einer Geschäftsbeziehung zwischen der verantwortlichen Stelle und dem Betroffenen ausgeht.[340] § 28 BDSG setzt demnach eine geschäftliche, berufliche oder gewerbliche Tätigkeit voraus.[341] Eine solche explizite Anforderung setzt § 29 BDSG gerade nicht. Demnach ist davon auszugehen, dass ein geschäftsmäßiges Handeln vorliegt, wenn ein Nutzer mit einer gewissen Regelmäßigkeit Beiträge anderer Nutzer auf seinem eigenen Profil teilt.[342] Dies ist bei vielen Nutzern ein durchaus übliches Vorgehen.

iii) Fehlen der Geschäftsmäßigkeit

Fraglich ist jedoch, welche Erlaubnisnorm zur Anwendung kommt, wenn ein Nutzer nur einmalig oder sehr selten Informationen hochlädt oder teilt. Wie gezeigt sind auch diese Tätigkeiten vom sachlichen Anwendungsbereich umfasst und unterfallen grundsätzlich nicht der Privilegierung des § 1 Abs. 2 Nr. 3 a. E. BDSG für ausschließlich persönliche oder familiären Tätigkeiten.

339 Vgl. sogleich Kap. 3 Pkt. A.III.2.a.aa.iii, S. 115.
340 *Taeger*, in: Taeger/Gabel, BDSG, § 28, Rn. 33.
341 *Simitis*, in: Simitis, BDSG, § 28, Rn. 22.
342 A. A. *Piltz,* Soziale Netzwerke im Internet, Pkt. 4.2.5.2.2, S. 110 f., der für die Erfüllung der Geschäftsmäßigkeit in § 29 Abs. 1 BDSG ein Interesse an den Daten und den darin enthaltenen Informationen selbst fordert.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

(1) Kein Rückgriff auf § 28 BDSG bei Fehlen der Geschäftsmäßigkeit

Ein Rückgriff auf § 28 BDSG kommt in diesen Fällen nicht in Betracht. Wie dargestellt erfolgt die Abgrenzung zwischen § 28 und § 29 BDSG anhand des verfolgten Zwecks.[343] Die Übermittlung i. S. d. § 28 Abs. 1 BDSG müsste nämlich „als Mittel für die Erfüllung eigener Geschäftszwecke" erfolgen; wie gezeigt erfolgt das Hochladen von Informationen bzw. Teilen von Beiträgen anderer Nutzer aber gerade zum Zweck der Übermittlung.[344] Für Nutzer, die nur gelegentlich Informationen hochladen bzw. Beiträge anderer Nutzer teilen, trifft dies jedenfalls nicht zu. Auch die Zulässigkeit der Übermittlung gem. § 28 Abs. 2 BDSG „für einen anderen Zweck" ist ausgeschlossen, da die Übermittlung zu einem anderen Zweck nur dann zulässig ist, wenn die vorhergehende Datenverarbeitung zur Erfüllung eigener Geschäftszwecke i. S. d. § 28 Abs. 1 BDSG zulässig ist.[345] Dies wird in Abgrenzung zu § 29 BDSG, der gerade den Datenumgang zum Zweck der Übermittlung regelt, klar. Eine Übermittlung auf Grundlage von § 28 BDSG scheidet demnach aus.

(2) Anwendbarkeit des § 29 BDSG bei Fehlen der Geschäftsmäßigkeit

In Fällen, in denen ein Nutzer einmalig einen Beitrag hochlädt oder teilt, fehlt die von § 29 BDSG geforderte Geschäftsmäßigkeit. In diesen Fällen muss jedoch in einem Erst-Recht-Schluss ebenfalls § 29 BDSG Anwendung finden: Wenn bereits das geschäftsmäßige Übermitteln i. S. d. § 29 BDSG erlaubt ist, muss dies erst recht für das einmalige Übermitteln von personenbezogenen Daten gelten. Andernfalls wäre für das einmalige

343 Vgl. Kap. 3 Pkt. A.III.2.a.aa, S. 113.

344 Vgl. Kap. 3 Pkt. A.III.2.a.aa, S. 113; ferner wäre eine Anwendbarkeit des § 28 Abs. 1 BDSG auf den Umgang mit personenbezogenen Daten im privaten Bereich bereits aufgrund der Systematik des § 28 Abs. 1 BDSG zumindest fraglich, da die Systematik des § 28 Abs. 1 BDSG das Vorliegen einer tatsächlichen Geschäftstätigkeit impliziert, wie der Wortlaut des § 28 Abs. 1 S. 1 BDSG und insbesondere des § 28 Abs. 1 S. 1 Nr. 1 BDSG zeigt, der ein Schuldverhältnis zwischen verantwortlicher Stelle und Betroffenem voraussetzt, vgl. *Taeger*, in: Taeger/Gabel, BDSG, § 28, Rn. 33; ähnlich *Wedde*, in: DKWW, BDSG, § 28, Rn. 11. Daher wird argumentiert, dass die verfolgten Zwecke geschäftlicher, beruflicher oder gewerblicher Natur sein müssen, *Simitis*, in: Simitis, BDSG, § 28, Rn. 22.

345 *Kramer*, in Auernhammer, BDSG, § 28, Rn. 78; *Wedde*, in: DKWW, BDSG, § 28, Rn. 69; *Taeger*, in: Taeger/Gabel, BDSG, § 28, Rn. 114.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Hochladen und Teilen keine Erlaubnisnorm einschlägig, für den Nutzer, der in einer Vielzahl von Fällen Beiträge anderer Nutzer teilt, jedoch schon. Damit wäre aufgrund des Verbots mit Erlaubnisvorbehalt das einmalige Hochladen und Teilen eines Nutzerbeitrages von vornherein verboten. § 29 BDSG ist dahingehend teleologisch auszuweiten, dass auch das einmalige Hochladen und Teilen eines Beitrages unter die Norm fällt.

bb) Erlaubnistatbestände in § 29 BDSG

i) Allgemein zugängliche Beiträge, § 29 Abs. 1 S. 1 Nr. 2 BDSG

§ 29 Abs. 1 S. 1 Nr. 2 BDSG erlaubt „[d]as geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung […], wenn […] die Daten aus allgemein zugänglichen Quellen entnommen werden können […], es sei denn, dass das schutzwürdige Interesse des Betroffenen […] offensichtlich überwiegt." Die Norm kommt in Betracht, wenn der geteilte Beitrag oder die hochgeladene Information öffentlich zugänglich ist. In zahlreichen sozialen Netzwerken haben die Nutzer die Möglichkeit, ihre Beiträge entweder für alle Internetnutzer zugänglich zu machen, oder aber nur einem bestimmten Personenkreis. Sofern der Nutzer, dessen Beitrag geteilt wird, diesen Beitrag also für alle Internetnutzer zugänglich gemacht hat, handelt es sich um eine allgemein zugängliche Quelle i. S. d. Norm.[346] In diesen Fällen ist die Erhebung zum Zwecke des Teilens zulässig, es sei denn, dass schutzwürdige Interessen des Betroffenen offensichtlich überwiegen. Dasselbe gilt, wenn ein Nutzer einen neuen Post mit bereits öffentlich zugänglichen Informationen verfasst. Dies gilt jedoch nur soweit die hochgeladenen personenbezogenen Daten nicht mit über das bereits öffentlich zugängliche Datum hinausgehenden Daten angereichert werden. Es müsste also genau die Information öffentlich zugänglich sein, die nun in einem Beitrag hochgeladen wird.

Die Schwelle der Zulässigkeit des Umgangs mit personenbezogenen Daten liegt bei § 29 Abs. 1 S. 1 Nr. 2 BDSG deutlich niedriger als bei § 29 Abs. 1 S. 1 Nr. 1 BDSG, bei dem bereits das Vorhandensein eines schutzwürdigen Interesses des Betroffenen ausreicht, um die Zulässigkeit zu verneinen. Die Formulierung in § 29 Abs. 1 S. 1 Nr. 2 BDSG „[…] es sei denn,

346 So auch *Kramer*, in: Auernhammer, BDSG, § 29, Rn. 32.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

dass […]" zeigt, dass eine Vermutung für das Überwiegen des Übermittlungsinteresses besteht.[347] Dabei spricht schon die Tatsache, dass der Betroffene die Daten seinerseits öffentlich zugänglich gemacht, hat gegen ein offensichtliches Überwiegen.[348] Ein offensichtliches Überwiegen der Betroffeneninteressen könnte bei besonderer Sensibilität der Daten vorliegen,[349] oder bei Minderjährigkeit des Betroffenen. Allgemein ergibt sich die Zulässigkeit des Erhebens, Speicherns, Veränderns oder Nutzens von Beiträgen, die vom Betroffenen selbst für jedermann zugänglich ins Netz gestellt wurden, jedoch aus § 29 Abs. 1 S. 1 Nr. 2 BDSG.

Probleme bereiten indes Konstellationen, in denen das Teilen nicht in einem bloßen zwei-Personen-Verhältnis vonstattengeht, sondern ein Beitrag vielfach und losgelöst vom originären Ersteller weiterverbreitet wird. Aus datenschutzrechtlicher Sicht ist dies freilich nur relevant, sofern der Inhalt des Beitrags selbst personenbezogene Daten enthält. Denn üblicherweise wird nur der Nutzername desjenigen, von dessen Profil der Beitrag „geteilt wird", automatisch genannt. Es besteht hingegen keine Verbreitung aller Nutzernamen, die zuvor diesen Beitrag ihrerseits geteilt haben. Dem Wortlaut nach wäre auch solch eine Kette an Verbreitungen gem. § 29 Abs. 1 S. 1 Nr. 2 BDSG möglich, solange die Daten zulässigerweise veröffentlicht werden durften. Allerdings könnte dieser Auslegung des § 29 Abs. 1 S. 1 Nr. 2 BDSG der Direkterhebungsgrundsatz, der in § 4 Abs. 2 S. 1 BDSG niedergelegt ist, entgegenstehen. Gem. § 4 Abs. 2 BDSG, der gleichermaßen für den Datenumgang durch öffentliche wie nicht-öffentliche Stellen gilt, sind Daten stets beim Betroffenen zu erheben. Ausnahmen sind nur unter den in § 4 Abs. 2 S. 2 BDSG gesetzten Bedingungen möglich. Dazu müsste gem. § 4 Abs. 2 S 2 Nr. 1 Alt. 1 BDSG eine Rechtsvorschrift dies ausdrücklich[350] vorsehen, was bei § 29 Abs. 1 S. 1 Nr. 2 BDSG nicht der Fall ist. Hierzu wird jedoch vertreten, dass § 29 Abs. 1 S. 1 Nr. 2 BDSG lex specialis zu § 4 Abs. 2 BDSG sei.[351] Dies überzeugt, da § 29 Abs. 1 S. 1 Nr. 2 BDSG Erleichterungen zum Umgang mit personenbezogenen Daten für die verantwortliche Stelle deswegen legitimiert, weil bereits (zulässigerweise) veröffentlichte Daten weniger schutzwürdig sind.

347 *Kramer,* in: Auernhammer, BDSG, § 29, Rn. 36.
348 *Weichert*, in: DKWW, BDSG, § 29, Rn. 46; *LG Berlin,* Urt. v. 25.10.2007, Az. 27 O 602/07, MMR 2008, 353.
349 *Weichert*, in: DKWW, BDSG, § 29, Rn. 47.
350 *Weichert*, in: DKWW, BDSG, § 4, Rn. 7.
351 *Ehmann*, in: Simitis, BDSG, Rn. 146.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Würde der Direkterhebungsgrundsatz auch hier gelten, wäre die Privilegierung weitgehend ausgehebelt.[352] Gleichwohl wird bei einer Kettenverbreitung von personenbezogenen Daten ein besonderes Augenmerk darauf zu legen sein, ob nicht schon durch die Kettenverbreitung das Betroffeneninteresse gegen den Datenumgang offensichtlich überwiegt i. S. d. § 29 Abs. 1 S. 1 Nr. 2 BDSG. Dies könnte dann der Fall sein, wenn die Daten ursprünglich nur mit einem bestimmten Personenkreis geteilt wurden und die Daten von einem anderen Nutzer auf einer anderen Legitimationsgrundlage basierend im Internet veröffentlicht werden. Solche Daten sind zwar zulässigerweise allgemein zugänglich, ihre Weiterverbreitung auf Grundlage von § 29 Abs. 1 S. 1 Nr. 2 i. V. m. § 29 Abs. 2 BDSG wird jedoch ganz besonders am möglicherweise entgegenstehenden Betroffeneninteresse zu messen sein.

ii) Nicht allgemein zugängliche Beiträge, § 29 Abs. 1 S. 1 Nr. 1 BDSG

Sofern der Beitrag, der geteilt werden soll, nicht aus allgemein zugänglichen Quellen entnommen werden kann i. S. d. § 29 Abs. 1 S. 1 Nr. 2 BDSG, ist die richtige Zulässigkeitsnorm § 29 Abs. 1 S. 1 Nr. 1 BDSG. Anders als bei § 29 Abs. 1 S. 1 Nr. 2 BDSG, bei der eine Vermutung für das Überwiegen der Interessen der verantwortlichen Stelle besteht, muss die verantwortliche Stelle bei § 29 Abs. 1 S. 1 Nr. 1 BDSG eine Interessenabwägung zwischen den Interessen des Betroffenen und den Interessen der verantwortlichen Stelle – also des Hochladenden bzw. Teilenden – vornehmen.[353] Auf Seite des Hochladenden bzw. Teilenden können hier etwa politische Interessen, kulturelle oder sonstige ideelle Beweggründe stehen.[354] Im Nutzer-Nutzer-Verhältnis muss jedoch regelmäßig von einem Überwiegen der Betroffeneninteressen ausgegangen werden, soweit personenbezogene Daten über ihn ohne sein Wissen hochgeladen oder geteilt werden sollen. Im Einzelfall ist es zwar denkbar, dass von diesem Grundsatz abgewichen werden kann. In der Regel wird jedoch auf seine Einwilligung zurückzugreifen sein.[355]

---

352 *Ehmann*, in: Simitis, BDSG, Rn. 146.
353 *Kramer*, in: Auernhammer, BDSG, § 29, Rn. 22 ff.
354 *Taeger*, in: Taeger/Gabel, BDSG, § 29, Rn. 28; *Weichert*, in: DKWW, BDSG, § 29, Rn. 14.
355 Vgl. Kap. 3 Pkt. A.III.3.a, S. 131, zu den Voraussetzungen der Einwilligung im Nutzer-Nutzer-Verhältnis nach dem BDSG bzw. der DSRL.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

iii) Zulässigkeit der Übermittlung i. S. d. § 29 Abs. 2 BDSG

Soweit es sich um Daten aus allgemein zugänglichen Quellen handelt, ist das Erheben, Speichern, Verändern oder Nutzen i. S. d. § 29 Abs. 1 Nr. 2 BDSG grundsätzlich zulässig. Allerdings müssten für die Zulässigkeit der Übermittlung auch noch die zusätzlichen Voraussetzungen des § 29 Abs. 2 BDSG vorliegen. Dazu müsste der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse glaubhaft dargelegt haben i. S. d. § 29 Abs. 2 S. 1 Nr. 1 und es dürfte kein Grund zu der Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Problematisch ist daran, dass gem. § 29 Abs. 2 S. 1 Nr. 1 BDSG der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an der Übermittlung glaubhaft dargelegt *haben* muss, das bedeutet, dass die Norm in zeitlicher Hinsicht eine der Übermittlung vorgeschaltete Darlegung berechtigter Interessen verlangt. Dies ist jedoch bei Übermittlungen im Internet an einen unbestimmten Personenkreis nicht gegeben. Bei strenger Auslegung der Norm gilt dies selbst dann, wenn personenbezogene Daten von im öffentlichen Leben stehenden Personen – wie etwa Politikern – in Frage stehen und zwar auch dann, wenn es sich hierbei nur etwa um den Namen des Politikers, etwa der Bundeskanzlerin, handelt.

(1) Historischer Ursprung der Norm

Fraglich ist, ob die Norm auch anders ausgelegt werden könnte. In systematischer Hinsicht lässt sich feststellen, dass § 28 Abs. 1 S. 1 Nr. 2 BDSG die Übermittlung allgemein zugänglicher Quellen zu eigenen Geschäftszwecken erlaubt, es sei denn, dass schutzwürdige Betroffeneninteressen offensichtlich überwiegen. Das Element der glaubhaften Darlegung von Drittinteressen ist also nicht gegeben. Hierbei lässt sich auf die Unterscheidung der Erlaubnistatbestände verweisen. § 28 BDSG erlaubt den Umgang mit personenbezogenen Daten zu Zwecken eigener Geschäftsinteressen, während bei § 29 BDSG der Umgang mit personenbezogenen Daten zum Zweck der Übermittlung im Vordergrund steht. Die unterschiedlichen Anforderungen könnten sich daraus erklären, dass § 29 BDSG in historischer

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Sicht den Fall einer geschäftsmäßigen Übermittlung an konkrete Empfänger im Blick hatte. Die Norm entspringt letztlich dem BDSG 1977.[356] Der Wortlaut wurde folglich weit vor der flächendeckenden Nutzung des Internets verfasst. So verweist auch der *BGH* auf den technischen Wandel, der seit Einführung der Norm stattgefunden hat.[357] Zwar könnte man gegen dieses Argument einwenden, dass der Gesetzgeber seit 1990 die Norm in vier Änderungsgesetzgebungen modifiziert hat,[358] ohne den fraglichen Passus zu verändern. Gleichwohl lässt sich aus dem Untätigbleiben des Gesetzgebers nicht automatisch auf dessen Wille zu dem Ergebnis, dass Übermittlungen von personenbezogenen Daten im Internet per se unzulässig sind, schließen.

(2) Verfassungskonforme Auslegung durch den BGH

Der *BGH* hat hierzu ausgeführt, dass § 29 Abs. 2 S. 1 Nr. 1 BDSG dahingehend auszulegen sei, dass sich die Zulässigkeit aufgrund einer Gesamtabwägung des Persönlichkeitsrechts des Betroffenen einerseits und des Informationsinteresses der Dritten andererseits ergeben solle.[359]

Zusätzlich zu dem historischen Argument führt der *BGH* an, dass die Norm gegen die Kommunikationsfreiheit aus Art. 5 Abs. 1 GG verstoße und daher verfassungskonform auszulegen sei.[360] § 29 Abs. 2 BDSG beschränke die Meinungs- und Informationsfreiheit aus Äußerungen ohne datenmäßig geschützten Inhalt.[361] Die Beschränkung der Meinungs- und Informationsfreiheit sei jedoch nur rechtmäßig, wenn sie verhältnismäßig sei. Die Zulässigkeit der Übermittlung der personenbezogenen Daten an Dritte

356 § 29 Abs. 2 Nr. 1 lit. a BDSG 1990 (Gesetz v. 20.12.1990, BGBl. I 1990, 2954) basiert auf § 32 Abs. 2 BDSG 1977 (Gesetz v. 20.01.1977, BGBl. I 1977, 201), vgl. BT-Drucks. 11/4306, S. 48.

357 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 343 f., Rn. 42 – spickmich.de.

358 Gesetz v. 18.05.2001, BGBl. I 2001, 904; Gesetz v. 29. 7. 2009, BGBl. I 2009, 2254; Gesetz v. 29. 7. 2009, BGBl. I 2009, 2355; Gesetz v. 14. 8. 2009, BGBl. I 2009, 2814.

359 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 343 f., Rn. 42 f.; *BGH,* Urt. v. 23.09.2014, Az. VI ZR 358/13, BGHZ 202, 242, 257 f., Rn. 45 – Ärztebewertung II; ebenso: *Iraschko-Luscher/Kiekenbeck*, ZD 2012, 261, 262; *Kramer*, in: Auernhammer, BDSG, § 29, Rn. 49.

360 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 343 f., Rn. 42 – spickmich.de.

361 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 343 f., Rn. 42 – spickmich.de.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

sei daher anhand einer Gesamtabwägung zwischen dem Persönlichkeitsrecht des Betroffenen und dem Informationsinteresse desjenigen, dem die Daten übermittelt wurden, zu beurteilen.[362] Die Argumentation des *BGH* überzeugt. Ein generelles gesetzliches Übermittlungsverbot von personenbezogenen Daten im Internet würde einen erheblichen Eingriff in die Meinungs- und Informationsfreiheit der Internetnutzer bedeuten. Demgegenüber erfahren die personenbezogenen Daten der Betroffenen bereits den Schutz der kumulativen Anforderungen aus § 29 Abs. 1 und Abs. 2 BDSG. Für eine Zulässigkeit der Übermittlung im Internet ist die Abwägung mit den Betroffeneninteressen in zweifacher Sicht erforderlich: Erstens bei der Erhebung und Nutzung i. S. d. § 29 Abs. 1 BDSG und zweitens bei der Übermittlung i. S. d. § 29 Abs. 2 S. 1 BDSG. Da es sich bei der Übermittlung von personenbezogenen Daten in sozialen Netzwerken um Daten aus allgemein zugänglichen Quellen handelt, ist durch diese Auslegung auch keine unerwünschte und unverhältnismäßige Einschränkung des Schutzes personenbezogener Daten zu befürchten.

(3) Vereinbarkeit des § 29 Abs. 2 S. 1 Nr. 1 BDSG mit Art. 7 lit. f DSRL

Zudem ist fraglich, ob eine strenge Auslegung des § 29 Abs. 2 S. 1 Nr. 1 BDSG mit Augenmerk auf die zeitlich vorgeschaltete Darlegungspflicht des Datenempfängers mit Art. 7 DSRL vereinbar wäre. Der *EuGH* hat bereits festgestellt, dass die DSRL vollharmonisierende Wirkung hat und die Mitglieder keine neuen Grundsätze der Zulässigkeit der Datenverarbeitung aufstellen dürfen sowie die Tragweite dieser Grundsätze der Zulässigkeit nicht verändert werden darf.[363] § 29 Abs. 2 BDSG stellt zwar keinen neuen Grundsatz für die Zulässigkeit der Übermittlung auf, er könnte aber die Tragweite des Art. 7 lit. f DSRL verändern. Denn Art. 7 lit. f DSRL sieht

362 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 343 f., Rn. 42 – spickmich.de; allerdings ist fraglich, ob den *BGH* nicht bei Überzeugung von der Verfassungswidrigkeit des § 29 Abs. 2 BDSG eine Vorlagepflicht an das *BVerfG* getroffen hätte; s. hierzu etwa *BVerfG,* Nichtannahmebeschl. v. 16.06.2009, 1 BvR 2269/07, BAuR 2009, 1424.

363 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 30, 32 – ASNEF und FECEMD m. Anm. *Kühling*, EuZW 2012, 281; ausführlich *Raab,* Die Harmonisierung des einfachgesetzlichen Datenschutzes, S. 32 ff.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

zwar ebenfalls das Erfordernis einer Interessenabwägung zwischen den Interessen des Verantwortlichen, der Betroffenen und der Dritten, denen die Daten übermittelt werden, vor. Ihm ist aber nicht dieselbe zeitliche Komponente zu entnehmen, die § 29 Abs. 2 S. 1 Nr. 2 BDSG vorsieht. Wie gezeigt würde eine strenge Auslegung des Wortlauts des § 29 Abs. 2 S. 1 Nr. 1 BDSG aber die Tragweite des Art. 7 lit. f DSRL dahingehend verändern, dass Übermittlungen im Internet faktisch nicht möglich wären und ginge damit über den Art. 7 lit. f DSRL hinaus. Die vom *BGH* vorgenommene Auslegung ist daher auch unionsrechtlich geboten.

(4) Zwischenergebnis

§ 29 Abs. 1 Nr. 1, Nr. 2 i. V. m. § 29 Abs. 2 S. 1 BDSG kann als Zulässigkeitstatbestand für das Hochladen und Teilen von Beiträgen anderer Nutzer herangezogen werden, allerdings nur im Zuge verfassungs- wie richtlinienkonformer Auslegung.

iv) Zusammenfassung

Das BDSG hält nur für den Umgang mit allgemeinzugänglichen personenbezogenen Daten einen gesetzlichen Zulässigkeitstatbestand für das Hochladen und Teilen von Beiträgen anderer Nutzer bereit.

b) Zulässigkeit nach der DSRL

Die Zulässigkeitstatbestände in der DSRL sind weit weniger ausdifferenziert als im BDSG. Sie finden sich in Art. 7 DSRL. In Betracht kommt vorliegend Art. 7 lit. f DSRL, nach dem die Verarbeitung von personenbezogenen Daten zulässig ist, wenn sie zur Verwirklichung des berechtigten Interesses, das von der verantwortlichen Stelle oder einem Dritten, dem die Daten übermittelt werden, erforderlich ist, sofern nicht die Interessen, Grundfreiheiten oder Grundrechte des Betroffenen überwiegen. Art. 7 lit. f DSRL setzt also kumulativ drei Voraussetzungen: Die Verarbeitung muss zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder des

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Empfängers (1) erforderlich (2) sein und dieses Interesse muss die Betroffeneninteressen überwiegen (3).[364]

Auf Seiten der Betroffenen stehen die grundrechtlich geschützten Positionen aus Art. 7, 8 GRCh, auf Seiten des den Beitrag teilenden Nutzers etwa die Meinungsfreiheit aus Art. 11 Abs. 1 GRCh sowie auf Seiten des Empfängers die Informationsfreiheit. Der *EuGH* hat für das Überwiegen der Betroffeneninteressen aus Art. 7, 8 GRCh[365] – nicht ganz unproblematisch – eine Vermutungswirkung aufgestellt.[366] Allerdings handelte es sich hierbei um Persönlichkeitsrechtsgefährdungen durch marktmächtige Akteure wie Google[367], wohingegen sich in der fraglichen Situation zwei Nutzer gegenüberstehen.

Auffällig ist zudem, dass Art. 7 lit. f DSRL weiter gefasst ist als §§ 28, 29 BDSG. Denn Art. 7 lit. f DSRL stellt nicht die in § 28 und § 29 BDSG zusätzlichen Anforderungen – etwa die Erfüllung zu Geschäftszwecken in § 28 Abs. 1 BDSG oder die Darlegung eines Empfängerinteresses in § 29 Abs. 2 BDSG – auf. Anders als das BDSG sieht die DSRL damit einen Zulässigkeitstatbestand vor, unter den sich, unter bestimmten Voraussetzungen, auch das Hochladen und Teilen von Beiträgen anderer Nutzer fassen ließe. Speziell zu Art. 7 lit. f DSRL hat der *EuGH* indes wiederholt entschieden, dass die nationalen Umsetzungsgesetze keine zusätzlichen Anforderungen zu denen des Art. 7 DSRL für die Zulässigkeit des Umgangs mit personenbezogenen Daten aufstellen dürfen.[368] Gleichzeitig sieht Art. 5 DSRL jedoch die Möglichkeit vor, dass die Mitgliedstaaten die Zulässigkeitstatbestände des Art. 7 DSRL näher konkretisieren dürfen. Eine Präzisierung hinsichtlich der in Frage kommenden Interessen, wie es etwa § 29

---

364 *EuGH,* Urt. v. 04.05.2017, Rs. C-13/16, ECLI:EU:C:2017:336, Rn. 28 – Rīgas.

365 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 38, 40 – ASNEF und FECEMD; *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 74 – Google und Google Spain.

366 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 81, 97; kritisch hierzu *Schneider*, in: BeckOK DatenschutzR, Syst. B, Völker- und unionsrechtliche Grundlagen, Rn. 94; *Hoeren*, ZD 2014, 325; zweifelnd *Kühling*, EuZW 2014, 527, 529 f.; vgl. auch *EuGH*, Urt. v. 06.10.2015, C-362/14, ECLI:EU:C:2015:650 – Schrems, in dem der *Gerichtshof* die kollidierenden Interessenpositionen kaum berücksichtigt; hierzu kritisch *Kühling/Heberlein*, NVwZ 2016, 7, 9, 12.

367 Vgl. etwa *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317 – Google und Google Spain.

368 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 35 ff;49 – ASNEF und FECEMD; *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779, Rn. 59 ff. – Breyer.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Abs. 1 BDSG für die Übermittlung zu Werbezwecken vorsieht, ist daher grundsätzlich von Art. 5 DSRL gedeckt.

c) Zulässigkeit nach der DSGVO

In der DSGVO gibt es, ähnlich wie in der DSRL, keine in dem BDSG ähnlich differenzierter Weise ausgestalteten Zulässigkeitstatbestände. In Betracht kommt vorliegend Art. 6 Abs. 1 S. 1 lit. f DSGVO. Danach ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten des Betroffenen überwiegen. Die Verarbeitung schließt gem. Art. 4 Nr. 2 DSGVO die „Offenlegung durch Übermittlung" ein und ist damit mit der Übermittlung i. S. d. BDSG gleichzusetzen.[369]

aa) Art. 6 Abs. 1 S. 1 lit. f DSGVO als umfassende Erlaubnisnorm

Art. 6 Abs. 1 S. 1 lit. f DSGVO ist beinahe wortlautgleich mit Art. 7 lit. f DSRL. Anders als Art. 7 lit. f DSRL wird Art. 6 Abs. 1 S. 1 lit. f DSGVO jedoch nicht in nationales Recht umgesetzt und dadurch näher präzisiert. Im Kommissionsentwurf zu Art. 6 DSGVO war in Abs. 5 daher vorgesehen, dass die Kommission die Vorschrift durch delegierte Rechtsakte näher regeln kann.[370] Aufgrund massiver Kritik an den zahlreichen delegierten Rechtsakten, die im Kommissionsentwurf vorgesehen waren,[371] wurden diese jedoch gestrichen. Dies hat den unerfreulichen Nachteil, dass nun neben der Einwilligung (Art. 6 Abs. 1 S. 1 lit. a DSGVO) eine unpräzise Vorschrift als Hauptlegitimationsgrundlage für Verarbeitungen durch nicht-öffentliche Stellen dienen wird.[372] Zwar bringt der offene Legitimationstatbestand des Art. 6 Abs. 1 S. 1 lit. f DSGVO mehr Flexibilität, jedoch führt er

369 Vgl. Kap. 3 Pkt. A.III.1, S. 111.

370 Art. 6 Abs. 5 des Kommissionsentwurfs der DSGVO, Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endg.

371 *Kühling/Martini*, EuZW 2016, 448, 449; *Schild/Tinnefeld*, DuD 2012, 312, 314, 316 f.; s. auch *Gola/Schulz*, RDV 2013, 1, 2 m. w. N.

372 Zurecht kritisch zu der Vorschrift *Roßnagel/Richter/Nebel*, ZD 2013, 103, 104; *Sydow/Kring*, ZD 2014, 271, 272.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

gleichermaßen für Betroffene wie für Verarbeiter zu Unsicherheiten: Die Interessenabwägung ist vom Verarbeiter selbst vorzunehmen,[373] was ihn in einen Interessenskonflikt führt.[374] Zudem sind der Mangel an klaren Legitimationstatbeständen und die resultierende Rechtsunsicherheit mit Blick auf das strenge Sanktionsregime der DSGVO für die Datenverarbeiter nicht unkritisch:[375] So bedroht Art. 84 Abs. 5 lit. a DSGVO Verstöße gegen Art. 6 DSGVO mit 20 Mio. Euro oder 4 % des weltweit erzielten Jahresumsatzes eines Unternehmens.[376] Auf Seiten des Betroffenen ist es freilich bedenklich, dass eine Abwägung ohne klare Maßstäbe von demjenigen getroffen wird, der ein Interesse an der Datenverarbeitung hat. Nur allzu leicht könnte die Norm wohlwollend im Sinne der Datenverarbeiter interpretiert werden und damit den Zweck des Verbots mit Erlaubnisvorbehalt konterkarieren. Denn statt einem Verbot mit klaren Erlaubnistatbeständen gibt es nunmehr ein Verbot mit einem möglicherweise sehr weitreichenden, unklaren Erlaubnistatbestand.

Aufgrund dieser Rechtsunsicherheit sah der Entwurf des Berichterstatters der DSGVO die Streichung des Art. 6 Abs. 1 lit. f DSGVO und die Ersetzung der Norm durch konkret geregelte Fälle vor.[377] So enthielt der Entwurf des Berichterstatters beispielsweise eine Vermutung für das Überwiegen der Meinungsfreiheit über die Betroffeneninteressen.[378] Diese Vermutung stünde nicht zuletzt entgegen der jüngsten *EuGH*-Rechtsprechung aus dem Fall *Google und Google Spain*, in dem der *Gerichtshof* jedenfalls für Suchmaschinen eine Vermutung für das Überwiegen der Betroffeneninteressen aufstellte.[379] Die Vorschläge fanden aber bereits keinen Eingang in den Parlamentsentwurf. Stattdessen sah der Parlamentsentwurf die Berücksichtigung der berechtigten Erwartungen des Betroffenen mit Blick auf deren Verhältnis zum Verantwortlichen vor.[380] Dieses Merkmal, das an das

373 *Frenzel*, in: Paal/Pauly, DSGVO, Art. 6, Rn. 27; *Ferretti*, CMLR 2014, 843, 858; für die Vorgängernorm des Art. 7 lit. f DSRL *GA Bobek,* Schlussanträge v. 26.01.2017, Rs. C-13/16, ECLI:EU:C:2017:43, Rn. 64 – Rīgas.

374 *Ferretti*, CMLR 2014, 843, 861.

375 Ebenso *Golla*, RDV 2017, 123, 125.

376 Vgl. Kap. 3 Pkt. D.II.2, S. 230.

377 *Albrecht*, CR 2016, 88, 92 mit Verweis auf COM(2012)0011 – C7 0025/2012 – 2012/0011(COD) v. 16.01.2013, S. 78 ff.

378 Vgl. Art. 6 Abs. 1b lit. a Var. 1 (Berichterstatter), COM(2012)0011 – C7 0025/2012 – 2012/0011(COD) v. 16.01.2013, S. 80.

379 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 81, 97 f. – Google und Google Spain.

380 Vgl. Art. 6 Abs. 1 lit. f des Parlamentsentwurfs der DSGVO, P7_TA(2014)0212.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

im US-amerikanischen Datenschutzrecht etablierte Merkmal der „reasonable expectation of privacy" erinnert,[381] birgt letztlich ebenso die Gefahr einer unklaren Auslegung und bietet demnach kaum einen Mehrwert zur Schaffung von Rechtssicherheit.[382] Letztlich ist der Entwurf des Berichterstatters Zeugnis davon, wie schwierig sich die allumfassende Regelung von Legitimationsgrundlagen gestaltet. Demgegenüber ist der klare Vorteil des Art. 6 Abs. 1 S. 1 lit. f DSGVO seine Flexibilität, um auf neue Situationen zu reagieren. Er hat damit tendenziell das Potential, auch bei stetigem technischem Fortschritt ein modernes Mittel zur Bemessung der Rechtmäßigkeit der Datenverarbeitung zu stellen.

Dennoch besteht gerade in der Anfangszeit der DSGVO die Gefahr, dass Datenverarbeiter sich zu Unrecht auf Art. 6 Abs. 1 S. 1 lit. f DSGVO berufen könnten, solange der Norm noch keine klaren Grenzen durch die Rechtsprechung und die Aufsichtsbehörden gezogen wurden. Dem könnte der europäische Datenschutzausschuss Abhilfe verschaffen, indem er Leitlinien zur Auslegung des Art. 6 Abs. 1 S. 1 lit. f DSGVO i. S. d. Art. 70 Abs. 1 S. 1 lit. e DSGVO entwirft.[383]

bb) Maßstab des Art. 6 Abs. 1 S. 1 lit. f DSGVO

Ungeachtet der genannten Problematik der Formulierung des Art. 6 Abs. 1 S. 1 lit. f DSGVO lassen sich für die Anwendbarkeit des Art. 6 Abs. 1 S. 1 lit. f DSGVO gewisse Maßstäbe aufstellen.

Diese ergeben sich zum Einen aus dem Wortlaut: Zunächst bedarf es eines *berechtigten Interesses* des Datenverarbeiters oder eines Dritten (dazu i.). Die Verarbeitung personenbezogener Daten muss zudem *erforderlich*[384] sein zur Interessenwahrung des Verarbeiters. Überdies dürfen Grundrechte, Grundfreiheiten oder *Interessen des Betroffenen* (dazu ii.) *nicht überwiegen* (dazu iii.).

---

381 Vgl. Kap. 4, Pkt. A.II.1, S. 243.

382 A. A. *Kampert,* Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, S. 228 f., der darin eine sinnvolle Eingrenzung der Abwägungsentscheidung sieht.

383 Ebenso *Heberlein*, in: Ehmann/Selmayr, DSGVO, Art. 6, Rn. 28.

384 Dabei muss der Begriff der Erforderlichkeit anhand der Ziele der DSGVO aus Art. 1 ausgelegt werden, so bereits für die DSRL *EuGH,* Urt. v. 16.12.2008, Rs. C-524/06, ECLI:EU:C:2008:724 – Huber; *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 30 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Ferner kann zur Auslegung auf die Erkenntnisse zu Art. 7 lit. f DSRL, an den Art. 6 Abs. 1 S. 1 lit. f DSGVO anknüpft, zurückgegriffen werden.

i) Berechtigtes Interesse des Datenverarbeiters oder eines Dritten

Berechtigtes Interesse kann jedes tatsächliche, wirtschaftliche oder ideelle Interesse sein.[385] Schon der Wortlaut des Art. 6 Abs. 1 S. 1 lit. f DSGVO, der begrifflich zwischen Grundrechten bzw. Grundfreiheiten und Interessen unterscheidet, spricht für diese Auslegung. Nicht notwendig ist demnach, dass sich das Interesse aus einem in der Charta verbürgten Recht ergibt.

Zurecht weisen kritische Stimmen darauf hin, dass dieses Interesse allzu leicht dahingehend verstanden werden könnte, dass es sich aus jeder rechtmäßigen Aktivität des Verarbeiters ergibt.[386] Dann hätten soziale Netzwerke wie Facebook, deren wirtschaftliche Grundlage aus der Verarbeitung personenbezogener Daten besteht, regelmäßig ein berechtigtes Interesse an der Verarbeitung.[387] Dieses Interesse ergibt sich allerdings bereits aus der unternehmerischen Freiheit (Art. 16 GRCh) der sozialen Netzwerke.

Im Nutzer-Nutzer-Verhältnis kommt regelmäßig das Interesse an freier Meinungsäußerung des Postenden in Betracht. Auf Seiten der Dritten, also anderer Internetnutzer, die die geteilten Nutzerbeiträge lesen, steht insbesondere die Informationsfreiheit im Vordergrund.

ii) Betroffeneninteressen

Auf Seiten der Betroffenen stehen zuvorderst ihr Recht auf den Schutz personenbezogener Daten bzw. Achtung des Privatlebens, wie es sich aus Art. 7, 8 GRCh ergibt. Allerdings können auch andere Betroffeneninteressen die berechtigen Interessen des Verarbeiters überwiegen, wie etwa die Abwehr wirtschaftlicher Nachteile.[388]

---

385 So *Buchner/Petri*, in: Kühling/Buchner, DSGVO, Art. 6, Rn. 146, die zurecht die Definition des berechtigten Interesses aus § 28 Abs. 1 BDSG heranziehen.
386 *Ferretti*, CMLR 2014, 843, 862.
387 *Ferretti*, CMLR 2014, 843, 864.
388 *Buchner/Petri*, in: Kühling/Buchner, DSGVO, Art. 6, Rn. 148.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

iii) Abwägung

Für die Abwägung selbst gibt die DSGVO zunächst in EG 47 bestimmte Hinweise. Danach sind bei der Interessenabwägung die „[…] vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen ruhen, zu berücksichtigen […]". Ferner soll in Betracht gezogen werden, ob der Betroffene vernünftigerweise vorhersehen konnte, dass eine Verarbeitung zu diesem Zweck stattfinden würde; daraus ergibt sich auch, dass die Betroffeneninteressen überwiegen können, wenn der Betroffene damit rechnen durfte, dass seine Daten zu diesem Zweck nicht verarbeitet würden, EG 47 S. 4 DSGVO. Als berechtigtes Interesse auf Seiten des Verarbeiters nennt EG 47 S. 7 DSGVO etwa die Direktwerbung.

Die Abwägung ist stets einzelfallbezogen zu treffen,[389] wobei freilich die unterschiedliche Eingriffsintensität für den Betroffenen je nach Fallgestaltung zu berücksichtigen ist.[390] So hat der *EuGH* zu Art. 7 lit. f DSRL ausgeführt, dass die Daten aus öffentlichen Quellen weniger schützenswert sind als nicht-öffentliche Daten.[391] Dass dies nicht vorbehaltslos gilt, zeigt die *Google und Google Spain*-Entscheidung, in der der *EuGH* auf die bedeutende Rolle der Suchmaschinen für die Informationsbeschaffung und der daraus resultierenden Macht der Suchmaschinenbetreiber und die entsprechende Bedrohung für die Persönlichkeitsrechte der Betroffenen hingewiesen hat.[392] Für den Fall von Suchmaschinen hat der *Gerichtshof* daher eine Vermutung für das Überwiegen der Betroffeneninteressen aufgestellt.[393]

Die generelle Unterscheidung von öffentlichen und nicht-öffentlichen Daten liegt indes auf der Hand, insbesondere, wenn der Betroffene die Da-

---

389 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 40 – ASNEF und FECEMD; *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779, Rn. 62 – Breyer; *EuGH,* Urt. v. 04.05.2017, Rs. C-13/16, ECLI:EU:C:2017:336, Rn. 31 – Rīgas.

390 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 44 – ASNEF und FECEMD.

391 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 44 f. – ASNEF und FECEMD; *EuGH,* Urt. v. 04.05.2017, Rs. C-13/16, ECLI:EU:C:2017:336, Rn. 31 – Rīgas.

392 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 36 ff., 80 f., 97 f. – Google und Google Spain.

393 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 81, 97 f. – Google und Google Spain; dazu kritisch *Schneider*, in: BeckOK DatenschutzR, Völker- und unionsrechtl. Grundlagen, Rn. 94.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ten selbst öffentlich gemacht hat und natürlich nur soweit die Daten tatsächlich öffentlich gemacht werden durften.[394] Jedenfalls im Nutzer-Nutzer-Verhältnis kann die Vermutung für das Überwiegen der Betroffeneninteressen nicht übertragen werden, da die Argumentation des *EuGH* sich gerade auf die bedeutende Rolle der Suchmaschinen für die Informationsbeschaffung und der daraus resultierenden enormen Macht der Suchmaschinenbetreiber stützte.[395] Diese Rolle nehmen private Nutzer in sozialen Netzwerken nicht ein. Die Gefahr der automatisierten Datenverarbeitung ergibt sich in diesem Verhältnis regelmäßig nicht.[396]

Daraus folgt, dass gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO das Hochladen von Informationen und das Teilen von Nutzerbeiträgen, die von den Nutzern selbst öffentlich gemacht wurden, üblicherweise erlaubt ist. Hier zeigt sich der Unterschied zur rechtlichen Bewertung nach dem BDSG, nach dem das Hochladen bzw. Teilen auch von öffentlichen Beiträgen aufgrund der hohen Anforderungen des § 29 Abs. 2 S. 1 Nr. 1 BDSG nur im Zuge einer verfassungs- wie richtlinienkonformen Auslegung möglich ist.[397]

Beim Hochladen von Informationen bzw. Teilen von Beiträgen, die explizit nicht öffentlich gemacht wurden, wird die Verarbeitung jedoch regelmäßig nicht zulässig sein.

3. Zulässigkeit der Verarbeitung von Informationen Anderer durch Einwilligung

Wie gezeigt steht nach dem Regime des BDSG derzeit in den meisten Fällen kein Zulässigkeitstatbestand für das Hochladen und Teilen der Informationen anderer Nutzer bereit. Soweit es sich um allgemein zugängliche Informationen handelt, ist die Übermittlung im Zuge verfassungs- wie richtlinienkonformer Auslegung möglich. Auch nach der DSGVO ist das Hochladen und Teilen nur teilweise zulässig; insbesondere bei nicht allgemein zugänglichen Informationen wird regelmäßig das Betroffeneninteresse

394 Vgl. dazu Kap. 3 Pkt. A.III.2.a.bb.i, S.117.

395 *EuGH,* Urt. v. 13.05.2014, Rs. C-131/12, ECLI:EU:C:2014:317, Rn. 36 ff., 80 f., 97 f. – Google und Google Spain.

396 Für die Unterscheidung zwischen automatisierter und konkreter Verarbeitung auch *GA Bobek,* Schlussanträge v. 26.01.2017, Rs. C-13/16, ECLI:EU:C:2017:43, Rn. 98 – Rīgas.

397 Vgl. Kap. 3 Pkt. A.III.2.a.bb.iii, S. 120.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

i. S. d. Art. 6 Abs. 1 S. 1 lit. f DSGVO überwiegen.[398] Als Legitimationstatbestand bleibt demnach meist allein die Einwilligung.[399]

a) Voraussetzungen der Zulässigkeit nach dem BDSG bzw. der DSRL

Die für die Wirksamkeit der Einwilligung maßgeblichen Vorgaben finden sich in § 4a Abs. 1 S. 1 BDSG sowie in Art. 2 lit. h, Art. 7 lit. a DSRL. Demnach muss die Einwilligung in inhaltlicher Hinsicht freiwillig, informiert und bestimmt erfolgen;[400] Vorgaben, deren Erfüllung gerade im Anbieter-Nutzer-Verhältnis oftmals zurecht in Zweifel gezogen werden.[401] Im Nutzer-Nutzer-Verhältnis ist hierbei die Freiwilligkeit der Einwilligung näher zu untersuchen. Denn es ist durchaus vorstellbar, dass sozialer Druck bei der Einwilligungserklärung der Nutzer in den Umgang mit den eigenen personenbezogenen Daten eine Rolle spielt.

Zudem müssen die strengen formellen Vorgaben des BDSG näher beleuchtet werden. § 4a Abs. 1 S. 3 BDSG stellt ein grundsätzliches Schriftformerfordernis für die Einwilligung auf. In der Realität wird jedoch selten ein Nutzer die schriftliche Einwilligung seiner Freunde und Bekannten einholen, bevor er Informationen über sie in sozialen Netzwerken preisgibt.

aa) Freiwilligkeit

Die Einwilligung muss freiwillig erfolgen. § 4a Abs. 1 S. 1 BDSG verlangt, dass die Einwilligung „[…] auf der freien Entscheidung des Betroffenen beruht." Art. 2 lit. h DSRL gibt ähnlich vor, dass die Einwilligung „ohne Zwang" erfolgen müsse. Die Freiwilligkeit der Einwilligung wird oftmals in Verbindung mit Verhandlungsungleichgewichten in Frage gestellt; das typische dabei besprochene Szenario bilden Anbieter-Nutzer-Verhältnisse[402] oder etwa die Einwilligung des Arbeitnehmers gegenüber dem Arbeitgeber.[403] Im Nutzer-Nutzer-Verhältnis könnte die Freiwilligkeit der

398 Vgl. Kap. 3 Pkt. A.III.2.c.bb.iii, S. 129.
399 A. A. wohl *Kampert,* Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, S. 110, der der Einwilligung ohne nähere Ausführungen „[…] praktisch kaum Relevanz […]" beimisst.
400 *Kühling/Seidel/Sivridis,* Datenschutzrecht, S. 143 ff.
401 Vgl. Kap. 3 Pkt. B.II, S. 182.
402 Vgl. Kap. 3 Pkt. B.II, S. 182.
403 Vgl. *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 36 ff.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Einwilligung dann entfallen, wenn sich ein Nutzer aus sozialem Druck verpflichtet fühlt, seine Einwilligung in den Umgang mit seinen personenbezogenen Daten zu geben. Hierzu lohnt es sich, die Bedeutung von sozialen Online-Netzwerken für die Sozialpflege näher zu beleuchten (dazu i.). Ferner können auch andere, in der Person selbst liegende Faktoren, die Freiwilligkeit der Einwilligung beeinträchtigen. Exemplarisch wird dies am Beispiel von Abhängigkeitserkrankungen dargestellt (dazu ii.).

i) Imagepflege durch Interaktion in sozialen Online-Netzwerken

Soziale Online-Netzwerke sind längst Bestandteil des Alltags geworden, insbesondere bei Jugendlichen und jungen Erwachsenen. In einer Studie aus dem Jahr 2010 gaben 76% der befragten Jugendlichen und jungen Erwachsenen an, ein Profil auf einem sozialen Netzwerk zu besitzen.[404] In einer Studie mit über 1000 Teilnehmern aus dem Jahr 2011 gaben 85 % der Teilnehmer an, die Website des sozialen Netzwerks *Facebook* täglich zu besuchen, während 70 % angaben, sich bei jeder Computernutzung in das Netzwerk einzuloggen. 26 % der Teilnehmer gaben sogar an, sich unwohl zu fühlen, wenn sie sich für eine längere Zeitspanne nicht auf *Facebook* einloggten.[405] Forschungen legen dabei nahe, dass die gesellschaftlichen Strukturen in sozialen Online-Netzwerken die der Offline-Welt spiegeln. Dieser Schluss wird aus der Beobachtung gezogen, dass Nutzer dazu tendieren, über lange Zeiträume hinweg trotz einer zahlenmäßig großen Kontaktliste nur mit derselben, begrenzten Anzahl von durchschnittlich etwa 10 Personen zu interagieren.[406] Daraus wird gefolgert, dass sich der Freundeskreis der Offline-Welt in der Online-Welt fortsetzt.[407] In diesem Kreis erweist sich die Gegenseitigkeit der Interaktion als besonders wichtig: Wenn ein Nutzer einen anderen „verlinkt", d. h. einen Link auf sein Profil in einem Beitrag oder Foto setzt, wird vom betroffenen Nutzer eine Reaktion in Form

404 *Autenrieth/Bänziger/Rohde/Schmidt,* Gebrauch und Bedeutung von Social Network Sites im Alltag junger Menschen: Ein Ländervergleich zwischen Deutschland und der Schweiz, in: Neumann-Braun/Autenrieth, S. 37.

405 *Denti/Barbopoulos/Nilsson/Holmberg/Thulin/Wendeblad/Andén/Davidsson*, GRI-rapport 2012:3, 15.

406 *Pfeffer/Neumann-Braun/Wirz,* Nestwärme in Bild-vermittelten Netzwerken – am Beispiel von Festzeit.ch, in: Fuhse/Stegbauer, S. 135.

407 *Wirz,* Nähe-orientiertes Handeln in den Weiten des Web, in: Neumann-Braun/Autenrieth, S. 135.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

eines Kommentars oder gar einer „Gegenverlinkung“ erwartet.[408] Bleibt diese „Anschlussfähigkeit“[409] hingegen aus, mindert dies den Wert des hochgeladenen oder geteilten Inhalts und bringt sogar potentiell das eigene Ansehen in Gefahr.[410] Denn das Profil in einem sozialen Netzwerk bietet eine Plattform zur Selbstvermarktung; Feedback über Kommentare mittels netzwerkinterner Werkzeuge wie *Facebooks* „Like-Button“ bewerten die Arbeit an der eigenen „Marke“ unmittelbar, wobei ausbleibendes Feedback als negativ bewertet wird.[411]

Diese Forschungsergebnisse zeigen auf, dass die Reziprozität in sozialen Netzwerken einen nicht unerheblichen Faktor für die Bildung von gesellschaftlichem Ansehen darstellt. Das bedeutet im Umkehrschluss aber auch, dass aktive Nutzer, die soziale Netzwerke gerade zur „Vermittlung eines Images der eigenen Person als Marke“[412] nutzen, davon abhängig sind, auf dieser Plattform gesehen zu werden und präsent zu sein.[413] Daraus kann man durchaus folgern, dass diese Nutzer eher geneigt sein werden, ihre Einwilligung in das Hochladen und Teilen der eigenen Informationen durch andere zu erteilen.

---

408 *Autenrieth,* MySelf. MyFriends. MyLife. MyWorld: Fotoalben auf Social Network Sites und ihre kommunikativen Funktionen für Jugendliche und junge Erwachsene, in: Neumann-Braun/Autenrieth, S. 132 f.

409 *Autenrieth,* MySelf. MyFriends. MyLife. MyWorld: Fotoalben auf Social Network Sites und ihre kommunikativen Funktionen für Jugendliche und junge Erwachsene, in: Neumann-Braun/Autenrieth, S. 158.

410 *Autenrieth,* MySelf. MyFriends. MyLife. MyWorld: Fotoalben auf Social Network Sites und ihre kommunikativen Funktionen für Jugendliche und junge Erwachsene, in: Neumann-Braun/Autenrieth, S. 154, 158.

411 *Autenrieth,* MySelf. MyFriends. MyLife. MyWorld: Fotoalben auf Social Network Sites und ihre kommunikativen Funktionen für Jugendliche und junge Erwachsene, in: Neumann-Braun/Autenrieth, S. 154.

412 *Autenrieth,* MySelf. MyFriends. MyLife. MyWorld: Fotoalben auf Social Network Sites und ihre kommunikativen Funktionen für Jugendliche und junge Erwachsene, in: Neumann-Braun/Autenrieth, S. 154.

413 Ähnlich *Walser,* "Darf ich dein Portemonnaie anschauen?", in: Neumann-Braun/Autenrieth, S. 85 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ii) Soziale Online-Netzwerke und Suchterkrankungen

Unabhängig davon wurde die extensive Nutzung von sozialen Online-Netzwerken in verschiedenen Studien auf ihr Suchtpotential untersucht.[414] Dabei legen diese Studien nahe, dass Suchterkrankungen im Zusammenhang mit sozialen Netzwerken auftreten können, wenngleich sie bisher nicht unter die Kategorie der Abhängigkeitserkrankungen des ICD-10 der *WHO* bzw. des DSM-5 der *APA* gefasst werden.[415] Als Motivation für die Nutzung der sozialen Netzwerke werden soziale Faktoren genannt.[416] In einer Studie gaben 61 % der Teilnehmer an, soziale Netzwerke zu nutzen, weil ihre Freunde sie ebenfalls nutzten.[417] Zugleich wurde ein Zusammenhang zwischen Suchterkrankungen im Kontext von sozialen Netzwerken und bestimmten Persönlichkeitszügen beobachtet.[418]

Suchterkrankungen im Zusammenhang mit sozialen Netzwerken zeigten in Studien dieselben Symptome wie Suchterkrankungen im Zusammenhang mit dem Missbrauch von Substanzen: Stimmungsschwankungen (d. h. die Veränderung der Gefühlslage durch die Nutzung sozialer Netzwerke), Vernachlässigung anderer Interessen (d. h. die verhaltensgebundene, gedankliche und emotionale Beschäftigung mit der Nutzung sozialer Netzwerke), Toleranz (d. h. die stete Erhöhung der Nutzung sozialer Netzwerke), Entzugserscheinungen (d. h. die Erfahrung emotionalen sowie körperlichen Unwohlseins, wenn die Nutzung verringert oder beendet wird), Konflikte (d. h. die Entwicklung zwischenmenschlicher oder intrapsychischer Probleme durch die Nutzung sozialer Netzwerke) und Rückfall (d. h. die zügige Wiederkehr exzessiver Nutzung sozialer Netzwerke nach einer Phase der Abstinenz).[419] Das ist deswegen interessant, weil damit die Erkenntnisse der Forschung zu Substanzsuchterkrankungen möglicherweis auf die Suchterkrankungen im Zusammenhang mit sozialen Netzwerken übertragen werden können. Dabei sind „Substanzabhängigkeiten […] typischer-

414 Exemplarisch *Guedes/Sancassiani/Carta/Campos/Machado/Spear King/Nardi*, Clin Pract Epidemiol Ment Health 2016, 43; *Kuss/Griffiths*, Int J Environ Res Public Health. 2011, 3528; *Subrahmanyam/Reich/Waechter/Espinoza*, J Appl Dev Psychol 2008, 420.

415 *Grant/Chamblerlain*, CNS Spectrums 2016, 300; *Guedes/Sancassiani/Carta/Campos/Machado/Spear King/Nardi*, Clin Pract Epidemiol Ment Health 2016, 43, S. 2 m. w. N.

416 *Kuss/Griffiths*, Int J Environ Res Public Health. 2011, 3528, S. 4 m. w. N.

417 *Subrahmanyam/Reich/Waechter/Espinoza*, J Appl Dev Psychol 2008, 420, 426.

418 *Kuss/Griffiths*, Int J Environ Res Public Health. 2011, 3528, S. 6 f.

419 *Kuss/Griffiths*, Int J Environ Res Public Health. 2011, 3528, S. 2.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

weise durch eine verminderte Kontrolle über den Substanzkonsum trotz negativer psychischer, sozialer oder körperlicher Folgen gekennzeichnet."[420] Studien zufolge sind Patienten mit einer Abhängigkeitserkrankung anders als gesunde Personen nicht in der Lage, ihr Verhalten an negative Konsequenzen psychischer, physischer oder sozialer Art anzupassen.[421]

Übertragen auf die Abhängigkeit von der Nutzung sozialer Netzwerke könnte das bedeuten, dass Erkrankte keinen oder nur verminderten Einfluss darauf haben, ob sie in die Verarbeitung ihrer personenbezogenen Daten einwilligen. Die Einwilligung in die Verarbeitung personenbezogener Daten würde demnach nicht freiwillig erfolgen.

iii) Auswirkungen auf die Freiwilligkeit der datenschutzrechtlichen Einwilligungserklärung

Fraglich sind die Auswirkungen der oben genannten Phänomene auf die datenschutzrechtliche Einwilligungserklärung. Hierbei sind die Ergebnisse zur Bedeutsamkeit der Reziprozität der Kommunikationshandlung unter den Nutzern von den Auswirkungen des Leidens an einer Abhängigkeitserkrankung zu unterscheiden.

(1) Auswirkungen von sozialem Druck auf die Wirksamkeit der Einwilligung

Sozialer Druck kann die Freiwilligkeit der datenschutzrechtlichen Einwilligungserklärung beeinträchtigen; in der Konsequenz könnte die Einwilligung nichtig sein, mit der Folge, dass die Datenverarbeitung ex tunc nichtig wäre. Hierbei könnten die Ergebnisse der *BGH*-Rechtsprechung zum Wettbewerbsrecht übertragbar sein.[422] So führte der *BGH* in verschiedenen Urteilen aus, dass Kunden sich dann zum Abschluss eines Kaufvertrages genötigt fühlen könnten, wenn sie aus dem Gefühl der Peinlichkeit und der

420 *Heberlein/Bleich*, Die Psychiatrie 2013, 239.
421 *Heberlein/Bleich*, Die Psychiatrie 2013, 239, 240 f. m. w. N.
422 *Radlanski,* Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 87 ff. mit ausführlicher Analyse.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Angst vor dem Verlust von Wertschätzung das Gefühl haben, dem Vertragsschluss nicht ausweichen zu können.[423] Bei den oben genannten Studien liegt der Fall jedoch anders: Die Einwilligung erfolgt ja gerade zum Ausbau und zur Pflege des erwünschten positiven Ansehens im gesellschaftlichen Kreis. Wie gezeigt verlagert sich lediglich die Pflege sozialer Kontakte aus der Realwelt zunehmen auch in die Online-Welt. Die Grenzen sind insofern durchaus fließend: Denn freilich ist es vorstellbar, dass Nutzer abhängig von ihrem sozialen Umfeld auch einem darüberhinausgehenden sozialen Druck zur Einwilligungserklärung ausgeliefert sind. Dennoch muss davor gewarnt werden, das Konstrukt der unfreiwilligen Einwilligung durch sozialen Druck zu leichtfertig zu bemühen. Die Einwilligung ist Ausdruck des Recht auf informationelle Selbstbestimmung.[424] Das Streben nach Ansehen alleine kann die Freiwilligkeit der Einwilligung nicht grundsätzlich entfallen lassen, da andernfalls letztlich kaum ein Nutzer sein Recht auf informationelle Selbstbestimmung in Form der Einwilligung wirksam ausüben könnte. Zweitens sind auch die Folgen für den Datenverarbeiter zu bedenken. Die fehlende Freiwilligkeit der Einwilligung macht die Einwilligungserklärung nichtig und die Datenverarbeitung damit ex tunc unzulässig; im Sinne der Rechtssicherheit müssen insofern für die Behauptung der Unfreiwilligkeit der Einwilligung belastbare Anhaltspunkte gegeben sein.

(2) Auswirkungen von Abhängigkeitserkrankungen auf die Wirksamkeit der Einwilligung

Von den Auswirkungen auf die Einwilligung durch sozialen Druck sind die Auswirkungen von Abhängigkeitserkrankungen zu unterscheiden. Denn soweit es sich um die Beurteilung der Freiwilligkeit der datenschutzrechtlichen Einwilligung handelt, dreht sich die Diskussion vorrangig um äußere Faktoren. Bei Abhängigkeitserkrankungen ist die Freiwilligkeit der Entscheidungsfähigkeit jedoch „von innen“ gefährdet. Es handelt sich damit nicht um einen klassischen Fall der entfallenen Freiwilligkeit der datenschutzrechtlichen Einwilligung, sondern vielmehr – unter Umständen – um

423 *BGH,* Urt. v. 04.12.1986, Az. I ZR 170/84, NJW 1987, 908 – Alles frisch; *BGH,* Urt. v. 29.06.1989, Az. I ZR 180/87, NJW 1989, 3013 – McBacon; *BGH,* Urt. v. 22.05.2003, Az. I ZR 185/00, GRUR 2003, 804, 805 – Foto-Aktion.; ausführlich *Radlanski,* Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 87 ff.

424 *Kühling/Seidel/Sivridis,* Datenschutzrecht, S. 143.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

einen Fall der eingeschränkten Urteilsfähigkeit. Dies gilt unabhängig davon, ob die Einwilligung als rechtsgeschäftliche Erklärung[425], als geschäftsähnliche Handlung[426] oder als Realakt[427] einzustufen ist. Bei der Einwilligung handelt es sich um die Wahrnehmung von Grundrechten, weswegen es nicht auf die Geschäftsfähigkeit des Betroffenen ankommen kann.[428] Aus den zuvor zitierten Studien geht hervor, dass Suchterkrankte während ihrer Erkrankung ihr Wahlverhalten nicht oder nur eingeschränkt beeinflussen können. Je nach konkretem Einzelfall kann demnach die Urteilsfähigkeit bei einer Abhängigkeitserkrankung eingeschränkt sein. In diesen Fällen wäre die Einwilligung nichtig.

iv) Zwischenergebnis

Die Freiwilligkeit der Einwilligung im Nutzer-Nutzer-Verhältnis kann durch sozialen Druck beeinflusst sein. Gleichwohl ist die Schwelle hier nicht zu niedrig anzusetzen: Die Freiwilligkeit entfällt nicht bereits deswegen, weil die Einwilligung im Rahmen der Imagepflege erteilt wird, die als Fortsetzung der Realkontaktpflege auch in Online-Netzwerken betrieben wird. Wenn in Folge einer Abhängigkeitserkrankung die Urteilsfähigkeit eingeschränkt ist, kann dies die Wirksamkeit der Einwilligung entfallen lassen. Dies ist jedoch kein klassischer Fall der entfallenen Freiwilligkeit der Einwilligung, sondern Folge der eingeschränkten Einsichts- und Urteilsfähigkeit des Betroffenen.

425 Vgl. *Simitis*, in: Simitis, BDSG, § 4a, Rn. 20, *Bergmann/Möhrle/Herb,* BDSG, §4a, Rn. 9; *Buchner,* Informationelle Selbstbestimmung im Privatrecht, S. 236 ff.

426 Vgl. *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 33 f.

427 Vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 4a, Rn. 20; *Schaffland/Wiltfang,* BDSG, § 4a, Rn. 21.

428 *BVerfG,* Beschl. v. 10.02.1960, Az. 1 BvR 526/53, 1 BvR 29/58, BVerfGE 10, 302 – Aufenthaltsbestimmungsrecht des Vormunds, vgl. *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 33 f.; *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 47.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

bb) Informiertheit und Bestimmtheit

Die Einwilligung muss ferner gem. Art. 2 lit. h DSRL „in Kenntnis der Sachlage erfolg[en]". § 4a Abs. 1 S. 2 BDSG präzisiert diese Anforderungen dahingehend, dass der Zweck des Umgangs mit personenbezogenen Daten darzulegen ist sowie die Folgen der Verweigerung der Einwilligung, soweit erforderlich oder dies vom Betroffenen verlangt wird. Im Nutzer-Nutzer-Verhältnis dürfte dies im Regelfall unproblematisch der Fall sein. Selbiges gilt für die Bestimmtheit der Einwilligung: Gem. Art. 2 lit. h DSRL muss sie „für den konkreten Fall" gegeben werden, das bedeutet, dass der Betroffene sich über den Inhalt seiner Einwilligung im Klaren sein muss.[429]

cc) Schriftformerfordernis

i) Schriftformerfordernis als Grundsatz im BDSG

Ferner ist gem. § 4a Abs. 1 S. 3 BDSG grundsätzlich die Schriftform für die wirksame Einwilligung erforderlich. Schriftform meint damit die eigenhändige Unterschrift i. S. d. § 126 BGB.[430] Zwar kann sie durch die elektronische Schriftform i. S. d. § 126a BGB ersetzt werden; sie besitzt im Lichte der Anforderungen einer „[…] qualifizierten elektronischen Signatur nach dem Signaturgesetz […]" i. S. d. § 126a Abs. 1 BGB jedoch kaum praktische Relevanz.[431] Das Schriftformerfordernis ist deswegen interessant, weil insbesondere im Nutzer-Nutzer-Verhältnis wohl regelmäßig keine schriftliche Einwilligungserklärung gegeben wird – der Gedanke, dass ein Nutzer einen anderen ein Schriftstück unterschreiben lässt, bevor er etwa seinen Namen in einem Post „verlinkt", erscheint geradezu abwegig.

Das Schriftformerfordernis in § 4a Abs. 1 BDSG ist nicht absolut; das BDSG schreibt es nur vor, „[…] soweit nicht wegen besonderer Umstände eine andere Form angemessen ist […]", § 4a Abs. 1 S. 3 Hs. 2 BDSG. Die Formulierung „soweit nicht" in § 4a Abs. 1 S. 3 Hs. 2 BDSG verdeutlich allerdings, dass es sich hier um eine Ausnahmevorschrift handelt und

429 *Kühling/Seidel/Sivridis,* Datenschutzrecht, S. 151.

430 *Simitis*, in: Simitis, BDSG, § 4a, Rn. 33; *Taeger*, in: Taeger/Gabel, BDSG, § 4a, Rn. 33; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 48; einschränkend *Thüsing/Schmidt/Forst*, RDV 2017, 116, 117 ff.

431 *Simitis*, in: Simitis, BDSG, § 4a, Rn. 37 f.; *Taeger*, in: Taeger/Gabel, BDSG, § 4a, Rn. 34; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 48.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

grundsätzlich die Schriftform erforderlich ist. So kann die Einwilligung zwar beispielsweise auch mündlich erteilt werden;[432] auch die Einwilligung per E-Mail oder unter Nutzung eines Messangerdienstes ist möglich. Gleichwohl liegt die Beweislast, dass ein Abweichen von der Schriftform wegen besonderer Umstände angemessen ist, bei der verantwortlichen Stelle. Zudem kann der Ausnahmecharakter der von der Schriftform abweichenden Formen der Einwilligungserklärung zu erhöhter Rechtsunsicherheit für Datenverarbeiter führen.

Zwar kann man mit guten Gründen bei der hier untersuchten Fallgestaltung – die Einwilligung im Nutzer-Nutzer-Verhältnis von sozialen Netzwerken – von „besonderen Umständen" ausgehen, die ein Abweichen vom Schriftformerfordernis rechtfertigen. Denn die Kommunikation von Nutzern sozialer Netzwerke findet tendenziell zu einem nicht unerheblichen Teil elektronisch statt.[433] Es wäre bei einem rein digitalen Sachverhalt jedoch unangemessen, eine „analoge" Unterschrift zu fordern. Dies gilt insbesondere deswegen, weil ein solches Vorgehen in der Praxis schlicht unüblich ist und das Hochladen und Teilen von Informationen Anderer auch trotz mündlich oder elektronisch erteilter Einwilligung unzulässig wäre. Da es hierzu jedoch bislang keine gefestigte Rechtsprechung gibt, bleibt die durch das grundsätzliche Schriftformerfordernis hervorgerufene Rechtsunsicherheit dennoch bestehen.

ii) Vereinbarkeit des Schriftformerfordernisses mit den Vorgaben der DSRL

Teilweise wird diskutiert, ob das Schriftformerfordernis europarechtswidrig ist, da die DSRL selbst kein Schriftformerfordernis vorsieht. Davon könnte man ausgehen, da die DSRL vollharmonisierende Wirkung hat und kein Abweichen im Schutzniveau zulässt.[434] Die Mitgliedstaaten dürfen „[…] weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 der Richtlinie 95/46 einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in

---

432 *Simitis*, in: Simitis, BDSG, § 4a, Rn. 43; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 49 ff.

433 i. E ähnlich *Taeger*, in: Taeger/Gabel, BDSG, § 4a, Rn. 37 ff.

434 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 30, 32 – ASNEF und FECEMD m. Anm. *Kühling*, EuZW 2012, 281; ausführlich *Raab,* Die Harmonisierung des einfachgesetzlichen Datenschutzes, S. 32 ff.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

diesem Artikel vorgesehenen Grundsätze verändern würden."[435] Hingegen dürfen die Mitgliedstaaten gem. Art. 5 DSRL die Voraussetzungen der Rechtmäßigkeit der Verarbeitung personenbezogener Daten näher bestimmen. Der *EuGH* hat hierzu ausgeführt, dass die Mitgliedstaaten von diesem Ermessen jedoch nur im Einklang mit dem Ziel der DSRL – also dem Schutz personenbezogener Daten einerseits und die Förderung des freien Verkehrs derselben zwischen den Mitgliedstaaten andererseits, vgl. Art. 1 DSRL – Gebrauch machen dürfen.[436]

Mit dem Erfordernis der Schriftform stellt § 4a Abs. 1 S. 3 BDSG keinen neuen, von Art. 7 DSRL abweichenden Grundsatz auf. Art. 7 lit. a DSRL sieht die Einwilligung als Legitimationstatbestand vor, § 4a Abs. 1 BDSG setzt diese Vorgabe um. Fraglich ist jedoch, ob das Schriftformerfordernis eine zusätzliche Bedingung aufstellt, die die Tragweite der Einwilligung als Legitimationstatbestand verändert, oder ob i. S. d. Art. 5 DSRL hiermit eine zulässige nähere Bestimmung der Voraussetzungen gegeben ist.

Für eine Veränderung der Tragweite spricht die oben dargestellte datenschutzrechtliche Realität: Das Schriftformerforderns der Einwilligung wird in der Praxis, insbesondere soweit es sich um mit dem Internet verbundenen Sachverhalten handelt, kaum eingehalten und erhöht die Rechtsunsicherheit für die verantwortliche Stelle.

Allerdings sieht § 4a Abs. 1 S. 3 Hs. 2 BDSG durchaus die Möglichkeit anderer Formen der Einwilligungserklärung vor. Man könnte das Schriftformerfordernis auch als Präzision der Vorgabe des Art. 7 lit. a DSRL sehen, die eine Einwilligung „ohne jeden Zweifel" verlangt. Denn das Schriftformerfordernis hat eine Warnfunktion für den Betroffenen, der sich über die Folgen seiner Einwilligung im Klaren sein soll.[437]

Dadurch, dass § 4a Abs. 1 S. 3 BDSG die Schriftform zwar als vorrangige Form der Einwilligungserklärung vorsieht, jedoch Raum für andere Formen der Einwilligungserklärung belässt, sprechen die besseren Argumente dafür, dass es sich hier um eine zulässige Konkretisierung der Voraussetzungen handelt und nicht um eine Bedingung, die die Tragweite des

---

435 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 32 – ASNEF und FCEMD; vgl. zudem *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779, Rn. 57 – Breyer.

436 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 36 – ASNEF und FCEMD; vgl. zudem *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779, Rn. 58 – Breyer.

437 *Simitis*, in: Simitis, BDSG, § 4a, Rn. 33; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 49.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Legitimationstatbestands der Einwilligung verändert.[438] Dies bedeutet jedoch auch, dass die Anforderungen an das Vorliegen der „besonderen Umstände" i. S. d. § 4a Abs. 1 S. 3 Hs. 2 BDSG nicht zu hoch gesetzt werden dürfen. Die Einwilligung im Nutzer-Nutzer-Verhältnis zum Teilen von Informationen stellt vorliegend einen solchen „besonderen Umstand" dar.

iii) Nutzereinstellungen als konkludente Einwilligungserklärung

Fraglich ist, ob Nutzereinstellungen als konkludente Einwilligungserklärung in die Datenverarbeitung durch andere Nutzer angesehen werden können. Die konkludente Einwilligung ist grundsätzlich möglich, solange sie den genannten inhaltlichen Voraussetzungen entspricht.[439]

In den meisten sozialen Netzwerken können Nutzer einstellen, mit welchen ihrer Kontakte sie bestimmte Informationen teilen wollen. Gleichzeitig haben viele soziale Netzwerke Funktionen integriert, mittels derer die hochgeladenen Informationen einfach weiterverbreitet werden können. Beispielhaft kann hier *Facebooks* „Share-Button" genannt werden, der mit einem einzigen Klick die Weiterverbreitung einer Information zulässt. Daraus könnte man schließen, dass ein Nutzer konkludent in die Weiterverbreitung der von ihm hochgeladenen personenbezogenen Daten einwilligt.

Allerdings wird es bei derartigen Fallgestaltungen regelmäßig mindestens an der Bestimmtheit der Einwilligungserklärung fehlen. Denn die Einwilligung muss i. S. d. Art. 2 lit. h „für den konkreten Fall" erteilt werden. Dies bezieht sich aber nicht nur auf das konkrete personenbezogene Datum, sondern auch auf die konkreten Umstände des Umgangs mit personenbezogenen Daten an sich.[440] Dies ist aber nicht gegeben, wenn die Funktion, mit der die personenbezogenen Daten weiterverwendet werden können, pauschal bei jeder hochgeladenen Information erscheint. Das gilt umso mehr, als in den meisten sozialen Netzwerken zwar die Sichtbarkeit des jeweils hochgeladenen Beitrags personengenau angegeben werden kann, es jedoch

438 Ebenso *Radlanski,* Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, S. 109 f.; offen *Krohm*, ZD 2016, 368, 369; a. A. *Piltz,* Soziale Netzwerke im Internet, S. 129 ff.; *Vulin*, ZD 2012, 414, 417.

439 So auch *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 50; *Piltz,* Soziale Netzwerke im Internet, S. 133 ff; *Taeger*, in: Taeger/Gabel, BDSG, § 4a, Rn. 41 ff.; *Däubler*, in: DKWW, BDSG, § 4a, Rn. 16; *Bergmann/Möhrle/Herb,* BDSG, § 4a, Rn. 85; *Kramer*, in: Auernhammer, BDSG, § 4a, Rn. 33; a. A. *Simitis*, in: Simitis, BDSG, § 4a, Rn. 44.

440 *Kühling/Seidel/Sivridis,* Datenschutzrecht, S. 148 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

meist keine individuelle Regelungsmöglichkeit für die Funktion zur Weiterverbreitung gibt. Doch auch wenn es solche individuellen Steuerungsmöglichkeiten gäbe, müssten strenge Anforderungen zur Wahrung der Informiertheit und Bestimmtheit der Einwilligung erfüllt werden: Denn zur Wahrung der Informiertheit und Bestimmtheit muss der Betroffene sich konkret im Klaren sein, welche Phasen des Datenumgangs geplant sind.[441] So würde es noch keine konkludente Einwilligungserklärung begründen, wenn der Nutzer auch die Funktion zur Weiterverbreitung nur bestimmten Personen zugänglich machen könnte. In diesem Fall wäre nämlich über den konkreten Umgang mit den personenbezogenen Daten noch keine Aussage getroffen. Dementsprechend kann auch nicht von einer „Generalerlaubnis" in sämtliche Möglichkeiten des weiteren Umgangs mit den personenbezogenen Daten ausgegangen werden. Regelmäßig ist davon auszugehen, dass die wenigsten Nutzer bei der Aktivierung der Funktion, mittels derer ihre personenbezogenen Daten geteilt werden können, sich über alle Möglichkeiten der Weiterverbreitung – namentlich sämtliche ihrer Kontakte, die Zugang zu der Funktion haben und sämtliche Möglichkeiten der Weiterverbreitung durch diese Personen – bewusst sind oder sich darüber Gedanken gemacht haben.

Es ist also auch dann eine Einwilligung in den konkreten Umgang mit personenbezogenen Daten zu verlangen, wenn der Betroffene personenbezogene Daten in einem sozialen Netzwerk teilt und das entsprechende soziale Netzwerk Funktionen bereitstellt, mittels derer die Informationen weiterverbreitet werden können.

b) Voraussetzungen der Zulässigkeit nach der DSGVO

Vorschriften zur Einwilligung finden sich in der DSGVO in Art. 7, 8 DSGVO sowie in Art. 4 Nr. 11 DSGVO.

Gem. Art. 4 Nr. 11 DSGVO ist die Einwilligung „[…] jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebener Willensbekundung […]". Gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO muss die Einwilligung „für einen oder mehrere bestimmte Zwecke" erteilt worden sein.

Aus dem Zusammenspiel dieser Normen und unter Hinzuziehung der einschlägigen Erwägungsgründe – namentlich EG 32 f. und EG 42 f.

441 *Kühling/Seidel/Sivridis,* Datenschutzrecht, S. 148 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

DSGVO – lässt sich zunächst feststellen, dass sich die inhaltlichen Anforderungen aus dem BDSG bzw. der DSRL der Freiwilligkeit, Informiertheit und Bestimmtheit in den Vorgaben der DSGVO wiederfinden; dahingehend kann auf die Ausführungen in Bezug auf das BDSG bzw. die DSRL verwiesen werden. Die Anforderungen an die Freiwilligkeit werden nunmehr in Art. 7 Abs. 4 DSGVO in Form eines Koppelungsverbots präzisiert.[442]

Eine elementare Änderung bietet die DSGVO jedoch hinsichtlich der Form der Einwilligung. Das grundsätzliche Schriftformerfordernis aus § 4a Abs. 1 S. 3 BDSG findet kein Pendant in der DSGVO. Im Gegenteil: Gem. Art. 4 Nr. 11 DSGVO muss eine „[…] Erklärung oder […] sonstige[ ] eindeutige[ ] bestätigende[ ] Handlung […]“ vorliegen. EG 32 S. 1 DSGVO präzisiert, dass auch eine mündliche oder elektronisch erklärte Einwilligung wirksam ist. Damit ist die durch das BDSG grundsätzlich vorgeschriebene Schriftformerfordernis hervorgerufene Rechtsunsicherheit unter der DSGVO beseitigt. Zugleich trägt jedoch für das Vorliegen der Einwilligung gem. Art. 7 Abs. 1 DSGVO der Verarbeiter die Beweislast. Dahingehend wird es also auch künftig den Datenverarbeitern zu raten sein, die Einwilligung nicht nur mündlich einzuholen. Allerdings geht durch die Klarstellung in EG 32 S. 1 DSGVO nunmehr eindeutig hervor, dass eine Einwilligung auf elektronischem Wege, etwa über einen Messenger oder per E-Mail, auch den Formerfordernissen der DSGVO entspricht. Gerade durch die gelockerten Anforderungen hinsichtlich der Form der Einwilligung erweist sich die DSGVO damit als Fortschritt gegenüber dem strengen Schriftformerfordernis des BDSG und bietet wertvolle Neuerungen, die an die datenschutzrechtliche Realität der digitalen Kommunikation angepasst sind.

IV. Zulässigkeit der Verarbeitung von Fotos Anderer

Neben der Verarbeitung von Informationen Anderer in sozialen Netzwerken muss ferner die Zulässigkeit des Hochladens oder Teilens von Fotos Anderer diskutiert werden. Die Möglichkeit Urlaubsfotos, Fotos der eigenen Person und des Freundeskreises mit seinen Kontakten zu teilen, wird von einer Vielzahl von Nutzern intensiv genutzt.

442 Vgl. Kap. 3 Pkt. B.II.1.a.bb, S. 186.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

1. Divergierende Zulässigkeitsvoraussetzungen i. S. d. KUG und BDSG/DSRL sowie DSGVO

Bei Fotos kommen für die Zulässigkeit der Verarbeitung nicht nur die Normen des Datenschutzrechts, also des BDSG bzw. der DSRL und der DSGVO in Betracht, sondern auch die des KUG[443]. Gem. § 22 S. 1 KUG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Das bedeutet, dass nach dem KUG außer der Einwilligung keine weiteren Legitimationsmöglichkeiten vorgesehen sind, die das Verbreiten oder die öffentliche Zurschaustellung zulassen. Gewisse Ausnahmen von diesem Grundsatz sind in §§ 23 f. KUG geregelt (sog. „abgestuftes Schutzkonzept"[444]). Darüber hinaus sieht das KUG keine dem BDSG ähnlichen Erlaubnisnormen vor.

Mit dem Schriftformerfordernis in § 4a Abs. 1 S. 3 BDSG stellt das BDSG grundsätzlich höhere Anforderungen an die Form der Einwilligung als das KUG. Das KUG enthält keine Vorschriften über die Form der Einwilligung, sie kann also auch mündlich, konkludent und sogar stillschweigend erteilt werden.[445] Das BDSG hingegen sieht ein Abweichen von der Schriftform zwar auch vor, „[…] soweit nicht wegen besonderer Umstände eine andere Form angemessen ist […]", § 4a Abs. 1 S. 3 Hs. 2 BDSG, allerdings nur als Ausnahme zum grundsätzlichen Erfordernis der Schriftform. Daher wird in der Literatur eine restriktive Handhabung dieser Vorschrift gefordert.[446]

Die DSGVO enthält, wie schon die DSRL, kein Schriftformerfordernis. Gleichwohl muss die Einwilligung „unmissverständlich" abgegeben wer-

---

443 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie Vom 9. Januar 1907, RGBl. 1907, 7, im Folgenden: KUG.

444 *Engels,* in: BeckOK UrhR, KUG, § 22, Rn. 11 ff.

445 *Fricke*, in: Wandtke/Bullinger, UrhR, KUG, § 22, Rn. 13; *Specht*, in: Dreier/Schulze/Specht, UrhR, KUG, § 22, Rn. 17; *Engels*, in: BeckOK UrhR, KUG, § 22, Rn. 31.

446 *Simitis,* in: Simitis, BDSG, § 4a, Rn. 44; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 49; *Däubler*, in: DKWW, BDSG, § 4a, Rn. 15; zwar ist im Nutzer-Nutzer-Verhältnis in sozialen Netzwerken regelmäßig das Vorliegen „besonderer Umstände" i. S. d. § 4a Abs. 1 S. 3 Hs. 2 BDSG zu bejahen, so dass sich zu den Vorgaben des KUG im Ergebnis keine Änderungen ergeben. Dies ist aber umstritten und nicht durch gefestigte Rechtsprechung gesichert, vgl. Kap. 3 Pkt. A.III.3.a.cc, S. 138.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

den, Art. 4 Nr. 11 DSGVO. Stillschweigende oder mutmaßliche Einwilligungen sind also auch nach der DSGVO nicht ausreichend, EG 32 S. 3 DSGVO.[447]

Darüber hinaus ist die datenschutzrechtliche Einwilligung grundsätzlich frei widerruflich. In der DSGVO ist dies gem. Art. 7 Abs. 3 S. 1 explizit festgelegt. Aber auch unter dem BDSG ist die datenschutzrechtliche Einwilligung als Ausdruck des Rechts auf informationelle Selbstbestimmung frei widerruflich.[448] Im Gegensatz dazu ist die Widerruflichkeit der Einwilligung nach dem KUG umstritten und wird nur in bestimmten Fällen als möglich erachtet.[449]

2. Sachlicher Anwendungsbereich des KUG

Wegen dieser Divergenz an Anforderungen an die Zulässigkeit der Datenverarbeitung muss zunächst eruiert werden, ob sich der sachliche Anwendungsbereich von KUG und BDSG bzw. DSRL sowie DSGVO überschneiden. Gem. § 1 Abs. 3 S. 1 BDSG ist das BDSG grundsätzlich subsidiär, „[…] [s]oweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind […]". Dies gilt unabhängig davon, ob das Spezialgesetz den Schutz des BDSG über- oder unterschreitet.[450] Die Grenze „nach unten" stellt freilich die Einhaltung der vom *BVerfG* im Volkszählungsurteil[451] aufgestellten Grundsätze zum informationellen Selbstbestimmungsrecht dar.[452]

Der Subsidiaritätsgrundsatz gilt nur für deckungsgleiche Regelungen.[453] Nur dann stellt sich die Frage, in welchem Verhältnis die Vorschriften zueinanderstehen. Eine solche Überschneidung könnte vorliegen, wenn ein

---

447 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 7, Rn. 57.

448 *Simitis,* in: Simitis, BDSG, § 4a, Rn. 94 f.; *Taeger,* in: Taeger/Gabel, BDSG, § 4a, Rn. 81 f.; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 31.

449 Vgl. den Überblick bei *Fricke*, in: Wandtke/Bullinger, UrhR, KUG, § 22, Rn. 19 f. m. w. N.

450 *Schmidt*, in: Taeger/Gabel, BDSG, § 1, Rn. 55; *Weichert*, in: DKWW, BDSG, § 1, Rn. 14; *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 1, Rn. 24.

451 *BVerfG,* Urt. v. 15.12.1983, Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 – Volkszählung.

452 Ähnlich *Dix*, in: Simitis, BDSG, § 1, Rn. 172.

453 *Schmidt*, in: Taeger/Gabel, BDSG, § 1, Rn. 34; *Dix*, in: Simitis, BDSG, § 1, Rn. 170; vgl. dazu sogleich Kap. 3 Pkt. A.IV.3 f., S. 149.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Nutzer ein Foto einer anderen Person in einem sozialen Netzwerk für Andere zugänglich macht. Dazu müsste gem. § 22 S. 1 KUG ein Bildnis „verbreitet oder öffentlich zur Schau gestellt werden".

a) Bildnis

Bei einem Bildnis handelt es sich um die „[…] Darstellung einer Person, die deren äußere Entscheinung [*sic*] in einer für Dritte erkennbaren Weise wiedergibt […]".[454] Für die Erkennbarkeit reicht bereits aus, wenn der Abgebildete davon ausgehen darf, dass er von Dritten erkannt wird.[455] Dies deckt sich mit der Voraussetzung für die Anwendbarkeit des BDSG bzw. der DSRL und der DSGVO, wonach die Person gem. § 3 Abs. 1 BDSG bzw. Art. 2 lit. a DSRL und Art. 4 Nr. 1 DSGVO zumindest bestimmbar sein muss, § 1 Abs. 1, 2 BDSG bzw. Art. 3 Abs. 1 DSRL und Art. 12 Abs. 1 DSGVO. Sofern es sich also z. B. um ein hochgeladenes oder geteiltes Foto einer darauf erkennbaren Person handelt, ist zunächst der Anwendungsbereich von beiden Regelwerken eröffnet.

b) Verbreiten oder öffentliches Zurschaustellen

aa) Verbreiten

Ferner müsste es sich nach dem KUG bei dem Hochladen oder Teilen eines Bildnisses um ein Verbreiten oder öffentliches Zurschaustellen i. S. d. § 22 S. 1 KUG handeln. Verbreiten i. S. d. Norm bedeutet allerdings nur das körperliche Verbreiten und kommt bei der Zugänglichmachung in sozialen Netzwerken daher nicht in Betracht.[456]

---

454 *BGH,* Urt. v. 01.12.1999, Az. I ZR 226/97, NJW 2000, 2201, 2202 – Der blaue Engel; ebenso *Engels*, in: BeckOK UrhR, KUG, § 22, Rn. 19; *Herrmann*, in: BeckOK InfoMedienR, KUG, § 22, Rn. 2.

455 *Fricke*, in: Wandtke/Bullinger, UrhR, KUG, § 22, Rn. 7; *Engels*, in: BeckOK UrhR, KUG, § 22, Rn. 22; *Specht*, in: Dreier/Schulze/Specht, UrhR, KUG, § 22, Rn. 4.

456 *Engels*, in: BeckOK UrhR, KUG, § 22, Rn. 51; *Herrmann*, in: BeckOK InfoMedienR, KUG, § 22, Rn. 11; *Specht*, in: Dreier/Schulze/Specht, UrhR, KUG, § 22, Rn. 9.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

bb) Öffentliches Zurschaustellen

Es könnte sich bei dem Hochladen oder Teilen von Bildnissen in sozialen Netzwerken jedoch um ein öffentliches Zurschaustellen handeln. Unter Zurschaustellung ist zunächst das Zugänglichmachen eines Bildnisses, insbesondere die unkörperliche Wiedergabe desselben, an das Publikum gemeint.[457] Eine öffentliche Zurschaustellung liegt vor, wenn die Zurschaustellung gegenüber einer Mehrzahl von Personen erfolgt, es sei denn, dass der Personenkreis abgegrenzt ist und eine Verbundenheit des Personenkreises durch gegenseitige Beziehungen oder Beziehungen zum Zurschaustellenden vorliegt (§ 15 Abs. 3 UrhG).[458] Somit liegt zumindest in solchen Fällen, in denen ein Nutzer ein Foto einer anderen Person in einem sozialen Netzwerk dergestalt zugänglich macht, dass es nicht nur für seine mit ihm verbundenen Kontakte, sondern für jeden Internetnutzer einsehbar ist, eine öffentliche Zurschaustellung i. S. d. § 15 Abs. 3 UrhG vor,[459] da es hier bereits an dem Merkmal des abgegrenzten Personenkreises fehlt. Mindestens in diesem Fall überschneiden sich also die sachlichen Anwendungsbereiche der §§ 22, 23 KUG und des BDSG bzw. der DSGVO.

Darüber hinaus könnte ein öffentliches Zurschaustellen auch in den Fällen vorliegen, in denen der Nutzer das Foto für alle mit ihm verbundenen Kontakte freigibt. Zwar ist in diesen Fällen der Personenkreis, dem das Foto zugänglich gemacht wird, abgegrenzt. Nur allzu oft haben Nutzer in sozialen Netzwerken jedoch hunderte, gar tausende mit ihnen vernetzte Kontakte, sog. „Freunde“. Ein öffentliches Zurschaustellen i. S. d. § 22 S. 1 KUG läge dann vor, wenn zwischen demjenigen, der das Foto zugänglich macht und seinen „Freunden“ im sozialen Netzwerk – oder unwahrscheinlicher, zwischen seinen mit ihm verbundenen Kontakten –, eine innere Verbundenheit nicht besteht. Für das Vorliegen einer inneren Verbundenheit ist eine familiäre oder freundschaftliche Bindung nicht zwangsläufig notwendig, es muss jedoch ein enger, regelmäßiger Kontakt bestehen.[460] Hierfür

457 *Engels*, in: BeckOK UrhR, KUG, § 22, Rn. 54; *Herrmann*, in: BeckOK InfoMedienR, Rn. 12; *Fricke*, in: Wandtke/Bullinger, UrhR, KUG, § 22, Rn. 9; *Specht*, in: Dreier/Schulze/Specht, UrhR, KUG, § 22, Rn. 10.

458 *Engels*, in: BeckOK UrhR, KUG, § 22, Rn. 54; *Herrmann*, in: BeckOK InfoMedienR, KUG, § 22, Rn. 12.

459 So auch *Piltz,* Soziale Netzwerke im Internet, S. 193 ff., 200.

460 *Dreier*, in: Dreier/Schulze/Specht, UrhR, UrhG, § 15, Rn. 43; *Heerma*, in: Wandtke/Bullinger, UrhR, UrhG, § 15, Rn. 25; *Wiebe*, in: Spindler/Schuster, Recht der elektronischen Medien, UrhG, § 15, Rn. 12.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

reicht eine rein technische Verbundenheit nicht aus.[461] Für das Merkmal der Öffentlichkeit gibt es keine festgelegten Zahlengrenzen, jedoch wird man davon ausgehen können, dass mit steigender Anzahl von Personen die innere Verbundenheit der Personen zueinander oder zu demjenigen, der das Bildnis zugänglich macht, umso weniger gegeben ist.[462] Deswegen wird teilweise die Zahlengrenze von über 100 Personen als Anhaltspunkt dafür genannt, wann man von einer inneren Verbundenheit nicht mehr ausgehen kann.[463] Zudem muss die innere Verbundenheit desjenigen, der das Foto hochlädt, zu all seinen „Freunden" im sozialen Netzwerk bestehen.[464]

Die innere Verbundenheit eines Nutzers eines sozialen Netzwerks zu all seinen mit ihm verbundenen Kontakten erscheint damit sehr fraglich.[465] Es ist durchaus üblich, dass Nutzer in sozialen Netzwerken mit einer Anzahl von anderen Nutzern im drei- bis vierstelligen Bereich verbunden sind. Dass darunter zumindest einige sind, mit denen der Nutzer nicht in engem Kontakt steht oder die er nicht persönlich kennt, ist ebenfalls Usus.

Darüber hinaus besteht die Gefahr, dass das Foto mittels weniger Klicks an Personen außerhalb dieses Personenkreises weitergeleitet werden kann. Zwar erscheint es in Einzelfällen durchaus denkbar, dass ein Nutzer nur mit wenigen, sorgfältig ausgewählten Kontakten vernetzt ist. In den meisten Fällen jedoch wird eine innere Verbundenheit nach den dargestellten Kriterien abzulehnen sein. Das spricht für die im Einzelfall widerlegbare Vermutung, dass auch das Einstellen von Fotos in sozialen Netzwerken, die nur den eigenen Kontakten sichtbar gemacht werden, unter die Regelung des § 22 S. 1 KUG fallen.

In diesen Fällen überschneiden sich also die sachlichen Anwendungsbereiche des KUG mit dem BDSG sowie der DSGVO.[466]

---

461 *Dreier*, in: Dreier/Schulze/Specht, UrhR, UrhG, § 15, Rn. 43; *Wiebe*, in: Spindler/Schuster, Recht der elektronischen Medien, UrhG, § 15, Rn. 12; *Heerma,* in: Wandtke/Bullinger, UrhR, UrhG, § 15, Rn. 26.

462 *Heerma,* in: Wandtke/Bullinger, UrhR, UrhG, § 15, Rn. 27; *Dreier*, in: Dreier/Schulze/Specht, UrhR, UrhG, § 15, Rn. 43; *OLG München,* Urt. v. 28.11.1985, Az. 6 U 4440/84, ZUM 1986, 482, 483.

463 *Heerma,* in: Wandtke/Bullinger, UrhR, UrhG, § 15, Rn. 27.

464 *Dreier*, in: Dreier/Schulze/Specht, UrhR, UrhG, § 15, Rn. 43.

465 So auch *Specht*, in: Dreier/Schulze/Specht, UrhR, KUG, § 22, Rn. 10; *Heerma,* in: Wandtke/Bullinger, UrhR, UrhG, § 15, Rn. 26.

466 Vgl. Kap. 3 Pkt. A.I.2, S. 95.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

3. Verhältnis KUG und BDSG

Da sich, wie gezeigt, der sachliche Anwendungsbereich von KUG und BDSG in den Fällen, in denen ein Nutzer ein Foto eines anderen in einem sozialen Netzwerk hochlädt oder teilt, überschneidet, muss geklärt werden, welche Regelungen in diesem Fall Anwendung finden.

a) KUG als Spezialgesetz

Damit der Subsidiaritätsgrundsatz greift, müsste das KUG lex specialis zum BDSG sein. Dazu müssen sich nicht nur die sachlichen Anwendungsbereiche überschneiden, das KUG müsste auch i. S. d. § 1 Abs. 3 S. 1 BDSG auf personenbezogene Daten anzuwenden sein.

Schutzgut der §§ 22 ff. KUG ist das Recht am eigenen Bild als Ausprägung des allgemeinen Persönlichkeitsrechts i. S. d. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.[467] BDSG und KUG verfolgen im Schutz von (im Falle des KUG: bestimmten) personenbezogenen Daten also denselben Zweck. Teilweise wird der Vorrang des KUG mit dem Argument abgelehnt, dass das KUG nur Verarbeitungsvorgänge, nicht jedoch personenbezogene Datenverarbeitung ausdrücklich voraussetze.[468] Dies kann jedoch nicht überzeugen, da § 22 S. 1 KUG mit dem Merkmal der Erkennbarkeit eine dem Merkmal der Bestimmbarkeit i. S. d. § 3 Abs. 1 BDSG identische Voraussetzung enthält. Zudem regelt § 22 S. 1 KUG, wie gezeigt, eindeutig die Verarbeitung eines personenbezogenen Datums, nämlich eines Bildnisses einer Person.

Damit gehen in sozialen Netzwerken die Regelungen der §§ 22 ff. KUG den Regelungen des BDSG grundsätzlich vor, soweit es sich um die Verbreitung oder öffentliche Zurschaustellung von Bildnissen anderer Personen handelt.[469]

---

467 *Herrmann*, in: BeckOK InfoMedienR, KUG, § 22, Rn. 3; *Fricke*, in: Wandtke/Bullinger, UrhR, KUG, § 22, Rn. 1; *Engels*, in: BeckOK UrhR, KUG, § 22, Rn. 5.

468 *Dix*, in: Simitis, BDSG, § 1, Rn. 170, Fn. 385 a. E.

469 *BAG,* Urt. v. 11.12.2014, 8 AZR 1010/13, NJW 2015, 2140, 2141, Rn. 16; *Renner*, ZUM 2015, 608, 609; einschränkend *Lorenz*, ZD 2012, 367, 369.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Ansätze zur Auflösung des Spannungsverhältnisses

Problematisch an diesem Ergebnis ist allerdings, dass hierdurch Wertungswidersprüche entstehen: Während das Hochladen und Teilen von Informationen – mangels Erlaubnisnormen[470] – unter dem Schutz des § 4a BDSG steht, greifen für Bildnisse die weniger schützenden Bestimmungen über die Einwilligung i. S. d. KUG. Auch wenn das Schriftformerfordernis des § 4a Abs. 1 S. 3 BDSG nach hier vertretener Ansicht i. S. d. § 4a Abs. 1 S. 3 Hs. 2 BDSG bei der Datenverarbeitung in sozialen Netzwerken nicht greift[471], führt dies zumindest auf dem Gebiet der freien Widerruflichkeit der Einwilligung zu einem Spannungsverhältnis. So besteht bei dem Verbreiten von Informationen über Andere in sozialen Netzwerken ein größerer Schutz als beim Verbreiten von Fotos. Wäre dies etwa bei dem Verbreiten der Heimadresse eines anderen Nutzers noch durchaus nachvollziehbar, wird das Spannungsverhältnis offenbar, wenn man sich vor Augen führt, dass somit auch die Veröffentlichung einer E-Mail-Adresse unter stärkerem Schutz steht als die Veröffentlichung von möglicherweise kompromittierenden „Partyfotos".

aa) Übertragbarkeit der Grundsätze des BDSG auf das KUG und vice versa

Wegen dieses Spannungsverhältnisses wird teilweise vertreten, dass die Anforderungen an die Einwilligung des BDSG auf das KUG zu übertragen seien. Zur Begründung wird einerseits angeführt, dass das KUG keine eigenständigen Regelungen über die Einwilligung enthalte und es insofern nicht abschließend sei.[472] Dies kann aber nicht überzeugen. Die Einwilligung nach dem KUG unterliegt, wie dargestellt, klaren Anforderungen. Eine Regelungslücke für die die Regelungen des BDSG heranzuziehen seien,[473] besteht demnach nicht.

Ebenfalls nicht zielführend erscheinen Überlegungen, wonach die Grundsätze des KUG für bestimmte Verarbeitungsschritte auf das BDSG zu übertragen seien. Hierfür wird angeführt, dass das KUG nur die Verbrei-

470 Vgl. Kap. 3 Pkt. A.III.2.a, S. 113.
471 Vgl. Kap. 3 Pkt. A.III.3.a.cc, S. 138.
472 *Lorenz*, ZD 2012, 367, 369; i. E. ähnlich *Jandt/Roßnagel*, MMR 2011, 637, 640.
473 So *Lorenz*, ZD 2012, 367, 369.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

tung und öffentliche Zurschaustellung regele, nicht jedoch auf „nötige Zwischenschritte“ wie die Aufnahme oder das Speichern des Fotos.[474] Damit sei jedoch die Einwilligung nach dem KUG zur Verbreitung oder öffentlichen Zurschaustellung wirkungslos, wenn die Einwilligung zur Herstellung des Bildnisses wesentlich strengeren Anforderungen unterliege.[475] Dass die Herstellung ein „Zwischenschritt“ zur öffentlichen Zurschaustellung sei, kann schon nicht gänzlich überzeugen. Fotos, die der Betroffene von sich selbst hergestellt hat, wie etwa sog. Selfies, wären davon schon nicht erfasst. Zudem lässt sich mit diesem Argument noch nicht eine Absenkung des klar gesetzlich geregelten Schutzes für nicht vom KUG erfasste Verarbeitungsschritte rechtfertigen.

bb) Verfassungskonforme Auslegung des KUG

Das Spannungsverhältnis ließe sich jedoch über eine verfassungskonforme Auslegung des KUG auflösen. Die ex-nunc Widerrufsmöglichkeit im BDSG ist nicht einfachgesetzlich geregelt, sondern ergibt sich aus dem Recht auf informationelle Selbstbestimmung.[476] Der Betroffene soll die Hoheit über den Umgang mit personenbezogenen Daten beibehalten.[477] Wenn dies aber für den Widerruf zur Einwilligung für das Hochladen und Teilen von Informationen Anderer gilt, muss dies auch für die Einwilligung für das Hochladen und Teilen von Bildnisses Anderer gelten. Dass auch der datenschutzrechtliche Widerruf an bestimmte Voraussetzungen geknüpft ist – insbesondere darf die Verarbeitung dem Betroffenen objektiv nicht mehr zumutbar sein und den Interessen des Verantwortlichen muss ausreichend Rechnung getragen werden –[478], führt zu einem angemessenen Ausgleich der Interessenlagen.

Etwas Anderes gilt für das Schriftformerfordernis aus § 4a Abs. 1 S. 3 BDSG.[479] Denn das Recht auf informationelle Selbstbestimmung ist auch gewahrt, sofern die Einwilligung mündlich oder elektronisch erklärt wird.

---

474 *Schnabel*, ZUM 2008, 657, 661; *Renner*, ZUM 2015, 608, 609 f.
475 *Schnabel*, ZUM 2008, 657, 661.
476 *Simitis,* in: Simitis, BDSG, § 4a, Rn. 94 f.; *Taeger,* in: Taeger/Gabel, BDSG, § 4a, Rn. 81 f.; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 31.
477 *Simitis,* in: Simitis, BDSG, § 4a, Rn. 94.
478 *Simitis,* in: Simitis, BDSG, § 4a, Rn. 98; 101.
479 So aber *BAG,* Urt. v. 11.12.2014, 8 AZR 1010/13, NJW 2015, 2140, Rn. 26, allerdings im Falle von Arbeitsverhältnissen.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Von den inhaltlichen Anforderungen an die Einwilligung wird dadurch nicht abgerückt.[480]

4. Verhältnis KUG und DSGVO

Die zuvor erörterten Abgrenzungsprobleme und -lösungen werden künftig nicht mehr in selbem Maße bestehen. Denn mit Gültigkeit der DSGVO ab dem 28. Mai 2018 werden die Bestimmungen der DSGVO das KUG (und freilich auch das BDSG) verdrängen. Gem. Art. 2 Abs. 1 DSGVO gilt die „[…] Verordnung […] für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten […]". Dabei gleicht der Begriff des personenbezogenen Datums aus Art. 4 Nr. 1 DSGVO dem aus § 3 Abs. 1 BDSG bzw. Art. 2 lit. a DSRL. Wie schon bei BDSG und KUG überschneiden sich die sachlichen Anwendungsbereiche also.[481] Anders als das BDSG enthält die DSGVO jedoch keine Subsidiaritätsklausel. Sie verdrängt das KUG demnach. Zwar enthält die DSGVO zahlreiche Öffnungsklauseln, die dem nationalen Gesetzgeber Regelungsspielräume einräumen,[482] diese betreffen größtenteils jedoch die Datenverarbeitung im öffentlichen Interesse. Einzig die Öffnungsklausel des Art. 6 Abs. 4 DSGVO i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 DSGVO könnte als Öffnungsklausel für die §§ 22 ff. KUG herangezogen werden.[483] Mit dieser Auslegung der Öffnungsklausel könnten jedoch beinahe alle nationalen Regelungen zur Datenverarbeitung im privaten Bereich aufrechterhalten werden und den Anspruch der DSGVO, den Datenschutz unionsweit einheitlich und umfassend zu regeln, konterkarieren. Eine derart extensive Auslegung ist daher abzulehnen.

Die DSGVO sieht, anders als das BDSG, für die Einwilligung kein Schriftformerfordernis mehr vor und regelt die Widerrufsmöglichkeit gem. Art. 7 Abs. 3 S. 1 DSGVO ausdrücklich. Auch behandelt das DSGVO Informationen oder Bildnisse nicht getrennt. Die Verarbeitung von Fotos richtet sich, ebenso wie die Verarbeitung von Informationen, zunächst nach Art. 6 Abs. 1 DSGVO.

---

480 Vgl. ausführlich zum Schriftformerfordernis Kap. 3 Pkt. A.III.3.cc, S. 138.

481 Vgl. Kap. 3 Pkt. A.IV.2, S. 145.

482 Vgl. ausführlich *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht; *Roßnagel*, Europäische Datenschutz-Grundverordnung.

483 Kritisch *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 428 ff.; S. 43 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Die Unsicherheiten, die sich aus den unterschiedlichen Vorgaben des KUG und des BDSG bisher ergaben, werden künftig also beseitigt sein.

V. Zusammenfassung

Die Verarbeitung im Nutzer-Nutzer-Verhältnis in sozialen Netzwerken unterliegt abgesehen von wenigen Ausnahmen nicht der Privilegierung für ausschließlich persönliche oder familiäre Tätigkeiten. Andernfalls wäre trotz eines potenziell sehr großen Empfängerkreises jegliche Verarbeitung im Nutzer-Nutzer-Verhältnis vom sachlichen Anwendungsbereich des BDSG bzw. der DSGVO ausgeschlossen und unterläge nicht den dort vorgesehenen Bestimmungen zum Schutz personenbezogener Daten.

Für den umfassenden Umgang mit personenbezogenen Daten in sozialen Netzwerken im Nutzer-Nutzer-Verhältnis findet sich nach aktuellem Recht kein Zulässigkeitstatbestand, sodass als Legitimationsmittel meist auf die Einwilligung zurückgegriffen werden muss. Durch das teilweise sehr streng verstandene Schriftformerfordernis des BDSG unterliegt die Einwilligung jedoch formellen Anforderungen, die in der Nutzerrealität regelmäßig nicht erfüllt werden. Zwar sieht das BDSG eine Ausnahme vom Schriftformerfordernis bei Vorliegen besonderer Umstände vor und solche besonderen Umstände stellt der Umgang mit personenbezogenen Daten im Nutzer-Nutzer-Verhältnis in sozialen Netzwerken dar. Allerdings bleibt wegen des Ausnahmecharakters der Vorschrift eine gewisse Rechtsunsicherheit für die verarbeitenden Nutzer bestehen. Zudem unterliegt der Umgang mit Bildnissen nicht den Vorgaben des BDSG, sondern den weniger strengen Vorgaben des KUG. Dieses Spannungsverhältnis kann durch eine verfassungskonforme Auslegung der entsprechenden Vorgaben des KUG aufgelöst werden.

Die DSGVO stellt mit Art. 6 Abs. 1 S. 1 lit. f DSGVO einen Erlaubnistatbestand bereit, der sehr weit ausgelegt werden kann. Richtigerweise muss bei der in dieser Norm vorgesehenen Interessenabwägung jedoch das Betroffeneninteresse dann überwiegen, wenn es sich um die Verarbeitung personenbezogener Daten handelt, die nicht allgemein zugänglich sind. Auch unter der DSGVO wird das Hauptlegitimationsmittel also die Einwilligung sein. Die DSGVO stellt keine formellen Anforderungen an die Einwilligung; allerdings muss der Verantwortliche die Einwilligung nachweisen. Dieser Nachweis könnte ihm jedoch auch gelingen, wenn die Einwilligung per E-Mail o. ä. erteilt wurde. Dies stellt eine den tatsächlichen Gegebenheiten angepasste und damit begrüßenswerte Neuerung dar. Zudem wird die

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

nach deutschem Recht teilweise schwierige Abgrenzung zwischen BDSG und vorrangigen bereichsspezifischen Regelungen unter dem Regime der DSGVO nicht mehr in selbem Maße geben. Allerdings bergen die nicht näher ausformulierten Zulässigkeitstatbestände des Art. 6 DSGVO die Gefahr, dass das in Art. 6 Abs. 1 DSGVO angelegte Verbot mit Erlaubnisvorbehalt durch eine allzu weit verstandene Interpretation durch die Verantwortlichen umgangen wird. Hier ist auf einen raschen Entwurf von Leitlinien durch den europäischen Datenschutzausschuss i. S. d. Art. 70 Abs. 1 S. 1 lit. e DSGVO zur Auslegung des Art. 6 Abs. 1 S. 1 lit. f DSGVO zu hoffen. Zudem sind die Aufsichtsbehörden und die Rechtsprechung gefordert, um Art. 6 Abs. 1 S. 1 lit. f DSGVO Kontur zu geben.

B. Zulässigkeit der Verarbeitung personenbezogener Daten im Anbieter-Nutzer-Verhältnis

Im Folgenden wird die Zulässigkeit der Verarbeitung personenbezogener Daten durch die Plattformbetreiber analysiert. Dabei muss zunächst das sachlich anwendbare Recht analysiert werden, bevor in einem nächsten Schritt die Zulässigkeit nach den sachlich anwendbaren Normen bewertet wird. Insbesondere wird zwischen der Datenverarbeitung mittels Tracking Tools und der Verarbeitung weiterer Daten zu unterscheiden sein. Schließlich wird aufgezeigt, dass auch bei der Datenverarbeitung durch Plattformbetreiber die Einwilligung ein wichtiges Legitimationsmittel darstellt. Hierbei muss ein besonderes Augenmerk auf die Freiwilligkeit der Einwilligung unter dem Aspekt marktmächtiger Plattformbetreiber gelegt werden.

I. Gesetzliche Erlaubnistatbestände

1. Sachlich anwendbares Recht

a) Sachlich anwendbares Recht im deutschen Datenschutzrecht

Im Folgenden wird die sachliche Anwendbarkeit deutscher datenschutzrechtlicher Vorschriften analysiert. Hierzu sind zunächst die einschlägigen Normen zur Bewertung der Zulässigkeit des Umgangs mit personenbezogenen Daten zu benennen. In einem ersten Schritt müssen dazu die Zuläs-

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

sigkeitstatbestände des TMG von Zulässigkeitstatbeständen des BDSG abgrenzt werden, da Normen des TMG dem BDSG wegen des Subsidiaritätsgrundsatzes des BDSG, § 1 Abs. 3 S. 1 BDSG, vorgehen.

aa) Grundsätzliche Unterschiede der Zulässigkeitsnormen

Für die Anwendbarkeit der datenschutzrechtlichen Regelungen des TMG müsste gem. § 11 TMG zunächst zwischen dem Plattformbetreiber und dem Nutzer ein Anbieter-Nutzer-Verhältnis i. S. d. TMG bestehen. Gem. § 2 S. 1 Nr. 1 TMG „[…] ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt […]". Die Plattformbetreiber halten unstreitig Telemedien zur Nutzung bereit. Ebenso sind die registrierten Nutzer eines sozialen Netzwerks problemlos als Nutzer i. S. d. § 11 Abs. 2, § 2 S. 1 Nr. 3 TMG zu klassifizieren. Damit sind die Regelungen der §§ 11 ff. TMG grundsätzlich anwendbar.

§ 12 Abs. 1 TMG regelt ein Verbotsprinzip mit Erlaubnisvorbehalt. Danach darf der Diensteanbieter „[…] personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat […]". Gem. § 12 Abs. 3 TMG sind jedoch die Vorschriften für den Schutz personenbezogener Daten – also insbesondere das BDSG – ergänzend heranzuziehen, soweit das TMG keine Regelungen trifft.[484] §§ 14 f. TMG regeln insbesondere die Zulässigkeit der Erhebung und Verwendung sog. Bestands- und Nutzungsdaten. Weitere Erlaubnistatbestände für den Umgang mit anderen Datenkategorien sieht das TMG nicht vor.

Die Abgrenzung zwischen den Erlaubnisnormen des TMG und denen des BDSG könnte deswegen von Bedeutung sein, weil das TMG in §§ 14 f. TMG für die Erhebung und Verwendung personenbezogener Daten einen Erforderlichkeitsgrundsatz ohne Abwägungsmöglichkeiten im Einzelfall vorsieht. Damit sind die Vorgaben der §§ 14 f. TMG deutlich strenger als die Erlaubnistatbestände der §§ 28 ff. BDSG. In Folge dessen beschäftigte sich die Literatur in der Vergangenheit intensiv mit dem sachlichen Anwendungsbereich für die verschiedenen Arten des Umgangs mit personenbezogenen Daten durch die Plattformbetreiber. Die Klassifikation der in Frage stehenden personenbezogenen Daten als Bestands- und Nutzungsdaten

484 Vgl. auch *Heckmann*, in: Heckmann, jurisPK-Internetrecht, Kap. 9, Rn. 232.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

gem. § 14 bzw. § 15 TMG und den übrigen anfallenden personenbezogenen Daten – sog. Inhaltsdaten[485] – könnte damit ganz entscheidend für die Beurteilung der Zulässigkeit des Umgangs mit personenbezogenen Daten sein. Insbesondere die sachliche Anwendbarkeit des TMG oder des BDSG auf Inhaltsdaten war umstritten, da diese im TMG nicht eigenständig geregelt sind.[486]

bb) Unvereinbarkeit der § 14 Abs. 1 und § 15 Abs. 1 TMG mit der DSRL

Jüngst hat die dargestellte Diskussion mit dem Urteil des *EuGH* im Fall *Breyer*[487] an Brisanz verloren. In dem Urteil führt der *EuGH* aus, dass „[…] Art. 7 Buchst. f der Richtlinie 95/46 einen Mitgliedstaat daran hindert, kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten auszuschließen, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen."[488] Da nach § 15 Abs. 1 TMG eine Interessenabwägung nicht möglich ist, hat dieser eine geringere Tragweite als Art. 7 lit. f DSRL.[489] Der *EuGH* bewegt sich mit dieser Auslegung des Art. 7 DSRL ganz auf einer Linie seiner *ASNEF und FECEMD*-Entscheidung[490], in der der *Gerichtshof* bereits festgestellt hat, dass Art. 7 DSRL eine erschöpfende Liste von Erlaubnistatbeständen vorsieht, die weder ein Abweichen im Schutzniveau „nach unten", noch „nach oben" zulässt[491] und damit die vollharmonisierende Wirkung der DSRL bestätigte.[492] Bereits nach der *ASNEF und FECEMD*-Entscheidung hätte damit deutlich sein müssen, dass § 15 Abs. 1

485 Vgl. Kap. 3 Pkt. B.I.1.a.dd.iii, S. 160.
486 Vgl. *Bauer*, MMR 2008, 435; *Kühnl,* Persönlichkeitsschutz 2.0, S. 146 ff; *Achtruth,* Der rechtliche Schutz bei der Nutzung von Social Networks, S. 71 ff.; *Heckmann*, in: Heckmann, jurisPK-Internetrecht, Kap. 9, Rn. 380 ff.; *Zscherpe*, in: Taeger/Gabel, BDSG, TMG, § 14, Rn. 21 ff.
487 *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779 – Breyer.
488 *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779, Rn. 62 – Breyer.
489 *EuGH,* Urt. v. 19.10.2016, Rs. C-582/14, ECLI:EU:C:2016:779, Rn. 59 f. – Breyer.
490 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181 – ASNEF und FECEMD.
491 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 30, 32 – ASNEF und FECEMD.
492 Dazu *Kühling*, EuZW 2012, 281; ausführlich *Raab,* Die Harmonisierung des einfachgesetzlichen Datenschutzes, S. 32 ff.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

TMG nicht den europarechtlichen Vorgaben entspricht.[493] Nunmehr ist diese Frage ausdrücklich entschieden, sodass kein Spielraum mehr für eine anderweitige Interpretation verbleibt.

Die Ergebnisse der Entscheidungen lassen sich ebenso auf § 14 Abs. 1 TMG übertragen. Gem. Art. 7 lit. b DSRL ist die Datenverarbeitung zulässig, soweit sie „[…] erforderlich [ist] für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist […]". Art. 7 lit. b DSRL sieht keine Interessenabwägung vor; zunächst scheint § 14 Abs. 1 TMG demnach nicht mit den Vorgaben des Art. 7 lit. b DSRL in Konflikt zu treten. Allerdings ist gem. § 14 Abs. 1 TMG die Erhebung und Verwendung von Bestandsdaten „nur" zulässig zur Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses. Ein alternativer Erlaubnistatbestand zur Verwirklichung berechtigter Interessen des Verarbeiters, wie Art. 7 lit. f DSRL ihn vorsieht, ist damit ausgeschlossen.[494]

Wegen des eindeutigen Wortlauts des § 14 Abs. 1 TMG sowie des § 15 Abs. 1 TMG kommt eine richtlinienkonforme Auslegung nicht in Betracht.[495]

cc) Konsequenzen der Unvereinbarkeit mit der DSRL

Fraglich sind die Konsequenzen dieser Feststellung. Zahlreiche Autoren plädieren für eine unmittelbare Anwendbarkeit von Art. 7 lit. f DSRL[496], wobei vereinzelt auf die Problematik hingewiesen wird, dass dies in den meisten Sachverhalten eine unmittelbare Horizontalwirkung[497] der Richtlinie bedeuten würde.[498] Dass die Norm für eine unmittelbare Anwendbarkeit

493 Vgl. bereits die Ausführungen bei *Raab,* Die Harmonisierung des einfachgesetzlichen Datenschutzes, S. 15 f.; *Kühling/Klar*, ZD 2017, 24, 29.

494 Ebenso *Raab,* Die Harmonisierung des einfachgesetzlichen Datenschutzes, S. 122 f.

495 *Moos/Rothkegel*, MMR 2016, 842, 847; *Raab,* Die Harmonisierung des einfachgesetzlichen Datenschutzes, S. 123.

496 Dahingehend wohl *Mantz/Spittka*, NJW 2016, 3579, 3583; *Richter*, EuZW 2016, 909, 914; *Raab,* Die Harmonisierung des einfachgesetzlichen Datenschutzes, S. 123 f.

497 Weiterführend hierzu vgl. etwa *Schroeder*, in: Streinz, EUV/AEUV, Art. 288 AEUV, Rn. 116.

498 *Mantz/Spittka*, NJW 2016, 3579, 3583.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

hinreichend genau ist, hat der *EuGH* bereits in seiner *ASNEF und FECEMD*-Entscheidung klargestellt.[499] Vorzugswürdig erscheint jedoch ein Rückgriff auf die Erlaubnistatbestände im BDSG, insbesondere die §§ 28 f. BDSG.[500] Denn die unmittelbare Anwendbarkeit einer Richtliniennorm setzt nicht nur ihre hinreichende Genauigkeit voraus, sondern auch ihre nicht fristgemäße oder unzureichende Umsetzung in nationales Recht.[501] Allerdings bestehen im BDSG mit §§ 28 f. BDSG Normen, die mit Art. 7 lit. f DSRL vereinbar sind: Anders als §§ 14 f. TMG lassen die §§ 28 f. BDSG gerade Raum für eine Interessenabwägung im Einzelfall. Die Normen der §§ 14 f. TMG sind auch deckungsgleich[502] zu den §§ 28 f. BDSG; andernfalls wäre bereits der Subsidiaritätsgrundsatz des BDSG nicht zum Tragen gekommen. Damit bestehen im deutschen Datenschutzrecht Umsetzungsnormen, die den Anforderungen des Art. 7 DSRL entsprechen. Da unionsrechtswidrige Normen von mitgliedstaatlichen Stellen unangewendet bleiben müssen,[503] können §§ 14 Abs. 1 und 15 Abs. 1 TMG dem BDSG nicht mehr vorgehen.

Eine unmittelbare Anwendbarkeit des Art. 7 lit. f DSRL ist damit ausgeschlossen. Stattdessen sind die Normen des BDSG heranzuziehen.

dd) Klassifikation als Bestands-, Nutzungs-, oder Inhaltsdatum

Die Einordnung in Bestands-, Nutzungs-, oder Inhaltsdatum hat demnach deutlich an Relevanz verloren. Wegen der ausgeprägten Diskussion über die Behandlung von sog. „Inhaltsdaten“ wird gleichwohl nachfolgend ein kurzer Überblick Aufschluss über die unterschiedlichen Kriterien zur Einordnung der Daten und der Zulässigkeit des Umgangs mit diesen Daten geben.

---

499 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 50 ff. – ASNEF und FECEMD.

500 *Moos/Rothkegel*, MMR 2016, 842, 846 f.

501 *Schroeder*, in: Streinz, EUV/AEUV, Art. 288 AEUV, Rn. 107.

502 Zum Begriff vgl. *Schmidt*, in: Taeger/Gabel, BDSG, § 1, Rn. 34; *Dix*, in: Simitis, BDSG, § 1, Rn. 170; zum Vorrang von bereichsspezifischen Regelungen vgl. auch Kap. 3 Pkt. A.IV.2, S. 145.

503 *Schroeder*, in: Streinz, EUV/AEUV, Art. 288 AEUV, Rn. 120 m. w. N.; i. Ü. gilt dies auch soweit die nationalen Gerichte die Normen für unionsrechtswidrig halten, vgl. *EuGH,* Urt. v. 19.01.2010, Rs. C-555/07, ECLI:EU:C:2010:21, Rn. 51 ff. – Kükükdeveci.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

i) Bestandsdaten

Bestandsdaten sind nach der Legaldefinition des § 14 Abs. 1 TMG solche Daten, die zur „[…] Begründung, inhaltliche[n] Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind […]". Die Bewertung der Erforderlichkeit hängt dabei vom konkreten Nutzungsverhältnis ab.[504] Bei einem sozialen Netzwerk kommen als für das Vertragsverhältnis[505] erforderliche Daten etwa eine E-Mail-Adresse zur Authentifikation sowie ein Nutzername in Betracht.[506] Auch können der Klarname, die Adresse und bei kostenpflichtigen sozialen Netzwerken bzw. kostenpflichtigen Funktionen in sozialen Netzwerken auch die Bankdaten als Bestandsdaten gelten.[507] An dem strengen Erforderlichkeitskriterium des § 14 Abs. 1 TMG wird klar, dass regelmäßig nicht alle von sozialen Netzwerken bei der Registrierung standardmäßig abgefragte Daten als Bestandsdatum gelten können. Dies wird etwa bei der von vielen sozialen Netzwerken verpflichtenden Angabe des Geschlechts deutlich. Zwar könnte diese Information beispielsweise für Online-Partnerbörsen ein Bestandsdatum darstellen.[508] Bei sozialen Netzwerken hingegen, deren Geschäftsmodell nicht das Kennenlernen der Nutzer untereinander ist, sondern die virtuelle Vernetzung von bereits im echten Leben bestehenden Bekanntschaften, ist die Erforderlichkeit der Geschlechtsangabe für das Vertragsverhältnis schwerlich begründbar.

---

504 *Heckmann*, in: Heckmann, jurisPK-Internetrecht, Kap. 9, Rn. 383.

505 An das Vorliegen eines Vertragsverhältnisses sind indes keine allzu hohen Anforderungen zu stellen. So wird der beidseitige Rechtsbindungswille regelmäßig bei der Registrierung in einem sozialen Netzwerk einerseits und der Bereitstellung des Accounts für den Nutzer durch den Plattformbetreiber andererseits gegeben sein, vgl. *Heckmann*, in: Heckmann, jurisPK-Internetrecht, Kap. 9, Rn. 378; *Achtruth,* Der rechtliche Schutz bei der Nutzung von Social Networks, S. 84 f.; *Kühnl,* Persönlichkeitsschutz 2.0, S. 145.

506 *Kühnl,* Persönlichkeitsschutz 2.0, S. 145; freilich handelt es sich nur um personenbezogene Daten sofern die dahinter stehende natürliche Person bestimmt oder bestimmbar i. S. d. § 3 Abs. 1 BDSG ist.

507 *Heckmann*, in: Heckmann, jurisPK-Internetrecht, Kap. 9, Rn. 386; *Bauer*, MMR 2008, 435, 436.

508 *Achtruth,* Der rechtliche Schutz bei der Nutzung von Social Networks, S. 91 f., der allerdings die Angabe des Geschlechts für alle sozialen Netzwerke als erforderlich erachtet.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ii) Nutzungsdaten

Nach der Legaldefinition des § 15 Abs. 1 S.1 TMG sind Nutzungsdaten solche Daten, die erforderlich sind, „[…] um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen […]", insbesondere „[…] Merkmale zur Identifikation des Nutzers […]", „[…] Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung […]" und „[…] Angaben über die vom Nutzer in Anspruch genommenen Telemedien […]", § 15 Abs. 1 S. 2 TMG. Damit könnten insbesondere mittels Tracking Tools aufgezeichnete Daten wie IP-Adressen als Nutzungsdaten kategorisiert werden. Allerdings ist auch hierbei der Erforderlichkeitsgrundsatz zu beachten.

iii) Inhaltsdaten

Zuletzt sind Bestands- und Nutzungsdaten von sog. Inhaltsdaten abzugrenzen. Dieser Begriff ist im TMG nicht definiert und meint die personenbezogenen Daten, die ohne Bestands- oder Nutzungsdatum zu sein bei der Interaktion des Diensteanbieters mit dem Nutzer anfallen.[509] Dies betrifft insbesondere die freiwilligen Angaben der Nutzer in sozialen Netzwerken, die diese in ihr Profil eintragen[510] sowie die Interaktion der Nutzer untereinander wie etwa Pinnwandeinträge[511].

Fraglich ist jedoch, nach welchen Normen die Zulässigkeit des Umgangs mit Inhaltsdaten zu bewerten ist, da diese nicht explizit im TMG geregelt sind. Insbesondere für den Fall von sozialen Netzwerken wird teilweise vertreten, dass solche freiwilligen Daten als Unterfall der Nutzungsdaten zu werten seien, mithin auch hierfür das TMG anzuwenden sei.[512] Zur Begründung wird angeführt, dass die Daten in direktem Zusammenhang mit der Erbringung des Telemediendienstes stünden und dass sich die gesamte Datenerhebung und -verwendung online und im Rahmen des Telemediendienstes abspiele.[513]

Allerdings widerspricht dies der Legaldefinition des Nutzungsdatums in § 15 Abs. 1 TMG. Nutzungsdaten i. S. d. Norm sind solche, die zur Ermöglichung der Inanspruchnahme von Telemedien erforderlich sind. Dies trifft

509 Vgl. *Zscherpe*, in: Taeger/Gabel, BDSG, TMG, § 14, Rn. 20.
510 *Heckmann*, in: Heckman, jurisPK-Internetrecht, Kap. 9, Rn. 382.
511 *Kühnl,* Persönlichkeitsschutz 2.0, S. 147.
512 *Bauer*, MMR 2008, 435, 436.
513 *Bauer*, MMR 2008, 435, 436.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

auf die freiwillige Bereitstellung von Nutzerinformationen und auf die Interaktion der Nutzer miteinander nicht zu. Stehen diese freiwillig bereitgestellten Daten zwar freilich in Zusammenhang mit der Inanspruchnahme der Telemedien, sind sie doch nicht erforderlich, um die Inanspruchnahme von Telemedien zu *ermöglichen*.

Als weiteres Gegenargument wird teilweise die Formulierung des § 12 Abs. 1 TMG angeführt, der sich auf „die Bereitstellung von Telemedien" bezieht; die Durchführung ist nach dieser Ansicht vom Begriff der Bereitstellung zu trennen und explizit im TMG nicht geregelt.[514] Dem kann allerdings entgegengehalten werden, dass die Vorgängervorschrift, § 3 Abs. 1 TDDSG, ebenda die „Durchführung von Telediensten" regelte. Die Änderung zum Begriff „Bereitstellung" sollte vielmehr klarstellen, dass die Regelungen des TMG auch zum Tragen kommen, wenn der Dienst nicht in Anspruch genommen wird.[515] Abgesehen davon sollte § 12 TMG ausweislich der Gesetzesbegründung jedoch die bisherigen Datenschutzgrundsätze von TDDSG[516] und MDStV[517] übernehmen.[518] Dies spricht dagegen, dass der begriffliche Wechsel eine inhaltliche Änderung darstellen sollte.

Überzeugender ist hingegen die Feststellung, dass die Frage, ob Inhaltsdaten vom Regelungsbereich des TDDSG umfasst sind, bereits bei Erlass des TMG stark diskutiert war und der Gesetzgeber dennoch keine eindeutige Regelung zu Inhaltsdaten im TMG aufgenommen hat.[519] Dies spricht dagegen, dass diese Daten vom TMG umfasst sein sollten.

Schließlich wird als weiteres Argument gegen eine Einordnung von Inhaltsdaten unter das Regime des TMG angeführt, dass dann auch die Löschpflicht des § 13 Abs. 4 Nr. 2 TMG zum Tragen komme; eine unmittelbare Löschung der Inhaltsdaten nach Ablauf des Zugriffs widerspricht jedoch gerade dem Zweck der Kommunikation in sozialen Netzwerken.[520]

---

514 *Achtruth,* Der rechtliche Schutz bei der Nutzung von Social Networks, S. 82.
515 *Moos*, in: Taeger/Gabel, BDSG, TMG, § 12, Rn. 14.
516 Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz - TDDSG) v. 22.07.1997; aufgehoben m. W. v. 01.03.2007 (BGBl. 2007 I, 179).
517 Staatsvertrag über Mediendienste v. 31.01.1997, aufgehoben m. W. v. 01.03.2007.
518 BT-Drucks. 16/13657, S. 16.
519 *Zscherpe*, in: Taeger/Gabel, BDSG, TMG, § 14, Rn. 26 mit Verweis auf *Imhof*, CR 2000, 110 und *Wolber*, CR 2003, 859.
520 *Kühnl,* Persönlichkeitsschutz 2.0, S. 148.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Die besseren Argumente sprechen damit gegen eine Kategorisierung der Inhaltsdaten als Nutzungsdaten. Es kommen daher die Erlaubnistatbestände des BDSG zum Tragen.[521]

ee) Zwischenergebnis

Aufgrund der vollharmonisierenden Wirkung der DSRL sind § 14 Abs. 1 TMG und § 15 Abs. 1 TMG unvereinbar mit der Regelung des Art. 7 DSRL. Der Umgang mit Bestands-, Nutzungs- und Inhaltsdaten richtet sich damit nach den Erlaubnisnormen des BDSG. Ihre Einordnung in eine der drei Kategorien besitzt inzwischen deutlich geringere praktische Relevanz.[522]

b) Sachlich anwendbares Recht unionsrechtlicher Normen

Auch nach der DSGVO wird sich die Einordnung in eine der Kategorien nicht mehr im selben Maße stellen. Denn die DSGVO sieht mit Art. 6 einen einheitlichen Erlaubnistatbestand für all diese Arten personenbezogener Daten vor. Dabei wird die DSGVO, vorbehaltlich gegebenenfalls genutzter Regelungsspielräume im Rahmen der Öffnungsklauseln im nationalen Recht, alle nationalen Normen, die Bestimmungen der DSRL umsetzen, ablösen, also auch datenschutzrechtliche Normen des TMG.[523] Freilich sind je nach Verarbeitungsfall unterschiedliche Erlaubnisnormen innerhalb des Art. 6 Abs. 1 DSGVO einschlägig; allerdings gibt es mit Art. 6 Abs. 1 S. 1 lit. f DSGVO nunmehr eine Auffangnorm, die die Interessenabwägung im Einzelfall vorsieht, auch wenn keiner der anderen Fälle in Art. 6 DSGVO einschlägig ist.

Der Unterschied zu dem Regime des TMG wird an einem Vergleich von § 14 Abs. 1 TMG mit Art. 6 Abs. 1 S. 1 lit. b DSGVO deutlich: So sieht

---

521 Dies entspricht der h. L., vgl. *Zscherpe*, in: Taeger/Gabel, BDSG, TMG, § 14, Rn. 26 m. w. N. in Rn. 40.

522 Vgl. Kap. 3 Pkt. B.I.1.a.dd, S. 158.

523 Ebenso *Keppeler*, MMR 2015, 779; zu beachten gilt allerdings, dass einige Normen des TMG zugleich als Umsetzung von Regelungen der ePrivacy-RL fungieren, die gem. Art. 1 Abs. 2 ePrivacy-RL den Regelungen der DSRL vorgehen und von einer ePrivacy-VO abgelöst werden sollen; vgl. hierzu Kap. 3 Pkt. B.I.3, S. 175.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

zwar auch Art. 6 Abs. 1 S. 1 lit. b DSGVO vor, dass die Verarbeitung rechtmäßig ist, wenn „[…] die Verarbeitung […] für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, […] erforderlich [ist] […]“ und regelt damit zumindest auch Fälle, die bislang unter § 14 Abs. 1 TMG fielen. Gem. Art. 6 Abs. 1 S. 1 DSGVO ist jedoch die Verarbeitung rechtmäßig, wenn „[…] mindestens eine der nachstehenden Bedingungen erfüllt ist […]“, d. h. dass andere Erlaubnistatbestände nicht durch Art. 6 Abs. 1 lit. b DSGVO ausgeschlossen werden. Hier besteht also ein offensichtlicher Unterschied zu § 14 Abs. 1 TMG, nach dem für sog. Bestandsdaten der Weg zu anderen Erlaubnisnormen, die Raum für eine Interessenabwägung gelassen hätten, versperrt blieb.

2. Verarbeitung von Angaben durch den Nutzer selbst

Zunächst ist die Zulässigkeit der Verarbeitung von Angaben zu analysieren, die der Nutzer aktiv preisgibt. Dabei kommen einerseits solche Daten, die der Nutzer beim Registrierungsprozess über sich preisgibt in Betracht (hierzu a.) als auch solche, die der Nutzer bei der Interaktion innerhalb des Netzwerks freigibt, sei es durch Profileinträge oder dem Gebrauchmachen von gewissen Funktionen innerhalb des sozialen Netzwerks (hierzu b.). Beispielhaft erwähnt für eine solche Funktion sei nur der sog. „Like-Button“ des Netzwerks *Facebook*, mit dem Nutzer nicht nur ihre Zustimmung kundtun können, sondern auch ihre Ablehnung, Trauer oder Zuneigung.

a) Registrierungsdaten

Wie bereits festgestellt kommt bei der Bewertung des Umgangs mit der freiwilligen Angabe personenbezogener Daten sowohl für Bestands- als auch für Inhaltsdaten das BDSG zur Anwendung.[524] Im Folgenden wird die Verarbeitung von personenbezogenen Daten, die während des Registrierungsprozesses von den Nutzern abgefragt werden, datenschutzrechtlich sowohl nach dem BDSG bzw. der DSRL als auch der DSGVO bewertet. Solche Daten umfassen üblicherweise den Klarnamen und eine E-Mail-Adresse, teilweise aber auch die Adresse des Nutzers und weitere Daten, wie etwa das Geschlecht.

524 Vgl. Kap. 3 Pkt. B.I.1.a, S. 154.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aa) Zulässigkeit des Datenumgangs nach dem BDSG bzw. der DSRL

Die Zulässigkeitstatbestände für den Umgang mit personenbezogenen Daten zwischen nicht-öffentlichen Stellen finden sich in den §§ 28 ff BDSG.

i) Abgrenzung zwischen § 28 und § 29 BDSG

Wie bereits beim Umgang mit personenbezogenen Daten im Nutzer-Nutzer-Verhältnis[525] sind auch hier zunächst die Erlaubnistatbestände der § 28 und § 29 BDSG voneinander abzugrenzen. Die Abgrenzung hat hierbei nach dem Zweck des Datenumgangs zu erfolgen.[526] Soweit es sich um den Umgang mit Registrierungsdaten handelt, erheben, verarbeiten und nutzen die Plattformbetreiber diese nicht hauptsächlich zur Übermittlung, sondern für die Erfüllung eigener Geschäftszwecke i. S. d. § 28 Abs. 1 S. 1 BDSG. Die Zulässigkeit des Umgangs mit Daten, die bei der Registrierung anfallen, richtet sich demnach nach § 28 BDSG.

ii) Zulässigkeit gem. § 28 Abs. 1 BDSG bzw. Art. 7 DSRL

In Betracht kommt zunächst die Zulässigkeit des Umgangs mit personenbezogenen Daten gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG, der Art. 7 lit. b DSRL umsetzt. Hierfür müsste der Datenumgang „[…] für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich […] [sein]“, § 28 Abs. 1 S. 1 Nr. 1 BDSG. Die Norm legitimiert also nur die Verwendung der personenbezogenen Daten, die in unmittelbar sachlichem Zusammenhang zum Vertragszweck stehen.[527] Welche Daten davon umfasst sind, ist demnach einzelfallabhängig.[528] So ist etwa die Angabe des Klarnamens in einem Netzwerk, das auf die Knüpfung beruflicher Kontakte ausgerichtet ist, für diesen Zweck erforderlich. Aber auch bei anderen sozialen Netzwerken hat der Betreiber regelmäßig ein berechtigtes Interesse daran, seinen Vertragspartner namentlich zu kennen. Dies gilt unbenommen

525 Vgl. hierzu bereits Kap. 3 Pkt. A.III.2.a.aa, S. 113.
526 *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328, 336, Rn. 24 – spickmich.de; *BGH,* Urt. v. 23.09.2014, Az. VI ZR 358/13, BGHZ 202, 242, 246 f., Rn. 14 ff. – Ärztebewertung II.
527 *Simitis*, in: Simitis, BDSG, § 28, Rn. 57 ff.
528 *Simitis*, in: Simitis, BDSG, § 28, Rn. 60.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

der Pflicht der Telemediendienstanbieter, die Nutzung von Telemedien mindestens unter Pseudonym oder gar anonymisiert zu ermöglichen i. S. d. § 13 Abs. 6 TMG; denn diese Pflicht gilt, wie der Wortlaut der Norm klarstellt, nur für die Nutzung, nicht für den Vertragsschluss über die Nutzung.[529] Sofern es sich um ein kostenpflichtiges soziales Netzwerk handelt, ist auch die Angabe von Bankdaten für die Durchführung des Schuldverhältnisses erforderlich. Ob die Angabe anderer Daten jedoch per se für die Begründung, Durchführung und Beendigung des Schuldverhältnisses erforderlich ist, ist Frage des Einzelfalls. So mag etwa die Erforderlichkeit der Geschlechterangabe für Partnerbörsen noch einleuchten, während dies bei den meisten anderen Arten von sozialen Netzwerken durchaus in Zweifel zu ziehen ist.[530]

Falls man den Erforderlichkeitsgrundsatz jedoch derart streng auslegt,[531] ist die Zulässigkeit der Verwendung dieser Daten auf jeden Fall nach anderen Erlaubnistatbeständen des § 28 Abs. 1 BDSG zu untersuchen. Fraglich ist dann insbesondere, ob für diese Daten möglicherweise § 28 Abs. 1 S. 1 Nr. 2 BDSG einschlägig ist; hierfür müsste die Verwendung der Daten „[…] zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich sein […]“ und schutzwürdige Interessen des Betroffenen dürften nicht überwiegen. Die Anwendung von § 28 Abs. 1 S. 1 Nr. 2 BDSG kann jedenfalls bei einem streng verstandenen Erforderlichkeitsgrundsatz nicht schon deswegen gesperrt sein, weil eine Datenverwendung nach § 28 Abs. 1 S. 1 Nr. 1 BDSG nicht zulässig ist; vielmehr stehen die Erlaubnistatbestände des § 28 Abs. 1 S. 1 BDSG in einem Alternativverhältnis.[532] Dies ergibt sich aus den Vorgaben des Art. 7 DSRL, der das Vorliegen „einer“ der nachfolgenden Voraussetzungen fordert, ohne eine Gewichtung der Erlaubnistatbestände vorzusehen. Art. 7 lit. f DSRL, der eine Güterabwägung vorsieht, wird demnach nicht von Art. 7 lit. b DSRL gesperrt.

529 So auch *Moos*, in: Taeger/Gabel, BDSG, TMG, § 13, Rn. 49 m. w. N.

530 Vgl. Kap. 3 Pkt. B.I.1.a.dd.i, S. 159.

531 Die Auslegung des Erforderlichkeitsgrundsatzes erfolgt insbesondere im Verhältnis zwischen nicht-öffentlichen Stellen nicht einheitlich. Teilweise wird er sehr streng verstanden, *Taeger*, in: Taeger/Gabel, BDSG, Rn. 51, teilweise wird die Erforderlichkeit am Kriterium der Zumutbarkeit bemessen, *Bergmann/Möhrle/Herb,* BDSG, § 28, Rn. 235 f., und teilweise gar als eine Art Abwägungsdirektive verstanden, *Kramer*, in: Auernhammer, BDSG, § 28, Rn. 31 ff.

532 *Kramer*, in: Auernhammer, BDSG, § 28, Rn. 57; *Wolff*, in: BeckOK DatenschutzR, BDSG, § 28, Rn. 20; *Schaffland/Wiltfang,* BDSG, § 28, Rn. 13; a. A. *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 29, Rn. 9, allerdings zurecht hinsichtlich vertraglicher Vertraulichkeitsbestimmungen.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Durch die vollharmonisierende Wirkung der DSRL darf das BDSG aber keine zusätzlichen Voraussetzungen für die Zulässigkeit des Umgangs mit personenbezogenen Daten aufstellen.[533] § 28 Abs. 1 S. 1 Nr. 1 BDSG kann demnach nicht den Zulässigkeitstatbestand des § 28 Abs. 1 S. 1 Nr. 2 BDSG sperren.

Teilweise wird in dem Begriff der „Erforderlichkeit" in § 28 Abs. 1 S. 1 Nr. 1 BDSG bereits eine Aufforderung zur Güterabwägung gesehen,[534] sodass die Zulässigkeit der Verwendung solcher Angaben bereits unter § 28 Abs. 1 S. 1 Nr. 1 BDSG diskutiert werden könnte. Auch wenn man davon ausgeht, dass dem Erforderlichkeitsbegriff bereits eine wertende Untersuchung inneliegt, so sieht § 28 Abs. 1 S. 1 Nr. 2 BDSG gleichwohl eine darüberhinausgehende, offenere Interessenabwägung vor. Dies zeigt sich schon daran, dass die Zulässigkeit der Datenverwendung gem. § 28 Abs. 1 S. 1 Nr. 2 BDSG ebenfalls dem Erforderlichkeitsgrundsatz unterliegt. Hieran wird der Unterschied zu § 14 Abs. 1 TMG deutlich, der eine solche Interessenabwägung nicht zulässt.[535] Klarstellend sei anzumerken, dass § 28 Abs. 1 S. 1 Nr. 2 BDSG freilich nicht für eine Zweckentfremdung der im Rahmen der § 28 Abs. 1 S. 1 Nr. 1 BDSG erhobenen Daten herangezogen werden kann.[536] Vorliegend geht es aber gerade um die Erhebung im Rahmen des Registrierungsprozesses solcher Daten, die nicht i. S. d. § 28 Abs. 1 S. 1 BDSG für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses erforderlich sind, und nicht um die weitere Verwendung bereits erhobener Daten, die sich nach § 28 Abs. 2 BDSG richtet.

Berechtigte Interessen können wirtschaftliche wie ideelle Interessen sein;[537] der Begriff des berechtigten Interesses ist demnach äußerst weit zu fassen. Dem dürften aber keine überwiegenden schutzwürdigen Betroffeneninteressen gegenüber stehen. Die Abwägung muss einzelfallbezogen erfolgen, wobei die Art der Daten, die verwendet werden sollen, eine entscheidende Rolle spielt.[538] Entscheidend ist jedoch, dass die Zwecke der Verarbeitung und Nutzung bereits bei der Erhebung festgelegt werden müssen, § 28 Abs. 1 S. 2 BDSG; diese Zwecke sind dem Betroffenen gem. § 4 Abs. 3 S. 1 Nr. 2 BDSG auch mitzuteilen.

---

533 *EuGH,* Urt. v. 24.11.2011, Rs. C-468/10 und C-469/10, C-468/10, C-469/10, Slg. 2011, I-12181, Rn. 38 f. – ASNEF und FECEMD.
534 Vgl. etwa *Kramer*, in: Auernhammer, BDSG, § 28, Rn. 31 ff.
535 Vgl. Kap. 3 Pkt. B.I.1.a.dd.i, S. 159.
536 *Simitis*, in: Simitis, BDSG, § 28, Rn. 99.
537 *Simitis*, in: Simitis, BDSG, § 28, Rn. 104; vgl. zum Begriff bereits Kap. 3 Pkt. A.III.2.c.bb.i, S. 128.
538 *Kramer*, in: Auernhammer, BDSG, § 28, Rn. 72.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Demnach kann die Erhebung der Geschlechterangabe gem. § 28 Abs.1 S. 1 Nr. 2 BDSG zulässig sein, sofern dies für die Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist. Aufgrund der weiten Auslegung der berechtigten Interessen kann dieses Interesse etwa in der besseren Angebotsgestaltung für den Nutzer liegen. Demgegenüber dürften die Betroffeneninteressen an dem Ausschluss der Verarbeitung oder Nutzung jedoch nicht überwiegen. Da sich das Geschlecht in den meisten Fällen schon aus der Namensangabe erschließt, deren Erhebung, Verarbeitung und Nutzung gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG zulässig ist, werden Betroffeneninteressen regelmäßig nicht überwiegen. Hierbei darf jedoch weder die Zweckbindung des § 28 Abs. 1 S. 2 BDSG noch die gründliche Prüfung der Erforderlichkeit im Einzelfall außer Acht gelassen werden.

bb) Zulässigkeit der Datenverarbeitung nach der DSGVO

Die Verarbeitung der Registrierungsdaten unter dem Regime der DSGVO richtet sich nach Art. 6 Abs. 1 DSGVO. Gem. Art. 6 Abs. 1 S. 1 lit. b DSGVO ist die Verarbeitung „[…] nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: […] die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich […]". Die Norm ist damit das Pendant zu Art. 7 lit. b DSRL bzw. § 28 Abs. 1 S. 1 Nr. 1 BDSG. Auch unter der DSGVO müssten die zu verarbeitenden Daten also für die Erfüllung des Vertrags erforderlich sein. Ebenso wie bisher wird demnach auch unter der DSGVO eine Einzelfallentscheidung vorzunehmen sein. Mit Blick auf soziale Netzwerke und andere Dienste, in denen Nutzer mit ihren Daten für die Leistungserbringung „bezahlen", wird vereinzelt diskutiert, ob es für die Bestimmung der Erforderlichkeit nicht auf die Erbringung der spezifischen Dienste, sondern auf das Geschäftsmodell des Tauschhandels „Daten gegen Leistung" ankommen soll.[539] Dem lässt sich jedoch der Wortlaut des Art. 6 Abs. 1 S. 1 lit. b DSGVO entgegenhalten: Denn dieser legitimiert die Datenverarbeitung nur, sofern sie für die *Erfüllung* des Vertrags erforderlich ist. Die Erfüllung des Vertrags liegt aber regelmäßig in der Bereitstellung der konkreten Dienste und nicht in der Datenverarbeitung der Nutzer. Zudem würde dies dazu führen, dass Art. 6

539 *Buchner/Petri*, in: Kühling/Buchner, DSGVO, Art. 6, Rn. 40 f.; Art. 7 Rn. 48, 51, allerdings mit der Maßgabe, dass der Tauschhandel für den Nutzer ausdrücklich transparent gemacht werden muss.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Abs. 1 S. 1 lit. b DSGVO weitflächig eine Verarbeitung von Nutzerdaten legitimieren würde, ohne eine Abwägung mit Betroffeneninteressen einzubeziehen. Mit dieser weiten Auslegung wären also schlagartig zahlreiche Datenverarbeitungen im Internet legitimiert. Das würde dazu führen, dass Datenverarbeitungen durch Diensteanbieter, die sich durch Nutzerdaten finanzieren, vom Schutz der DSGVO ausgenommen würden.

Überdies widerspricht diese Auslegung der Systematik des Art. 6 Abs. 1 S. 1 DSGVO. Denn sofern Art. 6 Abs. 1 S. 1 lit. b DSGVO die Datenverarbeitung nicht legitimiert, könnte eine Datenverarbeitung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO in Betracht kommen. Dass die Normen nebeneinander anwendbar sind, stellt Art. 6 Abs. 1 S. 1 DSGVO selbst klar, in dem er das Vorliegen „mindestens eine[r] der nachstehenden Bedingungen" vorschreibt.[540] Art. 6 Abs. 1 S. 1 lit. f DSGVO bietet genügend Raum, um die Verarbeiterinteressen an einer Verarbeitung der Nutzerdaten zu bedenken; dies jedoch eben unter Abwägung mit den Betroffeneninteressen. Daher ist eine derart extensive Auslegung des Art. 6 Abs. 1 S. 1 lit. b DSGVO weder nötig noch sachgerecht. Demnach sind für die Erforderlichkeit bei der Verarbeitung von Registrierungsdaten im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DSGVO dieselben Voraussetzungen anzusetzen, wie bereits bei § 28 Abs. 1 S. 1 Nr. 1 BDSG.[541] Erforderlich i. S. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO ist demnach wohl die Angabe des Klarnamens im Rahmen eines sozialen Netzwerks für berufliche Kontakte. Die Erforderlichkeit der Geschlechterangabe in einem sozialen Netzwerk, das nicht der Kontaktsuche, sondern der Online-Vernetzung von in der Realwelt bestehenden Verbindungen dient, ist demgegenüber zweifelhaft. Für diese Fallgruppen ist dann auf Art. 6 Abs. 1 S. 1 lit. f DSGVO abzustellen. Ebenso wie bei § 28 Abs. 1 S. 1 Nr. 2 BDSG liegt das berechtigte Interesse der Verarbeitung auf Seiten des Plattformbetreibers in der besseren Angebotsgestaltung, wobei die Betroffeneninteressen bei den durch den Nutzer selbst bereitgestellten personenbezogenen Daten nicht überwiegen.

---

540 Ebenso *GA Bobek,* Schlussanträge v. 26.01.2017, Rs. C-13/16, ECLI:EU:C:2017:43, Rn. 58 u. Fn. 13 – Rīgas.

541 Vgl. Kap. 3 Pkt. B.I.2.a.aa.ii, S. 164.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Weitere vom Nutzer selbst preisgegebene personenbezogene Daten

Neben Registrierungsdaten muss ferner auf die Zulässigkeit der Datenverarbeitung weiterer, freiwillig preisgegebener Informationen abgestellt werden. Hierzu zählt nicht nur die Datenverarbeitung von Inhalten, die die Nutzer selbst in dem sozialen Netzwerk hochladen, sondern auch die Inanspruchnahme bereitgestellter Funktionen. Als eines der bekanntesten Beispiele hierfür lässt sich der sog. „Like-Button" des sozialen Netzwerks *Facebook* anführen.

aa) Zulässigkeit nach dem BDSG

Die Zulässigkeit nach §§ 28 f. BDSG richtet sich nach dem Hauptzweck der Verwendung der Daten. Hierbei muss insbesondere zwischen zwei Intentionen bei der Verwendung der Daten unterschieden werden: Zum einen erfolgt der Umgang mit personenbezogenen Daten zum Zweck der Funktionalität des sozialen Netzwerks. So muss der Betreiber eines sozialen Netzwerks die eingegebenen Daten eines Nutzers an die anderen Nutzer übermitteln, da andernfalls das soziale Netzwerk nicht funktionieren würde; für diese Fälle ist § 29 BDSG die richtige Zulässigkeitsnorm. Zum Anderen erfolgt der Umgang mit personenbezogenen Daten zu eigenen Geschäftszwecken. Im Vordergrund steht hierbei die Verwendung zu Werbezwecken, wie exemplarisch aus dem Jahresbericht des sozialen Netzwerks *Facebook*[542] hervorgeht. Hier ist also auf § 28 BDSG abzustellen.

Wichtig ist indes zu erwähnen, dass ein und dieselbe Datenerhebung, -verarbeitung, und -nutzung demnach unterschiedliche Zwecke verfolgen kann und mehrere Zulässigkeitstatbestände parallel einschlägig sein können.[543]

542 Vgl. *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 5: „We generate substantially all of our revenue from selling advertising placements to marketers"; vgl. Kap. 1 Pkt. C.I, S. 38.

543 *Ehmann*, in: Simitis, BDSG, § 29, Rn. 23.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

i) Zulässigkeit zu Zwecken der Funktionalität des sozialen Netzwerks

Der Sinn eines sozialen Netzwerks ist zunächst die Kommunikation der Nutzer. Kernfunktion sozialer Netzwerke ist demnach, dass die Inhalte, die ein Nutzer postet, für die Einsicht durch andere Nutzer bereitstehen. Der Hauptzweck des Datenumgangs ist also die Übermittlung; sie erfolgt auch geschäftsmäßig, da es sich hierbei um eine auf Wiederholung und gewisse Dauer ausgerichtete Tätigkeit handelt.[544] Hinsichtlich der unterschiedlichen Erlaubnistatbestände kann auf die Ausführungen zur Zulässigkeit des Umgangs mit personenbezogenen Daten im Nutzer-Nutzer-Verhältnis verwiesen werden.[545] Sofern es sich um die Übermittlung personenbezogener Daten des postenden Nutzers selbst handelt, ist die Erhebung, Speicherung, Veränderung und Nutzung gem. § 29 Abs. 1 S. 1 Nr. 1 BDSG zulässig, da in diesem Fall von entgegenstehenden Interessen des Betroffenen regelmäßig nicht ausgegangen werden muss. Schwieriger erscheint die Datenverwendung, sobald ein Nutzer die personenbezogenen Daten einer anderen Person freigibt. Dahingehend kann auf die Ausführungen im Nutzer-Nutzer-Verhältnis verwiesen werden.[546] Soweit es sich nicht um allgemeinzugängliche Informationen handelt, wird das Betroffeneninteresse der anderen Person der Übermittlung entgegenstehen.[547] Als Legitimationsmittel bleibt dann nur die Einwilligung.

ii) Zulässigkeit der Datenverwendung zu Werbezwecken

(1) Keine Generalerlaubnis durch § 28 Abs. 1 S. 1 BDSG

Die Zulässigkeit der Erhebung personenbezogener Daten zu eigenen Geschäftszwecken, insbesondere zu Werbezwecken, richtet sich indes nach den Vorgaben des § 28 BDSG. Ebenso wie bei Art. 6 Abs. 1 S. 1 lit. b DSGVO würde es auch hier zu weit führen, als Legitimationsgrundlage § 28 Abs. 1 S. 1 Nr. 1 BDSG heranzuziehen und bei der Beurteilung der Erforderlichkeit für die Durchführung des Vertragsverhältnisses zwischen

544 *Ehmann,* in: Simitis, BDSG, § 29, Rn. 58 ff.; vgl. ausführlich Kap. 3 Pkt. A.III.2.a.aa, S. 113.
545 Vgl. Kap. 3 Pkt. A.III.2.a.bb, S. 117.
546 Vgl. Kap. 3 Pkt. A.III.2.a, S. 113.
547 Vgl. Kap. 3 Pkt. A.III.2.a.bb, S.117.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Nutzer und Plattformbetreiber auf das Geschäftsmodell der Datenverwendung zu Werbezwecken abzustellen.[548] Eine derart extensive Ausweitung des Tatbestands würde dazu führen, dass die Datenverarbeitung durch Plattformbetreiber, die sich mit personenbezogenen Nutzerdaten finanzieren, regelmäßig per se erlaubt wäre, ohne dass eine Abwägung mit Betroffeneninteressen vorgenommen würde.

(2) Privilegierung der Datenverwendung i. S. d. § 28 Abs. 3 BDSG

(a) Verarbeitung und Nutzung bei Einwilligung

Zunächst gestattet § 28 Abs. 3 S. 1 BDSG die Verarbeitung oder Nutzung personenbezogener Daten „für Zwecke des Adresshandels oder der Werbung", soweit der Betroffene eingewilligt hat. Zudem sieht das BDSG für diese Zwecke eine ausdrückliche Erleichterung des Schriftformerfordernisses aus § 4a Abs. 1 S. 3 BDSG vor. Gem. § 28 Abs. 3 S. 1 i. V. m. § 28 Abs. 3a S. 1 BDSG ist ausdrücklich auch die elektronische Erklärung der Einwilligung möglich, was nach der Systematik des § 4a Abs. 1 S. 3 Hs. 2 BDSG im Regelfall nur ausnahmsweise möglich ist.[549]

(b) „Listenprivileg" i. S. d. § 28 Abs. 3 S. 2 BDSG

Eine Einwilligung i. S. d. § 28 Abs. 3 S. 1 BDSG ist jedoch dann nicht nötig, wenn die Verarbeitung und Nutzung personenbezogener Daten „für Zwecke des Adresshandels oder der Werbung" gem. § 28 Abs. 3 S. 2 BDSG privilegiert ist. Liegen die Voraussetzungen des § 28 Abs. 3 S. 2 BDSG vor, ist die Verarbeitung und Nutzung der dort genannten Daten erlaubt; die Erlaubnisnorm ist insofern lex specialis zu den übrigen Erlaubnisnormen des § 28 BDSG.[550] Um eine zu extensive Privilegierung auszuschließen, muss der Werbebegriff enger als i. S. d. Wettbewerbsrechts definiert werden;[551] Voraussetzung ist „eine konkrete Absicht zum Absatz von

548 Vgl. Kap. 3 Pkt. B.I.2.a.bb, S. 167.
549 Zur Möglichkeit der elektronischen Einwilligung i. S. d. § 13 Abs. 2 TMG vgl. Kap. 3 Pkt. B.II.2, S. 190.
550 *Kramer*, in: Auernhammer, BDSG, § 28, Rn. 92.
551 *Kramer*, in: Auernhammer, BDSG, § 28, Rn. 92.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Waren und Dienstleistungen".[552] Diese ist bei der Verwendung von Nutzerdaten durch die sozialen Netzwerke jedenfalls dann gegeben, wenn diese die Daten verwenden, um zielgerichtet Werbung schalten zu können.

Das sog. „Listenprivileg"[553] des § 28 Abs. 3 S. 2 BDSG umfasst nur die dort genannten Daten, namentlich „[…] listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe […], die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken […]". § 28 Abs. 3 S. 2 Nr. 1 BDSG ist zunächst beschränkt auf die erforderliche Verarbeitung und Nutzung zu Werbezwecken für *eigene* Angebote der verantwortlichen Stelle, die diese zuvor nach Maßgabe des § 28 Abs. 1 S. 1 Nr. 1 BDSG oder aus allgemein zugänglichen Verzeichnissen erhoben hat. Das BDSG sieht damit eine Durchbrechung des Zweckbindungsgrundsatzes bei bereits gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG erhobenen Daten für die weitere Verwendung zu Werbezwecken vor; eine erneute Erhebung ist nicht notwendig.

Gem. § 28 Abs. 3 S. 3 BDSG darf die verantwortliche Stelle für Zwecke nach § 28 Abs. 3 S. 2 Nr. 1 BDSG zudem weitere Daten in die Liste hinzuspeichern, ohne dass die Norm eine Begrenzung auf die Art der Daten vornimmt.[554]

(c) Nutzung für fremde Angebote i. S. d. § 28 Abs. 3 S. 5 BDSG

Plattformbetreiber finanzieren sich aber gerade durch die Werbung für *fremde* Angebote. Für sie lässt § 28 Abs. 3 S. 5 BDSG die Nutzung von Daten zu, solange die verantwortliche Stelle für den Betroffenen eindeutig erkennbar ist. Beispielhaft wird in der Literatur regelmäßig der Anwendungsfall der „Beipackwerbung" genannt,[555] d. h. die Beilegung von Werbung für fremde Angebote zur eigenen Werbung. Der Wortlaut beschränkt die Nutzung für fremde Angebote aber keinesfalls auf die Werbung als Annex zur Werbung für eigene Angebote und ist auch ausweislich der Gesetzesbegründung nicht darauf begrenzt.[556] Zudem ist auffällig, dass das

552 *Kramer*, in: Auernhammer, BDSG, § 28, Rn. 97.
553 *Simitis*, in: Simitis, BDSG, § 28, Rn. 230.
554 *Simitis*, in: Simitis, BDSG, § 28, Rn. 240.
555 *Wedde*, in: DKWW, BDSG, § 28, Rn. 115; *Simitis*, in: Simitis, BDSG, § 28, Rn. 244; *Taeger*, in: Taeger/Gabel, BDSG, § 28, Rn. 207.
556 BT-Drucks. 16/13657, S. 19.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

BDSG die Nutzung zu Zwecken der Werbung für fremde Angebote nicht auf die in § 28 Abs. 3 S. 2 BDSG genannten Listendaten beschränkt.

Interessanter als der Anwendungsfall der „Beipack-Werbung" ist der Fall der Schaltung von Werbung im Internet. Am Beispiel von *Facebook* lässt sich dies verdeutlichen: Daten, die *Facebook* rechtmäßig erhoben hat, etwa die Stammdaten seiner Nutzer i. S. d. § 28 Abs. 1 S. 1 Nr. 1 BDSG,[557] darf *Facebook* für die Schaltung von Werbung für fremde Angebote nutzen. Die erlaubte Nutzung umfasst ferner die listenmäßig zusammengefassten Daten des § 28 Abs. 3 S. 2 BDSG.[558] Dies ist freilich für *Facebook*, das sich nach eigenen Aussagen über Einnahmen durch Werbeplatzierung finanziert,[559] deutlich relevanter als die Werbeschaltung für eigene Angebote.

(d) Übermittlung an Dritte

Schließlich dürfen die nach § 28 Abs. 3 S. 2 verarbeiteten Daten auch an Dritte übermittelt werden, § 28 Abs. 3 S. 4 BDSG. „Dritte" i. S. d. § 3 Abs. 8 S. 2 BDSG ist jede Stelle außerhalb der verantwortlichen Stelle. Dabei gelten auch unterschiedliche Unternehmen innerhalb einer Unternehmensgruppe als „Dritte".[560] Beispielhaft kann zu dieser Problematik auf *WhatsApp* verwiesen werden, das personenbezogene Daten an *Facebook* übermittelte.[561]

---

557 Vgl. Kap. 3 Pkt. B.I.2.a, S. 163.

558 *Simitis*, in: Simitis, BDSG, § 28, Rn. 244.

559 *Facebook Inc.*, Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017), S. 5; vgl. Kap. 1 Pkt. C.I, S. 38.

560 *Dammann*, in: Simitis, BDSG, § 3, Rn. 232.

561 *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Anordnung gegen Massendatenabgleich zwischen WhatsApp und Facebook, abrufbar unter https://www.datenschutz-hamburg.de/news/detail/article/anordnung-gegen-massendatenabgleich-zwischen-whatsapp-und-facebook.html (abgerufen am 13.10.2017); *VG Hamburg,* Beschl. v. 24.04.2017, Az. 13 E 5912/16, abrufbar unter http://justiz.hamburg.de/contentblob/8628058/8d1290fe1e894141c634755236d8394d/data/13e5912-16.pdf (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

bb) Zulässigkeit nach der DSGVO

Im Rahmen der DSGVO ist als Ausgangspunkt regelmäßig die Erlaubnisnorm des Art. 6 Abs. 1 DSGVO heranzuziehen. Anders als die Erlaubnistatbestände des BDSG ist Art. 6 Abs. 1 DSGVO deutlich schlichter aufgebaut und erwähnt auch die Verarbeitung zu Werbezwecken nicht ausdrücklich. Als Erlaubnisnorm muss demnach – wiederum – regelmäßig Art. 6 Abs. 1 S. 1 lit. f DSGVO herangezogen werden. Die Erlaubnis zur Verarbeitung hängt also im Einzelfall von einer vom Verantwortlichen selbst getroffenen Interessenabwägung ab.[562] EG 47 S. 6 DSGVO stellt dabei explizit klar, dass „[d]ie Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung […] als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden [kann].“ In der Praxis könnte diese unbestimmte Norm in Verbindung mit der Tatsache, dass die Interessenabwägung dem Verantwortlichen selbst obliegt, durchaus zu einer Zunahme der Verarbeitung zu Werbezwecken führen. Umso wichtiger erscheinen dabei die „Schutzmaßnahmen“, die die DSGVO für diese Fälle errichtet: So sieht die DSGVO in Art. 21 Abs. 2, 3 DSGVO ein Widerspruchsrecht bei der Verarbeitung zum Zwecke der Direktwerbung vor.[563] Freilich stellt dies zum BDSG, das in § 28 Abs. 4 BDSG ein Widerspruchsrecht in die Verarbeitung und Nutzung zu Zwecken der Werbung vorsieht, kein Novum dar, könnte aber wegen der fehlenden Begrenzung auf listenmäßig erfasste Daten eine noch bedeutsamere Rolle für den Betroffenen zum Schutz seiner personenbezogenen Daten spielen – vorausgesetzt, der Betroffene macht von diesem Widerspruchsrecht Gebrauch, woran sich in der Praxis regelmäßig zweifeln lässt. Zudem stellt EG 58 S. 3 der DSGVO klar, dass im Sinne des Transparenzgebotes die Betroffenen insbesondere bei Werbung im Internet wissen müssten, wer zu welchem Zwecke Daten über sie erfasst. Dieses Transparenzgebot, das in Art. 5 Abs. 1 lit. a DSGVO festgelegt ist, spielt eine essentielle Rolle für die Betroffenen bei der Wahrnehmung ihrer Rechte. Gleichwohl vermögen diese Betroffenenrechte nur nachträglichen Schutz zu bieten. Letztlich ist es sehr wahrscheinlich, dass der eigentlich präventiv intendierte Schutz des Art. 6 Abs. 1 DSGVO durch die allzu ungenaue Norm des Art. 6 Abs. 1 S. 1 lit. f DSGVO unterlaufen wird.

562 Vgl. zu Art. 6 Abs. 1 S. 1 lit. f DSGVO ausführlich Kap. 3 Pkt. A.III.2.c, S. 125 und Kap. 3 Pkt. B.I.2a.bb, S. 167.

563 Dazu Kap. 3 Pkt. D.I.2, S. 217.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

3. Verarbeitung von mittels Tracking Tools erhobenen Daten

a) RL 2002/136/EG bzw. RL 2009/136/EG

Fraglich ist, welche Normen für die Verarbeitung von mittels Tracking Tools – also etwa HTTP-Cookies[564] – erhobenen Daten sachlich anwendbar sind. Für diese Informationen könnten nicht die Vorgaben der DSRL, sondern der RL 2002/58/EG[565] i. d. F. der Änderung durch Art. 2 der RL 2009/136/EG[566] (im Folgenden: ePrivacy-RL[567]) maßgeblich sein. Gem. Art. 1 Abs. 2 ePrivacy-RL stellen die Regelungen der ePrivacy-RL „[…] eine Detaillierung und Ergänzung […]" der DSRL dar. Regelungen in der ePrivacy-RL, die auf Tracking Tools anwendbar sind, gehen den Regelungen der DSRL also vor.

Gem. Art. 5 Abs. 3 der ePrivacy-RL ist „[…] der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet, wenn der betreffende Teilnehmer oder Nutzer auf Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat."

Bei den genannten Tracking Tools müsste es sich also um im Endgerät des Nutzers gespeicherte Informationen handeln, und es müsste ferner ein Zugriff darauf erfolgen.

---

564 Vgl. Kap. 1 Pkt. C.II.1, S. 41.

565 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl.EG 2002 L 201, 37.

566 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, Abl.EU 2009 L 337, 11.

567 Soweit konkret auf Bestimmungen nur der RL 2002/58/EG bzw. nur der RL 2009/136/EG abgestellt wird, werden die Regelwerke entsprechend bezeichnet.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aa) Sachlicher Anwendungsbereich hinsichtlich Cookies

Dass Cookies vom sachlichen Anwendungsbereich des Art. 5 Abs. 3 ePrivacy-RL umfasst sind, ist unumstritten.[568] In EG 25 der RL 2002/58/EG sowie in EG 66 der RL 2009/136/EG werden Cookies beispielhaft als Instrumente genannt, mit deren Hilfe Informationen über Nutzer gespeichert und abgerufen werden können. Nicht zuletzt etablierte sich für die ePrivacy-RL sogar der Spitzname „Cookie-Richtlinie".[569] HTTP-Cookies sind kleine Textdateien, die auf dem Rechner des Nutzers beim Besuch einer Website gespeichert werden können und die Informationen zur Identifikation des Nutzers enthalten können.[570] Sie sind damit geeignet, Informationen auf dem Nutzer-PC oder sonstigen Endgeräten zu speichern und speichern Informationen, auf die zugegriffen werden kann i. S. d. Art. 5 Abs. 3 ePrivacy-RL.

bb) Sachlicher Anwendungsbereich hinsichtlich anderer Tracking Tools

Fraglich ist, ob Art. 5 Abs. 3 ePrivacy-RL hinreichend offen formuliert ist, um auch auf andere Tracking Tools anwendbar zu sein. Voraussetzung ist nach dem Wortlaut des Art. 5 Abs. 3 ePrivacy-RL, dass auf dem Endgerät des Nutzers – also etwa seinem PC – Informationen gespeichert werden oder auf bereits im Endgerät gespeicherte Informationen zugegriffen wird. Der Begriff „Informationen" wird in der ePrivacy-RL nicht definiert; deswegen wird teilweise diskutiert, ob unter „Information" i. S. d. Art. 5 Abs. 3 ePrivacy-RL nicht Cookies selbst anzusehen seien.[571] Dem widerspricht jedoch bereits die Formulierung in den Erwägungsgründen der ePrivacy-RL. So unterscheiden EG 24 f. der RL 2002/58/EG ausdrücklich zwischen Informationen und „Instrumenten" mittels derer die Informationen erlangt

568 Vgl. etwa *Dietrich*, ZD 2015, 199, 200; *Schmidt/Babilon*, K&R 2016, 86, 87; *Rauer/Ettig*, ZD 2014, 27, 28; *Art. 29-Datenschutzgruppe*, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht. WP 194 (07.06.2012), S. 2 ff.; *Art. 29-Datenschutzgruppe*, Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies. WP 208 (02.10.2013), S. 2 ff.

569 *Dietrich*, ZD 2015, 199, 200.

570 *Roesner/Kohno/Wetherall*, Detecting and Defending Against Third-Party Tracking on the Web, abrufbar unter https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (abgerufen am 13.10.2017), S. 2; vgl. Kap. 1 Pkt. C.II.1, S. 41.

571 *Dietrich*, ZD 2015, 199, 200 f. m. w. N.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

werden. Ferner nennt EG 25 S. 1 der RL 2002/58/EG „[…] z. B. so genannte Cookies […]“ als ein solches Instrument und macht damit bereits deutlich, dass es sich hierbei lediglich um eine beispielhafte Nennung handeln soll. Damit schließt nicht bereits der Wortlaut des Art. 5 Abs. 3 ePrivacy-RL die Anwendbarkeit auf andere Tracking Tools aus. Soweit es sich um verschiedene Arten von Cookies handelt, die auf dem Endgerät des Nutzers gespeichert sind – wie etwa Flash Cookies[572] –, ist Art. 5 Abs. 3 ePrivacy-RL unproblematisch anwendbar.

Fraglich ist jedoch, wie es sich bei anderen Tracking Methoden verhält, etwa dem sog. Canvas Fingerprinting. Canvas Fingerprinting ist eine Methode, mit der Informationen über den Nutzer-PC ausgelesen werden, wie etwa der verwendete Browser und sein Betriebssystem. Aus der Vielzahl der Informationen ergibt sich ein „Fingerabdruck“, mit dem Nutzer identifiziert werden können.[573] Hier wird keine Datei auf dem Endgerät des Nutzers abgelegt, sodass Art. 5 Abs. 3 S. 1 Var. 1 ePrivacy-RL, d. h. die Speicherung von Informationen auf dem Endgerät des Nutzers, nicht einschlägig ist. Allerdings wird mit dieser Methode auf „[…] Informationen, die bereits im Endgerät eines […] Nutzers gespeichert sind […]“ i. S. d. Art. 5 Abs. 3 S. 1 Var. 2 ePrivacy-RL zugegriffen. Auch für diesen Fall ist Art. 5 Abs. 3 ePrivacy-RL also anwendbar und verdrängt insofern die Vorgaben der DSRL.

cc) Vorgaben der ePrivacy-RL für den Einsatz von Tracking Tools

Art. 5 Abs. 3 ePrivacy-RL verlangt, dass der Nutzer in die Speicherung von oder den Zugriff auf Informationen in seinem Endgerät die „Einwilligung gegeben hat“, also eine Einwilligung noch vor Beginn der Speicherung oder des Zugriffs. Die Anforderungen an die Einwilligung entsprechen gem. Art. 5 Abs. 3 S. 1 ePrivacy-RL wiederum den Vorgaben der DSRL, insbesondere also Art. 2 lit. h DSRL sowie Art. 7 lit. a DSRL.[574]

Ausnahmen von diesem Erfordernis sieht Art. 5 Abs. 3 S. 2 ePrivacy-RL vor, sofern die Speicherung von oder der Zugang zu Informationen „[…]

572 Vgl. Kap. 1 Pkt. C.II.1, S. 41.

573 *Acar/Eubank/Englehardt/Juarez/Narayanan/Diaz*, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, in: Association for Computing Machinery (Hrsg.), CCS'14, S. 679; vgl. Kap. 1 Pkt. C.II.2, S. 43.

574 Vgl. Kap. 3 Pkt. A.III.3, S. 130.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich erwünscht wurde, diesen Dienst zur Verfügung stellen kann."

dd) Umsetzung in deutsches Recht

Die ePrivacy-RL, deren Umsetzungsfrist bereits im Jahr 2011 ablief,[575] wurde formell nicht in deutsches Recht umgesetzt.[576] Nach Ansicht der Bundesregierung ist den Anforderungen des Art. 5 Abs. 3 ePrivacy-RL jedoch mit §§ 12, 15 TMG genüge getan.[577] § 12 Abs. 1 TMG stellt für die Erhebung und Verwendung personenbezogener Daten ein Verbot mit Erlaubnisvorbehalt; sie ist nur erlaubt, soweit der Betroffene eingewilligt hat, oder eine Norm des TMG oder eines anderen Gesetzes, das sich ausdrücklich auf Telemedien bezieht, dies bestimmt. Eine solche Erlaubnisnorm könnte indes der § 15 Abs. 1 TMG stellen: Er erlaubt die Erhebung und Verwendung personenbezogener Daten von Nutzern, „[…] soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen […]". Allerdings scheinen die Anwendungsbereiche des § 15 Abs. 1 TMG und des Art. 5 Abs. 3 ePrivacy-RL zunächst nicht dieselben zu sein. Denn Art. 5 Abs. 3 ePrivacy-RL bezieht sich, anders als § 15 Abs. 1 TMG, nach seinem Wortlaut auf alle „Informationen" und nicht nur auf personenbezogene Daten. Allerdings muss Art. 5 Abs. 3 ePrivacy-RL dergestalt ausgelegt werden, dass mit „Informationen" personenbezogene Daten gemeint sind. Dies ergibt sich aus der Systematik der ePrivacy-RL. Denn der Anwendungsbereich der ePrivacy-RL bezieht sich gem. Art. 1 Abs. 1 auf „[…] die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation […]". Zudem stellt Art. 5 Abs. 3 ePrivacy-RL eine Detaillierung der DSRL i. S. d. Art. 1 Abs. 2 ePrivacy-RL dar, die nur auf personenbezogene Daten Anwendung findet.[578]

---

575 Art. 4 RL 2009/136/EG.

576 *Dietrich*, ZD 2015, 199, 202.

577 Questionnaire on the implementation of the Article 5(3) of the ePrivacy. COCOM11-20, abrufbar unter https://www.telemedicus.info/uploads/Dokumente/COCOM11-20QuestionnaireonArt.53e-PrivacyDir.pdf (abgerufen am 13.10.2017), S. 4 f.

578 i. E. ähnlich *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 21.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Gleichwohl bezieht sich § 15 Abs. 1 TMG auf alle Nutzungsdaten und deckt damit auch Fälle wie IP-Adressen ab, die nicht in den Bereich der ePrivacy-RL, sondern in den Anwendungsbereich der DSRL fallen. Für diese Fälle ist § 15 Abs. 1 TMG jedoch mangels der Möglichkeit einer Interessenabwägung unvereinbar mit Art. 7 lit. f DSRL.[579] Art. 5 Abs. 3 ePrivacy-RL sieht jedoch, ebenso wie § 15 Abs. 1 TMG, ein Erforderlichkeitserfordernis vor, das keine Interessenabwägung zulässt. Allerdings erlaubt § 15 Abs. 3 TMG die Erstellung von Nutzungsprofilen zu Zwecken der Werbung, Marktforschung oder bedarfsgerechten Gestaltung der Telemedien und regelt hierfür lediglich ein Widerrufsrecht des Nutzers, nicht aber seine vorherige Einwilligung. Die Norm wurde bereits zurecht vielfach als unvereinbar mit Art. 5 Abs. 3 ePrivacy-RL kritisiert.[580] § 15 Abs. 3 TMG umfasst auch Fälle wie Cookies, die gem. Art. 5 Abs. 3 ePrivacy-RL ausdrücklich eine Einwilligung fordern. In Betracht kommt demnach eine richtlinienkonforme Auslegung der Norm oder eine unmittelbare Anwendung des Art. 5 Abs. 3 ePrivacy-RL. Doch selbst wenn die Richtliniennorm für hinreichend bestimmt erachtet werden kann, wird die unmittelbare Horizontalwirkung von Richtlinien weitgehend abgelehnt.[581] Die Möglichkeit einer richtlinienkonformen Auslegung des § 15 Abs. 3 TMG wird indes wegen des klaren Wortlauts zurecht abgelehnt.[582] Teilweise wird daher argumentiert, dass die Norm zwischen nicht-öffentlichen Stellen weiterhin volle

---

579 Zur Unvereinbarkeit des § 15 Abs. 1 TMG mit Art. 7 lit. f DSRL vgl. Kap. 3 Pkt. B.I.1.a.bb, S. 156.

580 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-UmsetzungDatenschutzrichtlinie.html?nn=5217228 (abgerufen am 13.10.2017); *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015 zur Verfolgung des Nutzerverhaltens im Internet, abrufbar unter https://www.datenschutz-bayern.de/dsbk-ent/DSK_88p-Cookies.html (abgerufen am 13.10.2017); *Dietrich*, ZD 2015, 199, 202; *Schmidt/Babilon*, K&R 2016, 86, 89 f.

581 *Schroeder*, in: Streinz, EUV/AEUV, Art. 288 AEUV, Rn. 116; *Schmidt/Babilon*, K&R 2016, 86, 90; zweifelnd *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 21.

582 *Schmidt/Babilon*, K&R 2016, 86, 89 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Wirkung entfaltet.[583] Dies kann jedoch nicht überzeugen. Denn unionsrechtswidrige Normen müssen von mitgliedstaatlichen Stellen unangewendet bleiben,[584] sodass die verantwortliche Stelle sich nicht auf diesen Erlaubnistatbestand berufen kann. Verantwortlichen Stellen ist daher regelmäßig zu raten, auch für Fälle des § 15 Abs. 3 TMG die Einwilligung der Nutzer einzuholen.

b) Entwurf einer ePrivacy-VO

Im Januar 2017 stellte die Kommission einen Entwurf für eine neue ePrivacy-VO (im Folgenden: ePrivacy-VO-E) vor, die die ePrivacy-RL ablösen soll.[585] Ebenso wie die ePrivacy-RL die DSRL ergänzt, soll die ePrivacy-VO die DSGVO ergänzen, Art. 1 Abs. 3 ePrivacy-VO-E.[586] Zu diesem Zweck soll sie zeitgleich mit der DSGVO ab dem 28. Mai 2018 anwendbar sein, Art. 29 Abs. 2 ePrivacy-VO-E. Die bisher bestehende Unsicherheit um die unzureichende Umsetzung der ePrivacy-RL wird dann beseitigt sein.

Art. 8 ePrivacy-VO-E soll dem Schutz von Informationen, die in Endgeräten der Nutzer gespeichert sind oder damit im Zusammenhang stehen, dienen. Ausweislich der EG 20 – 24 ePrivacy-VO-E sind damit ausdrücklich Informationen, die im Zusammenhang mit Tracking Tools wie Cookies gewonnen werden, gemeint. Nach den Vorgaben des e-Privacy-VO-E sollen Cookies nur mit der Einwilligung der Nutzer gesetzt werden können, Art. 8 Abs. 1 lit. b ePrivacy-VO-E; davon ausgenommen sind jedoch solche Tools, die nötig sind zur Bereitstellung eines vom Endnutzers gewünschten Dienstes der Informationsgesellschaft, Art. 8 Abs. 1 lit. c ePrivacy-VO-E.

---

583 *Schmidt/Babilon*, K&R 2016, 86, 90.

584 *Schroeder*, in: Streinz, EUV/AEUV, Art. 288 AEUV, Rn. 120 m. w. N.; i. Ü. gilt dies auch soweit die nationalen Gerichte die Normen für unionsrechtswidrig halten, vgl. *EuGH,* Urt. v. 19.01.2010, Rs. C-555/07, ECLI:EU:C:2010:21, Rn. 51 ff. – Kükükdeveci.

585 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final, abrufbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52017PC0010&from=EN (abgerufen am 13.10.2017).

586 Vgl. auch COM(2017) 10 final, Pkt. 1.2.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Beispielhaft nennt EG 21 ePrivacy-VO-E Session-Cookies, die die Nutzereingaben bei Online-Formularen über mehrere Seiten hinweg speichern. Bereits unter der ePrivacy-RL gilt eine Ausnahme von dem Einwilligungserfordernis, soweit es sich um Tracking Tools handelt, die erforderlich sind, um einen Dienst der Informationsgesellschaft zur Verfügung zu stellen. Dazu gehören bereits nach Maßgabe des Art. 5 Abs. 3 ePrivacy-RL auch die oben genannten Cookies, die beispielsweis erforderlich sind, um die Eingaben in Online-Formulare für die Dauer der Sitzung zu speichern.[587]

Ferner sieht Art. 9 Abs. 2 ePrivacy-VO-E vor, dass die Einwilligung durch Browsereinstellungen gegeben werden kann; als Begründung hierfür geht EG 22 auf die bislang übliche Vorgehensweise von Bannern mit einer Aufforderung zur Einwilligung in die Nutzung von Cookies auf Websites ein. Mit Bezug auf sog. Third Party-Tracking Tools bestimmt Art. 10 Abs. 1 ePrivacy-VO-E ferner, dass Nutzern künftig die Möglichkeit gegeben werden sollte, bereits in den Voreinstellungen ihrer Software – etwa ihrem Browser – dem Einsatz solcher Tracking Tools durch Dritte ihre Einwilligung auszudrücken, vgl. EG 24 ePrivacy-VO-E.

Das bedeutet, dass die ePrivacy-VO ebenso wie die ePrivacy-RL zunächst von einem strengen Einwilligungsvorbehalt ausgeht. Die Möglichkeit der Einwilligung über die Browser-Einstellungen könnte hierbei eine Erleichterung für den Nutzer darstellen, indem er nicht bei jeder Website erneut in die Nutzung von Tracking Tools zustimmen muss. Insbesondere könnte es die Möglichkeit der informierten Einwilligung erhöhen, wenn der Nutzer nicht regelmäßig seine Einwilligung erteilen muss, sondern dies durch eine einmalige, aber bedachte Handlung erfolgen kann. Allerdings birgt diese Möglichkeit gerade bei unerfahrenen Internetnutzern die Gefahr, dass diese die Browser-Einstellungen nicht eingehend zu bedienen wissen. Art. 10 Abs. 2 ePrivacy-VO-E sieht zwar vor, dass die Software bei der Installation den Nutzer umfassend über die Einstellungsmöglichkeiten informieren muss. Die Wirksamkeit in der Praxis wird jedoch entscheidend von der tatsächlichen Umsetzung abhängen. Sollte die Information durch die Software sich als recht lang oder besonders komplex erweisen, wird der Nutzen dieser Information wohl gering ausfallen.

587 *Rauer/Ettig*, ZD 2014, 27, 29; kritisch zum Begriff "nötig" i. S. d. Art. 8 Abs. 1 ePrivacy-VO-E vgl. *Engeler/Felber*, ZD 2017, 251, 254 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

II. Zulässigkeit der Verarbeitung durch Einwilligung

Obwohl teilweise, insbesondere für Fälle des Adresshandels und der Werbung,[588] gesetzliche Erlaubnistatbestände für die Verarbeitung personenbezogener Daten bestehen, zeigt die bisherige Untersuchung, dass das hauptsächliche Legitimationsmittel für die Verarbeitung personenbezogener Daten durch die Plattformbetreiber die Einwilligung ist. Angaben zur Einwilligung finden sich im BDSG in § 4a, die teilweise durch § 13 Abs. 2 TMG modifiziert werden. Während die inhaltlichen Vorgaben des § 4a BDSG auch für die Einwilligung nach dem TMG gelten,[589] kann die Einwilligung i. S. d. § 13 Abs. 2 TMG elektronisch erklärt werden, unterliegt also nicht dem Schriftformerfordernis des BDSG.

In der DSGVO finden sich Bestimmungen über die Einwilligung in Art. 4 Nr. 11, Art. 7, 8 sowie als Zulässigkeitsnorm in Art. 6 Abs. 1 S. 1 lit. a. Die inhaltlichen Voraussetzungen der Freiwilligkeit, Bestimmtheit und Informiertheit der Einwilligung gelten dabei gleichermaßen für die Einwilligung nach dem BDSG und der Einwilligung nach der DSGVO, allerdings mit gewissen Unterschieden.[590] Ferner muss der Nutzer über ein Einwilligungsbewusstsein verfügen.[591]

1. Inhaltliche Anforderungen

a) Freiwilligkeit

Zunächst müsste die Einwilligung freiwillig erfolgen, vgl. § 4a Abs. 1 S. 1 BDSG bzw. Art. 2 lit. h DSRL sowie Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO. Besonders interessant im Anbieter-Nutzer-Verhältnis ist die Frage, ob die Einwilligung freiwillig erteilt wurde unter dem Aspekt eines (vermeintlichen) Machtungleichgewichts zwischen dem Plattformbetreiber und dem Nutzer. Denn wenn der Nutzer lediglich vor der Wahl steht, seine Einwilligung zu erteilen oder auf den Dienst zu verzichten – in Sinne von „take it or leave it“[592] – kann die Freiwilligkeit der Einwilligung in Frage gestellt sein. Der Gesetzgeber hat in § 28 Abs. 3b S. 1 BDSG für Fälle des Adress-

588 Vgl. Kap. 3 Pkt. B.I.2.b.aa.ii, S. 170.
589 *Moos*, in: Taeger/Gabel, BDSG, TMG, § 12, Rn. 24.
590 Vgl. bereits ausführlich Kap. 3 Pkt. A.III.3, S. 130.
591 Vgl. *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 7, Rn. 56.
592 *Buchner*, DuD 2015, 402, 404.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

handels und der Werbung ein Koppelungsverbot festgesetzt, d. h. der Abschluss eines Vertrags darf unter bestimmten Voraussetzungen nicht von der Erteilung der Einwilligung abhängig gemacht werden. Die DSGVO geht in Art. 7 Abs. 4 sogar noch einen Schritt weiter, und legt für die Beurteilung der Freiwilligkeit generell als Maßstab die Frage an, ob die Erfüllung eines Vertrags von der Einwilligung abhängig gemacht wurde.

aa) Koppelungsverbot i. S. d. § 28 Abs. 3b BDSG

Gem. § 28 Abs. 3b S. 1 BDSG darf der Vertragsschluss nicht von der Einwilligung abhängig gemacht werden, wenn der Betroffene keinen Zugang zu anderen gleichwertigen vertraglichen Leistungen hat oder dieser Zugang nicht in zumutbarer Weise offensteht.

Mit dem Abhängigmachen ist die eingangs beschriebene „take it or leave it"-Situation gemeint: Der Betroffene willigt entweder in den Umgang mit personenbezogenen Daten ein oder der Vertragsschluss kommt nicht zustande. Fraglich ist, wann i. S. d. § 28 Abs. 3b S. 1 BDSG der Betroffene keinen Zugang zu gleichwertigen vertraglichen Leistungen hat oder jedenfalls dieser Zugang dem Betroffenen nicht zumutbar ist. Die Zumutbarkeit entfällt entweder aufgrund der marktbeherrschenden Stellung des Unternehmens[593] oder wenn der Betroffene aufgrund der Gesamtsituation auf dem Markt jeweils nur durch Erteilung seiner Einwilligung Zugang zu gleichwertigen Angeboten hat.[594]

i) Nutzerinteressen als Maßstab für die Gleichwertigkeit

Fraglich ist, wann bei sozialen Netzwerken ein alternatives Angebot als „gleichwertig" gilt. Mit Blick auf soziale Netzwerke haben sich immer wieder Angebote entwickelt, die mit erhöhtem Datenschutz werben.[595] Gleichwohl bleibt *Facebook* unter deutschen Nutzern das soziale Netzwerk mit

593 BT-Drucks. 16/12011, S. 2, 30.

594 *Pauly/Ritzer*, WM 2010, 8, 13; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 39.

595 So war das soziale Netzwerk *Ello* ursprünglich als Alternative zu *Facebook* konzipiert, ist inzwischen jedoch von diesem Konzept beinahe vollständig abgerückt und nun als Plattform für Kunst und Künstler aktiv, vgl. *Ello PBC,* The Creators Network — Visibility. Influence. Opportunity., abrufbar unter https://ello.co/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

den höchsten Nutzerzahlen. Daher ist fraglich, ob die Gleichwertigkeit anhand der Funktionalität zu beurteilen ist, oder von den Nutzerzahlen des sozialen Netzwerks abhängt. Die Interaktion unter Freunden oder Bekannten ist gerade zentrales Element eines sozialen Online-Netzwerks, da sich soziale Netze aus der Realwelt in sozialen Online-Netzwerken fortsetzen.[596] Im Umkehrschluss lässt sich daraus schließen, dass es für die Beurteilung der Gleichwertigkeit nicht darauf ankommt, dass das alternative Angebot in jeder Hinsicht identische Funktionen anbietet. Entscheidend ist vielmehr, dass ein soziales Netzwerk für einen Nutzer dann seine volle Funktionalität entfaltet, wenn möglichst viele seiner sozialen Kontakte aus der Realwelt dasselbe Netzwerk nutzen. Somit könnte auch ein Messenger-Dienst ein gleichwertiges Angebot zu einem sozialen Netzwerk sein, sofern es in der entsprechenden Nutzergruppe vergleichbare Nutzerzahlen aufweist. Dafür spricht auch die Tatsache, dass seit einiger Zeit verschiedene Hybridangebote, die Elemente aus Messenger-Diensten und klassischen sozialen Netzwerken kombinieren,[597] sehr hohe Nutzerzahlen verzeichnen.[598]

ii) Zumutbarkeit

Die Beurteilung der Gleichwertigkeit greift bei sozialen Online-Netzwerken mit der Beurteilung der Zumutbarkeit der Inanspruchnahme solcher Alternativangebote eng ineinander. Ob die Inanspruchnahme datenschutzstarker Alternativangebote den Nutzern zumutbar ist, muss mit Blick auf die Nutzer selbst entschieden werden. So ist bereits seit einigen Jahren ein Aufstreben einer Vielzahl von Angeboten im Social Web zu verzeichnen, die parallel Nutzerzahlen in Millionen- oder gar Milliardenhöhe vorweisen

596 *Wirz,* Nähe-orientiertes Handeln in den Weiten des Web, in: Neumann-Braun/Autenrieth, S. 135; vgl. hierzu bereits Kap. 3 Pkt. A.III.3.a.aa.i, S. 132.

597 Vgl. Kap. 1 Pkt. B.I, S. 33.

598 Vgl. etwa *Snapchat* mit 150 Mio. täglich aktiven Nutzern, das Merkmale klassischer sozialer Netzwerke mit Messengermerkmalen vereint, *Statista GmbH*, Statistiken zum Instant-Messaging-Dienst Snapchat, abrufbar unter https://de.statista.com/themen/2546/snapchat/ (abgerufen am 13.10.2017); *WhatsApp* mit 1,3 Mrd. Nutzern, das neben der klassischen Messenger-Funktion auch die Möglichkeit bietet, Status-Updates hochzuladen, die alle Kontakte gleichermaßen einsehen können, *Statista GmbH*, Anzahl der monatlich aktiven Nutzer von WhatsApp weltweit in ausgewählten Monaten von April 2013 bis Juli 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

können.[599] Daraus kann geschlossen werden, dass Nutzer tendenziell bereit sind, sich bei mehr als einem Netzwerk anzumelden und mehr als einen Dienst zu nutzen und somit nicht auf die Nutzung eines einzigen, marktbeherrschenden Netzwerks angewiesen sind. Das lässt den Schluss zu, dass es dem mündigen Nutzer zuzutrauen ist, bei persönlicher Präferenz nach hohem Datenschutz die durchaus existierenden Alternativen in Betracht zu ziehen, möglicherweise sogar seine Freunde dazu zu animieren, sich ebenfalls bei entsprechenden alternativen Angeboten anzumelden. Wer sich jedoch aus eigenen Stücken entscheidet, Datenschutz im Gegenzug für eine bestimmte Dienstleistung aufzugeben, dem sollte dies auch möglich sein.[600] Ein allzu streng verstandenes Koppelungsverbot, das im Zuge staatlicher „Fürsorge" dem Nutzer dieses Wahlrecht unabhängig von seinem tatsächlichen Willen nimmt, würde den Nutzer in seinem Recht auf informationelle Selbstbestimmung zu sehr einschränken.[601]

iii) Strenger Maßstab bei Minderjährigen

Allerdings darf trotz dieses Einwands die tatsächliche Sogwirkung sozialer Netzwerke durch ihre Bedeutung für die Imagepflege insbesondere für Jugendliche[602] nicht verkannt werden. Es spricht daher einiges dafür, dass das Koppelungsverbot bei Minderjährigen streng verstanden werden muss. Denn durch die Bedeutung sozialer Online-Netzwerke für Jugendliche und junge Erwachsene kann bei dieser Nutzergruppe das Fernbleiben von bestimmten sozialen Online-Netzwerken stärkere Auswirkungen haben als bei Erwachsenen. Bei dieser Nutzergruppe müssen bei der Beurteilung der

599 Vgl. etwa *Snapchat* mit 150 Mio. täglich aktiven Nutzern, *Statista GmbH*, Statistiken zum Instant-Messaging-Dienst Snapchat, abrufbar unter https://de.statista.com/themen/2546/snapchat/ (abgerufen am 13.10.2017); *Instagram* mit 700 Mio. monatlich aktiven Nutzern, *Statista GmbH*, Anzahl der monatlich aktiven Instagram Nutzer weltweit in ausgewählten Monaten von Januar 2013 bis April 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/300347/umfrage/monatlich-aktive-nutzer-mau-von-instagram-weltweit/ (abgerufen am 13.10.2017); *WhatsApp* mit mehr als einer Mrd. Nutzer, *Statista GmbH*, Anzahl der aktiven Nutzer von WhatsApp weltweit von April 2013 bis Februar 2016 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/ (abgerufen am 13.10.2017).

600 Kritisch jedoch *Rost*, DuD 2013, 85, 86.

601 Ähnlich *Buchner*, DuD 2010, 39, 43; *Krönke*, Der Staat 2016, 319, 327, 334.

602 Vgl. Kap. 3 Pkt. A.III.3.a.aa.i, S. 132.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Gleichwertigkeit und Zumutbarkeit also die Nutzerzahlen in den in Frage stehenden sozialen Netzwerken mehr Beachtung finden als bei volljährigen Nutzern.

bb) Koppelungsverbot i. S. d. Art. 7 Abs. 4 DSGVO als Auslegungskriterium

Zur Beurteilung der Freiwilligkeit legt Art. 7 Abs. 4 DSGVO einen Maßstab zugrunde, den man nach deutschem Verständnis als allgemeines Koppelungsverbot bezeichnen kann:[603] „[I]n größtmöglichem Umfang" soll dem Umstand Rechnung getragen werden, ob der Vertragsschluss – und dazu zählt Art. 7 Abs. 4 DSGVO ausdrücklich die Erbringung einer Dienstleistung – „[…] von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind." EG 43 S.1 DSGVO bestimmt ferner, dass bei Vorliegen eines „klare[n] Ungleichgewicht[s]" die Einwilligung keine Legitimationsgrundlage liefern soll; als Beispiel eines klaren Ungleichgewichts nennt EG 43 S. 1 DSGVO eine Behörde als Verantwortliche, beschränkt sich jedoch nicht auf diese Fälle. Dennoch bietet dieses Beispiel des Verhältnisses zwischen Staat und Bürger einen Anhaltspunkt für den Maßstab, der bei der Beurteilung des Vorliegens eines Ungleichgewichts angelegt werden soll.[604] Ein klares Ungleichgewicht kann zwar auch zwischen Privaten bestehen. Allerdings ist hierbei zu berücksichtigen, dass das Beispiel des Verhältnisses zwischen Arbeitnehmer und Arbeitgeber, das EG 34 des Kommissionsentwurfs der DSGVO[605] noch angeführt hatte, nicht in die endgültige Fassung aufgenommen wurde. Dies lässt darauf schließen, dass das Vorliegen eines Ungleichgewichts nicht vorschnell angenommen werden sollte, selbst dann nicht, wenn ein Abhängigkeitsverhältnis zwischen dem Verantwortlichen und dem Betroffenen besteht.[606] Zwischen Plattformbetreibern und Nutzern ist nach diesen Kriterien wohl regelmäßig kein klares Ungleichgewicht i. S. d. EG 43 S. 1 DSGVO anzunehmen, da hier kein mit

---

603 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 7, Rn. 41; *Frenzel*, in: Paal/Pauly, DSGVO, Art. 7, Rn. 18; a. A. Stemmer, in: BeckOK DatenschutzR, DSGVO, Art. 7, Rn. 40.

604 Ähnlich *Schulz*, in: Gola, DSGVO, Art. 7, Rn. 21.

605 KOM(2012) 11 endgültig.

606 i. E. ähnlich *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 7, Rn. 44.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

der Entscheidungs- und Sanktionsmacht von Behörden gegenüber dem Bürger vergleichbares Machtgefälle besteht.[607] Darüber hinaus hat der Nutzer, wie bereits ausgeführt,[608] im Angesicht von den inzwischen zahlreich bestehenden Alternativen regelmäßig die Wahl, ob er den Dienst in Anspruch nimmt oder nicht.[609]

Zudem lässt der Wortlaut des Art. 7 Abs. 4 DSGVO darauf schließen, dass selbst bei Vorliegen eines Abhängigmachens und der fehlenden Erforderlichkeit der personenbezogenen Daten für die Vertragserfüllung die Einwilligung nicht zwingend unwirksam ist. Denn während in Art. 7 Abs. 4 des Kommissionsentwurfs noch klar formuliert wurde, dass die Einwilligung bei „erhebliche[m] Ungleichgewicht[ ]" keine Rechtsgrundlage für die Verarbeitung bietet und Art. 7 Abs. 4 des Parlamentsentwurfs[610] bestimmte, dass die Vertragserfüllung nicht von der Einwilligung bei fehlender Erforderlichkeit der Datenverarbeitung für die Vertragserfüllung abhängig gemacht werden „darf", ist Art. 7 Abs. 4 DSGVO deutlich offener formuliert: Nunmehr soll dem Umstand des Abhängigmachens und der fehlenden Erforderlichkeit nur „[…] in größtmöglichem Umfang Rechnung getragen werden […]". Art. 7 Abs. 4 DSGVO schreibt also, anders als seine Vorgänger, die Rechtsfolge der Unwirksamkeit nicht automatisch vor,[611] sondern stellt sich vielmehr als Auslegungsstütze für das Freiwilligkeitskriterium dar.

Fraglich ist, wann die Verarbeitung personenbezogener Daten für die Vertragserfüllung erforderlich ist. Denn man könnte argumentieren, dass die Verarbeitung personenbezogener Daten gerade das Geschäftsmodell von sozialen Netzwerken ist und demnach erforderlich für die Vertragserfüllung ist.[612] Dieses Verständnis des Erforderlichkeitsgrundsatzes bricht

---

607 Ebenso *Krönke*, Der Staat 2016, 319, 345, für sämtliche Fallgruppen der Datenverarbeitung durch Private.

608 Kap. 3 Pkt. B.II.1.a.aa, S. 183.

609 So auch *Kipker/Voskamp*, DuD 2012, 737, 738, die darauf abstellen, ob „[…] der Betroffene […] sich als vernünftig denkender Mensch Sorgen über mögliche Konsequenzen machen müsste, sollte er der Aufforderung, seine Einwilligung in die Datenverarbeitung zu erteilen, nicht nachkommen."

610 Art. 7 Abs. 4 des Parlamentsentwurfs der DSGVO, P7_TA(2014)0212.

611 Ähnlich *Schneider,* Datenschutz nach der EU-Datenschutz-Grundverordnung, S. 142 f.

612 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 7, Rn. 48, 51 allerdings mit der Maßgabe, dass dem Nutzer die kommerzielle Verwertung seiner personenbezogenen Daten im Tausch gegen die Nutzungsmöglichkeit des vermeintlich „kostenlosen" Angebots dargelegt werden muss; *Frenzel*, in: Paal/Pauly, DSGVO, Art. 7, Rn. 21.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

mit dem – jedenfalls nach deutschem Verständnis – tendenziell streng verstandenen Erforderlichkeitsgrundsatz.[613] Auf Ebene der DSGVO sprechen zudem systematische Gründe gegen diese Auslegung: Bei einer solch weiten Auslegung des Erforderlichkeitskriteriums stellt sich das Problem, dass damit i. S. d. Art. 6 Abs. 1 S. 1 lit. b DSGVO mit Hinweis auf die „Erforderlichkeit" der Datenverarbeitung zur Umsetzung des Geschäftsmodells bereits sämtliche Datenverarbeitungen durch Plattformbetreiber legitimiert wären, und die in Art. 6 Abs. 1 S. 1 lit. f DSGVO vorgesehene Interessenabwägung so umgangen werden könnte. Eine Einwilligung der Nutzer wäre dann unter Umständen gar nicht mehr nötig.[614]

Gleichzeitig birgt ein streng angelegter Erforderlichkeitsmaßstab das Problem, dass das Tauschmodell „Dienstleistung gegen personenbezogene Daten" nicht mehr möglich wäre und das Geschäftsmodell sozialer Netzwerke praktisch der Vergangenheit angehörte. Dies würde nicht nur einen besonders starken Eingriff in die unternehmerische Freiheit der Plattformbetreiber bedeuten, sondern wäre auch kaum im Sinne der Nutzer: Die Tatsache, dass trotz anhaltender Kritik an mangelndem Datenschutz *Facebook* der führende Anbieter sozialer Netzwerke ist,[615] lässt darauf schließen, dass nach Präferenz der Nutzer die Datenschutzbedenken den Zugriff auf das soziale Netzwerk nicht überwiegen, der Zugang zum sozialen Netzwerk von vielen Nutzern also höher bewertet wird als der Datenschutz. Stimmen, dass die Freiwilligkeit stets dann nicht gegeben ist, wenn personenbezogene Daten im Tausch gegen eine Dienstleistung gehandelt werden,[616] können vor diesem Hintergrund nicht überzeugen.

Dogmatisch ist dieser Konflikt dahingehend aufzulösen, dass, wie eingangs dargelegt, Art. 7 Abs. 4 DSGVO keine starre Unwirksamkeitsfolge festlegt, sondern lediglich eine Auslegungshilfe darstellt. Es spricht deswegen einiges dafür, dass neben der Erforderlichkeit noch andere Kriterien zu Rate gezogen werden, etwa ähnlich den Kriterien des § 28 Abs. 3b S. 1 BDSG.[617]

---

613 Vgl. zur Auslegung des Erforderlichkeitskriteriums bereits die Ausführungen bei Kap. 3 Pkt. B.I.2.a.aa.ii, S. 164.

614 Vgl. bereits die Kritik an dieser Auslegung bei Kap. 3 Pkt. B.I.2.a.bb, S. 167.

615 *Statista GmbH*, Aktuelle Statistiken zum Thema Soziale Netzwerke, abrufbar unter https://de.statista.com/themen/1842/soziale-netzwerke/ (abgerufen am 13.10.2017).

616 *Kamp/Rost*, DuD 2013, 80, 82.

617 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 7, Rn. 52; vgl. Kap. 3 Pkt. B.II.1a.aa, S. 183.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Informiertheit und Bestimmtheit

Die Einwilligung muss auch informiert und bestimmt erfolgen, § 4a Abs. 1 S. 2 BDSG bzw. Art. 2 lit. h, Art. 7 lit. a DSRL sowie Art. 4 Nr. 11 DSGVO, Art. 6 Abs. 1 S. 1 lit. a DSGVO. Die Informationspflicht bezieht sich auf jeden beabsichtigten Umgang mit personenbezogenen Daten.[618] Im Zusammenhang mit der Informiertheit der Einwilligung durch den Betroffenen wird kritisiert, dass im Angesicht langer, komplizierter und oftmals mehrteiliger Datenschutzerklärungen eine Informiertheit der Nutzer bloße Fiktion ist.[619] Als regelmäßig kritisiertes Negativbeispiel dient das soziale Netzwerk *Facebook*. Möchte ein Nutzer sich dort erstmalig registrieren, steht in kleingedruckter Schrift über dem „Registrieren"-Button: „Indem du auf „Registrieren" klickst, erklärst du dich mit unseren Nutzungsbedingungen einverstanden und bestätigst, dass du unsere Datenrichtlinie einschließlich unserer Cookie-Richtlinie gelesen hast. […]"[620] Angesichts dieser Formulierung ist schon fraglich, ob der Nutzer über das nötige Einwilligungsbewusstsein verfügt.[621] Denn die Einwilligung wird nur für die Nutzungsbedingungen verlangt, während der Nutzer lediglich bestätigt, dass er die Datenschutzbestimmungen „[…] gelesen hat […]".[622] Abgesehen davon ist es selbst für den engagierten Leser schwierig, sich aus dem Zusammenspiel aus Nutzungsbedingungen[623], Datenrichtlinie[624] sowie Cookie-Richtlinie[625] ein Bild über die genau beabsichtigte Verwendung der Daten zu machen.[626] Weitergehend stand *Facebook* in der Vergangenheit in der Kritik, Informationen unvollständig oder gar nicht preiszugeben.[627]

---

618 *Simitis*, in: Simitis, BDSG, § 4a, Rn. 72.

619 Vgl. etwa *Pollmann/Kipker*, DuD 2016, 378; *Arnold/Hillebrand/Waldburger*, DuD 2015, 730; i E. ähnlich *Ernst*, ZD 2017, 110, 113.

620 *Facebook Inc.,* Registrieren, abrufbar unter https://de-de.facebook.com/ (abgerufen am 13.10.2017).

621 Vgl. Kap. 3 Pkt. B.II.2.a, S. 190.

622 Kritisch *Düsseldorfer Kreis*, Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen; ebenso *Piltz,* Soziale Netzwerke im Internet, S. 154 f.

623 *Facebook Inc.,* Erklärung der Rechte und Pflichten, abrufbar unter https://www.facebook.com/legal/terms (abgerufen am 13.10.2017)

624 *Facebook Inc.,* Datenrichtlinie, abrufbar unter https://www.facebook.com/about/privacy (abgerufen am 13.10.2017).

625 *Facebook Inc.,* Cookies und andere Speichertechnologien, abrufbar unter https://www.facebook.com/policies/cookies/ (abgerufen am 13.10.2017).

626 Ausführlich *Buchner*, DuD 2015, 402, 403 ff.

627 Vgl. etwa *LG Berlin,* Urt. v. 28.10.2014, Az. 16 O 60/13, ZD 2015, 133; *Kühnl,* Persönlichkeitsschutz 2.0, S. 173 f. m. w. N.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

2. Anforderungen an die Form, insbesondere elektronische „opt-in"-Einwilligung

a) Formvorgaben des TMG und BDSG

Hinsichtlich der Formvorgaben ist zunächst zu klären, welche Vorgaben im TMG und BDSG für die Einwilligung der Nutzer gegenüber den Plattformbetreibern einschlägig sind. Angaben zur vorgeschriebenen Form der Einwilligung finden sich in § 4a BDSG sowie in § 13 Abs. 2 TMG. Während für die inhaltlichen Vorgaben des § 4a BDSG auch die Einwilligung nach dem TMG gilt,[628] ist eine Besonderheit des § 13 Abs. 2 TMG, dass die Einwilligung elektronisch erklärt werden kann und damit nicht dem Schriftformerfordernis des BDSG unterliegt. § 13 Abs. 2 TMG ist in konsequenter Anwendung der Trennung nach Bestands-, Nutzungs- und Inhaltsdaten[629] nur auf sog. Nutzungs- und Bestandsdaten anwendbar; für Inhaltsdaten gelten hingegen die Anforderungen des BDSG.[630] Aufgrund der Unvereinbarkeit der Erlaubnistatbestände der §§ 14 Abs. 1, 15 Abs. 1 TMG mit Art. 7 DSRL stellt sich die Frage, ob auch die Vorschrift des § 13 Abs. 2 TMG nicht mehr anwendbar ist. Allerdings widerspricht § 13 Abs. 2 TMG selbst nicht den Vorgaben der DSRL; insbesondere ist das Schriftformerfordernis aus § 4a Abs. 1 S. 3 BDSG nicht durch die DSRL vorgeschrieben.[631] Dies führt auch nicht zu Wertungswidersprüchen, da in Bezug auf soziale Netzwerke die elektronische Einwilligung ohnehin wegen „besonderer Umstände" i. S. d. § 4a Abs. 1 S. 3 BDSG möglich ist.[632] Das bedeutet, dass sowohl für Bestands-, Nutzungs-, als auch Inhaltsdaten die Einwilligung elektronisch möglich ist.

Gem. § 13 Abs. 2 TMG muss der Nutzer seine Einwilligung bewusst und eindeutig erklären, die Einwilligung muss protokolliert werden und der Nutzer muss den Inhalt der Einwilligung jederzeit abrufen können. Zudem muss der Nutzer seine Einwilligung jederzeit frei widerrufen können.

Nach dem Wortlaut des § 13 Abs. 2 Nr. 1 TMG wird verlangt, dass die Einwilligung „bewusst und eindeutig" zu ergehen hat. Dies wirft die Frage

---

628 *Moos*, in: Taeger/Gabel, BDSG, TMG, § 12, Rn. 24.
629 Vgl. zu dieser Unterscheidung Kap. 3 Pkt. B.I.1.a.dd, S. 158.
630 *Moos*, in: Taeger/Gabel, BDSG, TMG, § 13, Rn. 18; *Piltz,* Soziale Netzwerke im Internet, S. 123 ff.; *Achtruth,* Der rechtliche Schutz bei der Nutzung von Social Networks, S. 143 f.; *Kühnl,* Persönlichkeitsschutz 2.0, S. 177.
631 Vgl. Kap. 3 Pkt. A.III.3.cc, S. 138.
632 Vgl. oben Kap. 3 Pkt. A.III.3.a.cc, S. 138.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

auf, ob sog. „opt-out"-Einwilligungen, d. h. die vorformulierte Einwilligung, die der Nutzer explizit verweigern muss statt sie explizit zu erteilen, i. S. d. § 13 Abs. 2 TMG möglich sind. Wie ausgeführt, sind i. S. d. DSRL auch mündliche oder konkludente Einwilligungen möglich. Erforderlich ist jedoch, dass gesichert ist, dass der Betroffene über das erforderliche Einwilligungsbewusstsein verfügt und die Einwilligung informiert und bewusst erfolgt. Bei „opt-out"-Einwilligungen, gerade in Verbindung mit weiteren vertraglichen Ausführungen, besteht jedoch die Gefahr, dass der Einwilligende nicht das nötige Einwilligungsbewusstsein hat, etwa, weil er die Einwilligungsbestimmung übersieht. Für Einwilligungen i. S. d. § 4a BDSG sind nach Rechtsprechung des *BGH* allerdings sog. „opt-out"-Einwilligungen wirksam.[633] Vor dem Hintergrund des Art. 7 lit. a DSRL, der eine Einwilligung „ohne jeden Zweifel" verlangt, ist dies kritisch zu sehen. Zudem setzt auch die Einwilligung i. S. d. § 4a BDSG ein Einwilligungsbewusstsein voraus. Bei „opt-out"-Einwilligungen liegt dieses Bewusstsein aber nicht gesichert vor.[634]

Angesichts des Wortlauts des § 13 Abs. 2 TMG wird für Einwilligungen nach dem TMG vertreten, dass die „opt-in"-Einwilligung nötig ist.[635] Europarechtlich indiziert ist dies jedoch nur hinsichtlich des Einwilligungsbewusstseins; eine tatsächliche Formvorgabe gibt es dahingehend nicht. Dennoch ist die „opt-in"-Einwilligung zu befürworten, um eine bewusste Einwilligung des Betroffenen sicherzustellen. Dies gilt auch für elektronisch erteilte Einwilligungen nach § 4a BDSG. Denn das Abrücken vom strengen Schriftformerfordernis erfordert das Greifen anderer Mechanismen, die sicherstellen, dass der Betroffene sich über die Abgabe einer Einwilligung und deren Folgen bewusst ist. Die aktive Einwilligung im Gegensatz zum „opt-out"-Modell ist demnach erforderlich.

b) Formvorgaben der DSGVO

Wie bereits dargelegt, kennt die DSGVO kein Schriftformerfordernis. Allerdings verlangt Art. 4 Nr. 11 DSGVO, dass die Einwilligung „[…] in un-

---

633 *BGH,* Urt. v. 16.07.2008, Az. VIII ZR 348/06, BGHZ 177, 253 – Payback; *BGH,* Urt. v. 11.11.2009, Az. VIII ZR 12/08, DuD 2010, 493 – HappyDigits.

634 Kritisch zur *BGH*-Rspr. *Buchner*, DuD 2010, 39, 42.

635 *Moos*, in: Taeger/Gabel, BDSG, TMG, § 13, Rn. 21; *Kühnl,* Persönlichkeitsschutz 2.0, S. 175 f.; i. E. ebenso *Spindler/Nink*, in: Spindler/Schuster, Recht der elektronischen Medien, TMG, § 13, Rn. 13.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

missverständlicher Weise […]“ abgegeben wurde. EG 32 S. 1 DSGVO präzisiert dieses Erfordernis dahingehend, dass eine „[…] eindeutige bestätigende Handlung erfolgen […]“ muss. Explizit legen EG 32 S. 2, 3 DSGVO ferner dar, dass diese Anforderungen durch das Anklicken eines Kästchens erfüllt sind (S. 2) und bereits zuvor angeklickte Kästchen nicht ausreichend sind (S. 3). Hier zeichnet sich also ein klarer Wandel zur bisherigen Rechtslage in Deutschland ab; die bisher durch den *BGH* gebilligte „opt-out“-Einwilligung ist mit der DSGVO nicht mehr möglich.[636]

c) Formvorgaben bei Tracking Tools

Fraglich ist, welche Formvorgaben für die Einwilligung in das Setzen und Nutzen von Tracking Tools wie Cookies gelten. Inzwischen ist die Verwendung von Informationsbannern, dass die Website Cookies verwendet, durchaus übliche Praxis. Hierbei wird teilweise informiert, dass ein Verweilen als Zustimmung gewertet wird und teilweise wird eine aktive Einwilligung mittels eines Klicks gefordert.

aa) Formvorgabe durch die ePrivacy-RL als Ergänzung zur DSRL

Gem. Art. 5 Abs. 3 ePrivacy-RL muss der Nutzer seine Einwilligung in die Verwendung von Cookies „[…] auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält […]“ geben. Das bedeutet, dass die Anforderungen der Einwilligung in die Nutzung von Cookies grundsätzlich denen der Einwilligung nach der DSRL entspricht, die Einwilligung also ebenfalls „ohne jeden Zweifel“ i. S. d. Art. 7 lit. a DSRL gegeben werden muss. EG 66 der RL 2009/136/EG präzisiert zudem, dass, „[…] [w]enn es technisch durchführbar und wirksam ist […]“ die Einwilligung über die Browser-Einstellungen gegeben werden kann. Die Einwilligung mittels Browser-Einstellungen sieht die Art. 29-Datenschutzgruppe dann als geeignetes Mittel, wenn der Verantwortliche davon ausgehen darf, dass der Nutzer umfas-

636 Ebenso *Buchner/Kühling* in: Kühling/Buchner, DSGVO, Art. 7, Rn. 58; *Albrecht/Jotzo,* Das neue Dateschutzrecht der EU, S. 70.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

send informiert und aktiv seine Browser-Einstellungen dahingehend konfiguriert hat.[637] Nach derzeitigem Stand ist diese Methode der Einwilligungseinholung aber wohl regelmäßig kein geeignetes Mittel, um eine informierte, bestimmte und bewusste Einwilligung sicherzustellen.

Ferner verlangt die Art. 29-Datenschutzgruppe ein aktives Verhalten, etwa das Klicken auf einen Link oder Anklicken eines Kästchens.[638] Vor diesem Hintergrund sieht sie Informationsbanner auf Websites zur Verwendung von Cookies zwar als geeignetes Mittel an, empfiehlt jedoch, dass dieses Banner nicht verschwinden sollte, bevor der Nutzer seine Einwilligung mittels eines Klicks gegeben hat.[639] Allerdings ist, wie dargestellt, das Erfordernis eines Klicks keine explizite Vorgabe der DSRL und auch nicht der ePrivacy-RL, sondern vielmehr ein Mittel zur Sicherstellung, dass der Nutzer tatsächlich „ohne jeden Zweifel" i. S. d. Art. 7 lit. a DSRL eingewilligt hat. Vor diesem Hintergrund wird teilweise vertreten, dass ein Verweilen auf der Website, wenn der Banner darüber informiert, dass ein solches Verhalten als Zustimmung gewertet wird, als aktives Verhalten i. S. d. genannten Vorgaben der Art. 29-Datenschutzgruppe zu werten ist, sofern der Nutzer anschließend weiterhin aktiv auf der Website surft, etwa indem er trotz des Banners in der Website nach unten scrollt.[640] Allerdings ist durchaus zweifelhaft, dass aus diesem Verhalten eine bewusste Einwilligung abgeleitet werden kann. Daher ist auch bei Cookies regelmäßig eine „opt-in"-Einwilligung zu fordern, um sicherzustellen, dass die Betroffenen über das nötige Einwilligungsbewusstsein verfügen.

bb) Formvorgabe durch den ePrivacy-VO-E

Auch der Entwurf der Kommission für eine ePrivacy-VO[641] sieht explizit die Einwilligungsmöglichkeit mittels Browser-Einstellungen vor, Art. 9 Abs. 2 i. V. m. Art. 8 Abs. 1 lit. b ePrivacy-VO-E.

---

637 *Art. 29-Datenschutzgruppe*, Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies. WP 208 (02.10.2013), S. 4 f.

638 *Art. 29-Datenschutzgruppe*, Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies. WP 208 (02.10.2013), S. 4 f.

639 *Art. 29-Datenschutzgruppe*, Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies. WP 208 (02.10.2013), S. 4 f.

640 *Rauer/Ettig*, ZD 2014, 27, 31.

641 COM(2017) 10 final.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Durch die Möglichkeit der Einwilligung mittels Browser-Einstellungen soll explizit den eingangs beschriebenen Bannern auf Websites entgegen gewirkt werden, EG 22 S. 2 ff. ePrivacy-VO-E.

Im Gegensatz zur ePrivacy-RL schreibt der e-Privacy-VO-E allerdings in Art. 10 Abs. 2 bestimmte Bedingungen für die Einstellungsmöglichkeiten in den Browsern vor: Bereits bei der Installation soll Software die Nutzer über die Privatsphäre-Einstellungsmöglichkeiten informieren. Mit dieser Vorgabe könnte das derzeitige Problem gelöst werden, dass sich viele Nutzer ihrer konkreten Browser-Einstellungen gar nicht bewusst sind. Wenn die Vorgaben des Art. 10 ePrivacy-VO-E in der Praxis tatsächlich umgesetzt werden, könnte die Einwilligung mittels Browser-Einstellungen jedenfalls die Anforderungen an die Einwilligung der DSGVO erfüllen.[642] Dies wird jedoch entscheidend von der Art der Information bei Installation der Software abhängen. Sollte sich diese Information als lang oder komplex herausstellen, ist der Nutzen einer solchen Information insbesondere für unerfahrene Nutzer gering und man wird u. U. dann nicht davon ausgehen können, dass die Einwilligung mittels Browser-Einstellungen in informierter Weise erfolgte.

3. Einwilligung eines Kindes i. S. d. DSGVO

Art. 8 Abs. 1 UAbs. 1 S. 1 DSGVO stellt zusätzliche Anforderungen für die Wirksamkeit der Einwilligung durch „Kinder" „[…] gegenüber einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird […]". Art. 8 Abs. 1 UAbs. 1 S. 1 DSGVO regelt die Einwilligungsfähigkeit Minderjähriger: Wer das 16. Lebensjahr vollendet hat, kann selbst in die Verarbeitung seiner personenbezogenen Daten einwilligen. Damit setzt die DSGVO, anders als das BDSG, eine Altersgrenze fest, ab welcher der Jugendliche selbst einwilligen kann. Bisher kam es bei der Einwilligung durch einen Minderjährigen allein auf dessen Urteils- und Einsichtsfähigkeit an.[643] Hat der Minderjährige das 16. Lebensjahr noch nicht vollendet, soll es gem. Art. 8 Abs. 1 UAbs. 1 S. 2 DSGVO hingegen auf die Einwilligung durch die Eltern bzw. den gesetzlichen Vertreter des Kindes

642 Vgl. Kap. 3 Pkt. A.III.3.b, S. 142 sowie Kap. 3 Pkt. B.II, S. 182.

643 Vgl. *BVerfG,* Beschl. v. 10.02.1960, Az. 1 BvR 526/53, 1 BvR 29/58, BVerfGE 10, 302 – Aufenthaltsbestimmungsrecht des Vormunds; *Kühling*, in: BeckOK DatenschutzR, BDSG, § 4a, Rn. 32 f.; *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 47; *Simitis*, in: Simitis, BDSG, § 4a, Rn. 21.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

bzw. deren oder dessen Zustimmung zur Einwilligung durch das Kind ankommen. [644] Art. 8 Abs. 1 UAbs. 2 DSGVO sieht für die Einwilligung durch Minderjährige zwischen dem 13. und dem 16. Lebensjahr eine Öffnungsklausel vor, in der die Mitgliedstaaten eigene Altersgrenzen festlegen können. In dem BDSG-neu[645] wurde davon jedoch nicht Gebrauch gemacht, sodass es bei der Altersgrenze von 16 Jahren für die wirksame Einwilligung durch den Minderjährigen selbst bleibt. Auch bisher wurde in Deutschland ungefähr diese Altersgrenze in der Rechtsprechung für die Einsichtsfähigkeit angenommen, sodass sich diesbezüglich keine signifikanten Änderungen für die Rechtslage in Deutschland ergeben werden.[646]

a) „Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird"

Eine Definition von Diensten der Informationsgesellschaft findet sich in Art. 4 Nr. 25 DSGVO i. V. m. Art. 1 Nr. 1 lit. b RL 2015/1535/EU[647]; soziale Online-Netzwerke dürften regelmäßig den Hauptanwendungsfall bilden.[648] Fraglich ist jedoch, wann das Angebot einem Kind direkt gemacht wird. Die Formulierung erinnert an die Formulierung des US-amerikanischen Bundesgesetzes Children's Online Privacy Protection Act (im Folgenden: COPPA), das die Verarbeitung personenbezogener Daten von Kindern durch Websitebetreiber regelt, deren Angebot an Kinder gerichtet ist („directed to children", 15 U.S.C. § 6502(a)(1)).[649] Während in den USA jedoch klar definiert ist, dass es sich hierbei allein um solche Websites handelt, die sich hauptsächlich an Kinder richten[650], ist dies bei Art. 8 Abs. 1

644 Kritisch *Schulz*, in: Gola, DSGVO, Art. 8, Rn. 9, der darin eine Behinderung des Selbstbestimmungsrechts von medienkompetenten Minderjährigen unter 16 Jahren sieht.

645 BGBl. 2017 I, 2097; vgl. auch Einleitung und Gang der Untersuchung, Pkt. B, S. 28.

646 *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 47; *Ernst*, ZD 2017, 110, 111.

647 Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl.EU 2015 L 241, 1.

648 *Frenzel*, in: Paal/Pauly, DSGVO, Art. 8, Rn. 6; ähnlich *Schulz*, in: Gola, DSGVO, Art. 8, Rn. 13.

649 Vgl. *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 8, Rn. 16; Kap. 3 Pkt. B.I.4.b, S. 272.

650 15 U.S.C. § 6501(10); präzisiert in 16 C.F.R. § 312.2.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

DSGVO nicht der Fall. Auch aus teleologischer Sicht wäre eine derartige Beschränkung nicht vereinbar mit dem Ziel des Art. 8 DSGVO, personenbezogene Daten Minderjähriger umfassend zu schützen, EG 38 S. 1 DSGVO. Damit sind jedenfalls solche Angebote, die sowohl von Minderjährigen als auch Erwachsenen genutzt werden – wie etwa *Facebook* – von der Norm umfasst.[651] Schließlich wird teilweise argumentiert, dass sich das direkte Angebot auch darauf beziehen könnte, dass das Angebot den Minderjährigen direkt und nicht über Zwischenpersonen erreicht.[652] Mit dieser grammatikalischen Auslegung lässt sich jedenfalls gut argumentieren, dass Art. 8 DSGVO auch dann zum Tragen kommt, soweit es sich um primär an Erwachsene gerichtete Angebote handelt. Die Auslegung ist auch aus teleologischer Sicht indiziert: Denn der Minderjährige soll ja gerade vor „falschen Entscheidungen" geschützt werden, indem es nicht auf seine, sondern auf die Einwilligung seiner Eltern bzw. Vormundes ankommt. Weshalb dieser Schutz dem Jugendlichen jedoch bei dem Besuch von Websites, die sich ausschließlich an Erwachsene richten, verwehrt bleiben soll, lässt sich schwer begründen und ist ebenso durch die grammatikalische Auslegung nicht vorgegeben.[653]

Im Übrigen ist die festgelegte Altersgrenze der Einwilligungsfähigkeit von Jugendlichen bei 16 Jahren positiv zu bewerten. Für Jugendliche über 16 Jahren ebnet sie die Teilnahme an sozialen Strukturen, notwendigerweise auch gegen den Willen der Eltern, und für Datenverarbeiter bietet sie ein neues Maß an Rechtssicherheit.

b) Prüfpflichten und Umsetzbarkeit

Art. 8 Abs. 2 DSGVO legt dem Verantwortlichen sodann auf, sich zu vergewissern, dass die Einwilligung der Eltern bzw. eines Vormundes nach Maßgabe des Art. 8 Abs.1 UAbs. 1 S. 2 DSGVO auch tatsächlich vorliegt.

---

651 *Frenzel*, in: Paal/Pauly, DSGVO, Art. 8, Rn. 17; *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 8, Rn. 16; *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 8, Rn. 21; *Kampert*, in: Sydow, DSGVO, Art. 8, Rn. 9; a. A. *Gola/Schulz*, ZD 2013, 475, 477 f.

652 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 8, Rn. 16.

653 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 8, Rn. 17; *Buchner/Kühling*, DuD 2017, 544, 547; a. A. *Frenzel*, in: Paal/Pauly, DSGVO, Art. 8, Rn. 7; *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 8, Rn. 19; *Kampert*, in: Sydow, DSGVO, Art. 8, Rn. 9.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Hierfür wurden bereits in der Literatur verschiedene Lösungsansätze angeführt, unter anderem mit Verweis auf die Vorschläge der Federal Trade Commission (FTC)[654] zur Einhaltung der oben genannten Vorgaben des COPPA, wie sie in 16 C.F.R. § 312.5(b) dargelegt werden.[655] Dort wird etwa die Identifikationsmöglichkeit der Eltern über eine Kreditkarte oder ein Ausweisdokument gelistet sowie die Verifizierung mittels eines Telefonanrufs durch geschultes Personal. Wenngleich diese Methoden durchaus potentiell wirkungsvoll erscheinen, so muss doch darauf hingewiesen werden, dass sie vor allem auch mit einer weiteren Verarbeitung personenbezogener Daten einhergehen. Durch die Bereitstellung von Ausweisdokumenten oder Kreditkarten gewinnen die personenbezogenen Daten damit letztlich an Wert, da sie nun verifiziert sind und eine unrichtige Angabe ausgeschlossen wird. Weniger invasive Methoden, wie etwa die Bestätigung der Einwilligung der Eltern oder des gesetzlichen Vertreters durch eine vom Minderjährigen bereitgestellte E-Mail-Adresse der Eltern bzw. des gesetzlichen Vertreters,[656] sind demgegenüber von wohl minderer Effektivität: Denn jeder Minderjährige, der einen Account in einem sozialen Netzwerk anlegen kann, ist auch in der Lage, eine E-Mail-Adresse zu erstellen, die scheinbar den eigenen Eltern gehört.

Die mit den Prüfpflichten des Verantwortlichen einhergehende zusätzliche Datenverarbeitung und der steigende Wert der Daten durch diese Verifizierung erreichen zudem eine problematische Dimension, wenn man die Prüfpflichten des Verantwortlichen nicht nur auf die Einwilligung des gesetzlichen Vertreters, sondern auch auf die richtige Angabe des Alters erstreckt[657] – eine Notwendigkeit, die sich bei strikter Einhaltung der Vorgaben des Art. 8 Abs. 1 UAbs. 1 S. 2 DSGVO ergibt. Diese zwar durchaus sinnvolle Extension der Prüfpflichten führte aber in der Konsequenz zu einer Überprüfung aller Nutzer.

Vor diesem Hintergrund ist durchaus zweifelhaft, ob der durch Art. 8 Abs. 1 DSGVO einhergehende erhöhte Minderjährigenschutz die potentiellen Gefahren durch die Verifizierung der personenbezogenen Daten aller Nutzer – und insbesondere der Minderjährigen – auszugleichen vermag.

654 Vgl. auch Kap. 4 Pkt. B.I.3, S. 267 sowie Pkt. B.I.4.b, S. 272.
655 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 8, Rn. 24 f.
656 *Möhrke-Sobolewski/Klas*, K&R 2016, 373, 377 f.; *Frenzel*, in: Paal/Pauly, DSGVO, Art. 8, Rn. 13; *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 8, Rn. 24.
657 *Buchner/Kühling*, in: Kühling/Buchner, DSGVO, Art. 8, Rn. 28.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Daher erscheint es vorzugswürdig, die Altersbestätigung durch eine einfache Bestätigung mittels Klicks oder Eingabe des Alters zuzulassen[658] und erst in einem nächsten Schritt, sollte die Altersgrenze für eine Einwilligung durch den Nutzer selbst nicht erreicht sein, die Einwilligung der Eltern hinzuzuziehen. In diesem Licht stellt die Methode der E-Mail-Bestätigung durch die gesetzlichen Vertreter einen gangbaren Mittelweg dar: Zum einen wirkt die Angabe einer E-Mail-Adresse als zusätzliche Hürde und entfaltet zugleich eine mit einer eigenhändigen Unterschrift vergleichbare Warnfunktion für den Minderjährigen. Zum anderen ist durchaus denkbar, dass Minderjährige, die gewillt sind, eine falsche E-Mail-Adresse im Namen ihrer Eltern anzulegen, ebenso gewillt wären, eine Kopie eines Ausweisdokuments ohne Wissen der Eltern an den Datenverarbeiter zu übersenden. Demgegenüber ist die Bestätigung via E-Mail jedoch immerhin mit der Preisgabe deutlich weniger sensibler Informationen (im Gegensatz zu der auf Ausweisdokumenten hinterlegten Wohnadresse oder Ausweisnummern) verbunden. Diese Methode ist daher trotz möglicherweise höherer Missbrauchsmöglichkeiten durch die Minderjährigen selbst vorzugswürdig.

III. Zusammenfassung

Die Zulässigkeit des Umgangs mit personenbezogenen Daten richtete sich nach deutschem Recht nach einer Unterscheidung von Bestands-, Nutzungs- und Inhaltsdaten, wobei nach überwiegender Meinung nur Inhaltsdaten dem sachlichen Anwendungsbereich des BDSG unterfielen. Allerdings sind die Zulässigkeitstatbestände des TMG unvereinbar mit Art. 7 DSRL, so dass auch für Bestands- und Nutzungsdaten auf die Regelungen des BDSG zurückzugreifen ist. Allein für die Verarbeitung mittels Tracking Tools ist § 15 Abs. 1 TMG weiterhin anwendbar, da die Regelungen der ePrivacy-RL denen der DSRL vorgehen und § 15 Abs. 1 TMG den Anforderungen des Art. 5 Abs. 3 ePrivacy-RL entspricht.

Das BDSG sieht eine Privilegierung des Umgangs mit personenbezogenen Daten zu Werbezwecken vor. Für den Einsatz von Cookies ist jedoch eine Einwilligung des Nutzers erforderlich, sofern es sich nicht um für die Bereitstellung des Dienstes erforderliche Cookies handelt.

Ab Mai 2018 werden die Bestimmungen des BDSG sowie des TMG in der DSGVO aufgehen. Geplant ist zudem eine Ablösung der ePrivacy-RL

658 *Schulz* , in: Gola, DSGVO, Art. 8, Rn. 20; *Laue/Nink/Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, S. 101 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

durch eine ePrivacy-VO, für die die Kommission im Januar 2017 einen Entwurf vorgelegt hat. Für die Verarbeitung durch die Plattformbetreiber kommt, sofern es sich nicht um die Verarbeitung mittels Tracking Tools handelt, der Erlaubnistatbestand des Art. 6 Abs. 1 S. 1 lit. f DSGVO in Betracht. Erneut zeigt sich hier das Problem der sehr weiten Interpretationsmöglichkeiten der Norm, da die Interessenabwägung durch die verantwortliche Stelle selbst vorgenommen wird und keine mit dem BDSG vergleichbaren strukturierten Erlaubnisnormen vorhanden sind. Gleichwohl stellt die DSGVO in den Erwägungsgründen klar, dass Werbeinteressen ein berechtigtes Interesse des Verantwortlichen darstellen können.

Zudem ist die Einwilligung sowohl nach dem BDSG als auch nach der DSGVO ein wichtiger Legitimationstatbestand für die Datenverarbeitung durch Plattformbetreiber. Bei der Einwilligung ist insbesondere das Koppelungsverbot des BDSG für Zwecke des Adresshandels und der Werbung zu beachten sowie Art. 7 Abs. 4 DSGVO, der eine an ein allgemeines Koppelungsverbot angelehnte Auslegungshilfe für die Beurteilung der Freiwilligkeit darstellt. Bei der Beurteilung der Freiwilligkeit ist der Zugang zu gleichwertigen Leistungen und die Zumutbarkeit der Inanspruchnahme dieser Leistungen einerseits und die Nutzerinteressen und die Bereitschaft der Nutzer, mehrere Dienste parallel in Anspruch zu nehmen andererseits in Betracht zu ziehen. Da die Einwilligung Ausdruck der informationellen Selbstbestimmung der Nutzer ist, darf die Freiwilligkeit der Einwilligung nicht vorschnell verneint werden. Dies entspräche nicht dem Interesse der Nutzer zur Wahrnehmung bestimmter Angebote und würde zudem einen starken Eingriff in die unternehmerische Freiheit der Plattformbetreiber bedeuten.

In diesem Sinne ist bei der Beurteilung der Zulässigkeit der Datenverarbeitung durch soziale Netzwerke eine besonders sorgfältige Interessenabwägung vorzunehmen, bei der nicht pauschal dem Schutz personenbezogener Daten der Vorrang gegeben werden sollte.

C. *Zulässigkeit der Verarbeitung personenbezogener Daten durch Dritte am Beispiel von Social Plug-Ins*

Schließlich muss die Zulässigkeit der Verarbeitung personenbezogener Daten durch Dritte bewertet werden. Hierbei bietet sich das Beispiel von sog. Social Plug-Ins an, da anhand dieses Beispiels sowohl auf die Verwendung von sog. Inhaltsdaten, Nutzungsdaten als auch Cookies eingegangen werden kann. In diesem Zusammenhang ist mit „Social Plug-In“ ein Verweis

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

auf ein soziales Netzwerk in Form eines Links oder Icons gemeint, der auf einer Website außerhalb eines entsprechenden sozialen Netzwerks durch den Websitebetreiber integriert wird. Bekanntestes Beispiel hierfür ist wohl der sog. „Like-Button" von *Facebook.*[659] Der „Like-Button" wird über ein sog. iframe in die Website eingebunden und stellt somit eine Art „Website in der Website" dar.[660] Das bedeutet, dass beim Besuch einer Website, die den „Like-Button" eingebunden hat, automatisch auch Dienste von *Facebook* aufgerufen werden. *Facebook* erklärt dazu: „Die Daten, die wir erhalten, beinhalten Informationen wie die Nutzer-ID der Person, die besuchte Webseite, das Datum und die Uhrzeit sowie andere, Browser-bezogene Informationen."[661] Abhängig von der konkreten Website und abhängig davon, ob der Website-Besucher ein *Facebook*-Nutzer ist oder zumindest *Facebook*-Sites zuvor besucht hat, setzt das Social Plug-In einen oder diverse Cookie(s) auf dem Nutzer-PC, mit dem die Aktivitäten des Nutzers websiteübergreifend verfolgt werden können,[662] und zwar oftmals unabhängig davon, ob der Nutzer den Like-Button betätigt oder überhaupt wahrnimmt.[663] Auch Aktivitäten von Nutzern, die keinen Account bei *Facebook* haben, können damit verfolgt werden.[664] Übertragen wird zudem die IP-Adresse der Nutzer.[665] Das Einbinden von Plug-Ins auf Websites ist dabei durchaus nicht unüblich. Bereits im Jahr 2012 war der „Like-Button" in

---

659 Zu unterscheiden ist der „Like-Button" als Social Plug-In auf einer plattformfremden Seite indes von dem „Like-Button" innerhalb *Facebooks*, mit dem die Nutzer ihr Gefallen von Beiträgen ausdrücken können.

660 *Schleipfer*, DuD 2014, 318, 319.

661 *Facebook Inc.,* FAQ zu sozialen Plug-Ins, abrufbar unter https://developers.facebook.com/docs/plugins/faqs (abgerufen am 13.10.2017).

662 Siehe im Detail *Acar/van Alsenoy/Piessens/Diaz/Preneel*, Facebook Tracking Through Social Plug-ins. Technical Report prepared for the Belgian Privacy Commission, abrufbar unter https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf (abgerufen am 13.10.2017).

663 *OLG Düsseldorf,* Vorlagebeschl. v. 19.01.2017, Az. I-20 U 40/16, MMR 2017, 254, 255.

664 *Acar/van Alsenoy/Piessens/Diaz/Preneel*, Facebook Tracking Through Social Plug-ins. Technical Report prepared for the Belgian Privacy Commission, abrufbar unter https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf (abgerufen am 13.10.2017), S. 5 ff.

665 *ULD*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook (19. August 2011), S. 15.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

22 % der meist besuchten Websites eingebunden.[666] Als Beispiele bekannter deutscher Websites, die das Plug-In eingebunden haben, können die Websites der Tageszeitungen *Süddeutsche Zeitung*[667] und *Frankfurter Allgemeine Zeitung*[668] genannt werden.

I. Verantwortlichkeit der Websitebetreiber am Beispiel des „Like-Buttons"

Ähnlich wie bei sog. Fanpages[669] ist bei Social Plug-Ins bereits umstritten, wer für die Verarbeitung Verantwortlicher ist.[670] In Betracht kommen einerseits der Websitebetreiber, der das Plug-In auf seine Website einbindet und andererseits *Facebook* selbst. Es kommt also darauf an, ob der Websitebetreiber „[…] allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet […]" (Art. 2 lit. d DSRL bzw. Art. 4 Nr. 7 DSGVO).

1. Entscheidung über das „Ob" und „Wie" der Verarbeitung

Der Websitebetreiber müsste also das „Ob" und „Wie" der Verarbeitung steuern.[671] Die Steuerung des „Ob" der Verarbeitung obliegt dabei unproblematisch dem Websitebetreiber: Er allein entscheidet, ob er das Social Plug-In auf seiner Website einbinden möchte. Hier liegt ein entscheidender Unterschied zum Fanpage-Betreiber auf *Facebook*, der gerade nicht über das „Ob" der Verarbeitung entscheidet. Mit Eröffnung einer Fanpage stellt

---

666 *Chaabane/Kaafar/Boreli/Davis*, Big Friend is Watching You: Analyzing Online Social Networks Tracking Capabilities, in: Association for Computing Machinery (Hrsg.), WOSN'12, S. 9.

667 *Süddeutsche Zeitung*, abrufbar unter http://www.sueddeutsche.de/ (abgerufen am 13.10.2017).

668 *Frankfurter Allgemeine Zeitung*, abrufbar unter http://www.faz.net/ (abgerufen am 13.10.2017).

669 Vgl. Kap. 3 Pkt. A.II.2, S. 99.

670 In der Terminologie des BDSG: Verantwortliche Stelle, vgl. § 3 Abs. 7 BDSG. Auch wenn das BDSG i. d. F. v. 14.01.2003 noch Gültigkeit entfaltet, wird die Terminologie der DSGVO verwendet, sofern es sich nicht um Ausführungen konkret zu BDSG-Vorschriften handelt.

671 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsdatenverarbeiter". WP 169 (16.02.2010), S. 16; *Martini*, in: Paal/Pauly, DSGVO, Art. 26, Rn. 19.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Facebook dem Fanpage-Betreiber ungefragt Statistiken über die Besucher zur Verfügung. Einzig der Verzicht auf den Betrieb der Fanpage liegt in der Entscheidungsgewalt des Fanpage-Betreibers, nicht aber, ob er die Fanpage ohne die Zurverfügungstellung der Datenstatistiken betreiben möchte. Der Websitebetreiber hat diese Wahl indes schon: Denn seine Website kann er ebenso ohne die Einbindung eines Social Plug-Ins betreiben.[672] Die Vergleichbarkeit ergibt sich auch nicht daraus, dass mit der Einbindung des Social Plug-Ins die Datenverarbeitung von *Facebook* ungefragt vorgenommen wird. So stünden dem Websitebetreiber, anders als dem Betreiber einer Fanpage, durchaus technische Mittel zur Verfügung, um das Plug-In erst nach einer Bestätigung durch den Websitebesucher zu aktivieren.[673]

Fraglich ist jedoch, ob der Websitebetreiber über das „Wie" der Verarbeitung entscheidet. So wird in der Diskussion regelmäßig hervorgehoben, dass der Websitebetreiber keinen Einfluss auf den Verarbeitungsvorgang hätte.[674] Es wird vertreten, dass der Websitebetreiber die Daten weder erhebe noch speichere und auch nicht übermittle.[675] Dabei könnte in der Einbindung sehr wohl ein Erheben gesehen werden, das § 3 Abs. 3 BDSG als das Beschaffen von Daten über den Betroffenen definiert: Denn es ist die Website, die bei dem Websitebetreiber die Kommunikation mit *Facebook* initiiert. [676] Diese Deutung entspricht auch dem Art. 2 lit. b DSRL, der nicht die Erhebung selbst definiert, sondern die Verarbeitung als „[…] jeden mit

---

672 A. A. *Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages*, "Facebook-Kampagne" des ULD, abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017), S. 17.

673 So auch *LG Düsseldorf,* Urt. v. 09.03.2016, Az. 12 O 151/15, ZD 2016, 231, 233, Rn. 58.

674 *Schleipfer*, DuD 2014, 318, 320; *Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages*, "Facebook-Kampagne" des ULD, abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017), S. 17; *Piltz*, CR 2011, 657, 662; ähnlich *Voigt/Alich*, NJW 2011, 3541, 3542.

675 *Voigt/Alich*, NJW 2011, 3541, 3542; *Piltz*, CR 2011, 657, 662; *Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages*, "Facebook-Kampagne" des ULD, abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017), S. 17.

676 *Föhlisch/Pilous*, MMR 2015, 631; *Schröder/Hawxwell/Münzing*, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins, abrufbar unter https://www.datenschutzzentrum.de/uploads/facebook/WissDienst-BT-Facebook-ULD.pdf (abgerufen am 13.10.2017), S. 8 f.; *LG Düsseldorf,* Urt. v. 09.03.2016, Az. 12 O 151/15, ZD 2016, 231, 233, Rn. 62.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten […]". Die Definition wurde bewusst weit gefasst, um einen umfassenden Schutz personenbezogener Daten natürlicher Personen zu gewährleisten.[677] Diesem Ansatz folgt die DSGVO in Art. 4 Nr. 2 DSGVO, indem die Definition der DSRL dort beinahe wortlautgleich übernommen wurde.

Dafür spricht außerdem, dass *Facebook* den Websitebetreibern durchaus einige Wahlmöglichkeiten in Bezug auf den Like-Button gibt. So können diese etwa angeben, ob Besuchern die „Gesichter" (gemeint sind die Profilbilder) von Nutzern, die den Button betätigt haben, angezeigt werden sollen.[678]

2. Gewichtung des „Ob" und „Wie" der Verarbeitung

Es lässt sich feststellen, dass der Websitebetreiber in der Tat Einfluss auf den Verarbeitungsvorgang hat, wenn auch in eingeschränktem Umfang. Die Frage, die sich demnach stellt ist, ob eine vollumfängliche Entscheidungsbefugnis über den Zweck, also das „Ob" bzw. „Warum" der Verarbeitung, und nur ein geringfügiger Umfang über die Mittel, also das „Wie" der Verarbeitung, ausreicht, um nach der Definition des Art. 2 lit. d DSRL bzw. Art. 4 Nr. 7 DSGVO als (für die Verarbeitung) Verantwortlicher zu gelten. Die Art. 29-Datenschutzgruppe führt hierzu aus, dass die Entscheidung über den Zweck der Verarbeitung allein dem Verantwortlichen vorbehalten ist.[679] Zudem geht sie davon aus, dass die Verantwortung sich nicht auf alle Verarbeitungstätigkeiten erstrecken muss, sondern eine Verantwortung für die erste Phase der Datenverarbeitung ausreichend ist.[680] Diese Einschätzung fügt sich in die Systematik der DSRL sowie der DSGVO ein, die beide ausdrücklich vorsehen, dass der Verantwortliche „allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung […] entscheidet", Art. 2 lit. d DSRL bzw. Art. 4 Nr. 7 DSGVO. Dass auch das BDSG eine gemeinsame

---

677 COM(92) 422 final – SYN 287, ABl.EG 1992 C 311, 30, Commentary on the Articles, S. 10.

678 *Facebook Inc.,* FAQ zu sozialen Plug-Ins, abrufbar unter https://developers.facebook.com/docs/plugins/faqs (abgerufen am 13.10.2017).

679 *Art. 29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen "für die Verarbeitung Verantwortlicher" und "Auftragsdatenverarbeiter". WP 169 (16.02.2010), S. 19.

680 *Art. 29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavorial Targeting. WP 171 (22.06.2010), S. 14.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Verantwortlichkeit vorsieht, ist anerkannt.[681] Bei gemeinsamer Verantwortlichkeit ist jedoch nicht erforderlich, dass alle Verantwortlichen in gleichen Teilen über das „Warum" und „Wie" entscheiden; vielmehr kann die Entscheidungsbefugnis auch ungleich verteilt sein.[682]

Demnach reicht eine vollständige Entscheidungsgewalt über den Zweck der Verarbeitung mit einer geringfügigen Entscheidungsmacht über die Mittel der Verarbeitung aus, um eine Verantwortlichkeit der Websitebetreiber zu begründen, allerdings nur für den Anfang des Verarbeitungsprozesses, also für die Einbindung des Social Plug-Ins, durch die die Verarbeitung des Dritten – hier *Facebook* – ausgelöst wird. Für die weitere Verarbeitung durch *Facebook* kann keine Verantwortlichkeit des Websitebetreibers begründet werden, da ihm insofern jegliche Steuerungsmöglichkeiten fehlen. Der Websitebetreiber wird damit auch nicht über Gebühr in die Pflicht genommen, da seine Pflichten als Verantwortlicher auf das ihm Mögliche beschränkt sind.[683] Zu beachten ist allerdings Art. 26 DSGVO, der eine Vereinbarung gemeinsam für die Verarbeitung Verantwortlicher verlangt, aus der die Zuteilung der Verantwortlichkeit für die jeweiligen Verarbeitungsphasen hervorgeht.[684] Nur klarstellend sei erwähnt, dass diese Vereinbarung materiell nicht Voraussetzung für das Bestehen einer Mitverantwortlichkeit ist[685] und sich auch bei fehlender Vereinbarung nichts an dem hier vertretenen Ergebnis ändert. Allerdings ist eine Missachtung dieser formellen Vorgaben bußgeldbewehrt, Art. 83 Abs. 4 lit. a DSGVO. Es ist den Website- und Plattformbetreibern daher zu raten, ab Geltung der DSGVO eine solche Vereinbarung i. S. d. Art. 26 DSGVO bereitzuhalten.

---

681 Für eine richtlinienkonforme Auslegung dahingehend *Eßer*, in: Auernhammer, BDSG, § 3, Rn. 76; *Monreal*, ZD 2014, 611, 614; *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 5; i. E. ebenso *Dammann,* in: Simitis, BDSG, § 3, Rn. 221, der argumentiert, dass die Auslegung der gemeinsamen Verantwortlichkeit bereits vom Wortlaut des § 3 Abs. 7 BDSG gedeckt ist; vgl. bereits Kap. 3 Pkt. A.II.2.b.aa, S. 102.

682 *Martini/Fritzsche*, NVwZ-Extra 2015, 1, 15.

683 *Art. 29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavorial Targeting. WP 171 (22.06.2010), S. 14; wohl a. A. *ULD*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook (19. August 2011), S. 17, das eine „[…] datenschutzrechtliche Verantwortung für die dadurch ausgelöste Verarbeitung […]" sieht und damit wohl eine volle Anwendbarkeit der Betroffenenrechte gegen den Websitebetreiber befürwortet; vgl. zur konkreten Ausgestaltung der Pflichten des Websitebetreibers Kap. 3 Pkt. C.II.2, S. 211 und Pkt. C.II.3, S. 215.

684 *Hartung*, in: Kühling/Buchner, DSGVO, Art. 26, Rn. 22.

685 Ebenso *Hartung*, in: Kühling/Buchner, DSGVO, Art. 26, Rn. 20.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

3. Keine Auftragsverarbeitung durch den „Like-Button“

Ferner ist anzumerken, dass durch den „Like-Button“ keine Auftragsverarbeitung vorgenommen wird. Bemerkenswert ist, dass sowohl eine Auftragsverarbeitung durch *Facebook* für den Websitebetreiber[686] als auch eine Auftragsverarbeitung durch den Websitebetreiber für *Facebook*[687] diskutiert wird. Der Schwerpunkt der Verarbeitungsleistung wird jedoch von *Facebook* wahrgenommen; dass der Websitebetreiber somit im Auftrag von *Facebook* personenbezogene Daten verarbeitet, ist ausgeschlossen. Plausibler ist indes die Überlegung, dass *Facebook* für den Websitebetreiber personenbezogene Daten verarbeitet. Allerdings müsste dazu, genauso wie bei Fanpages[688], die Verarbeitung durch den Auftragsverarbeiter auf Weisung des Verantwortlichen ausgeführt werden. Hieran fehlt es jedoch: Zwar hat der Websitebetreiber einen geringfügigen Einfluss auf die Mittel der Verarbeitung, den Umfang bestimmt *Facebook* jedoch selbst. *Facebook* agiert gerade nicht als „verlängerter Arm“ des Websitebetreibers auf dessen Weisung.[689]

4. Websitebetreiber und Plug-In-Anbieter als Diensteanbieter i. S. d. TMG

Im Übrigen ist der Websitebetreiber – unabhängig von der datenschutzrechtlichen Verantwortlichkeit – Diensteanbieter i. S. d. § 2 S. 1 Nr. 1 TMG und zwar auch für das Social Plug-In. Denn nach der Definition des § 2 S. 1

---

686 *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 16 f.; *Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages*, "Facebook-Kampagne" des ULD, abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017), S. 17; *Kühnl,* Persönlichkeitsschutz 2.0, S. 121 f.

687 *Föhlisch/Pilous*, MMR 2015, 631, 633; *Ernst*, NJOZ 2010, 1917, 1918; *Schröder/Hawxwell/Münzing*, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins, abrufbar unter https://www.datenschutzzentrum.de/uploads/facebook/WissDienst-BT-Facebook-ULD.pdf (abgerufen am 13.10.2017), S. 8 f.

688 Vgl. Kap. 3 Pkt. A.II.2.c, S. 104.

689 *Martini*, in: Paal/Pauly, DSGVO, Art. 28, Rn. 2; *Petri*, in: Simitis, BDSG, § 11, Rn. 20.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Nr. 1 TMG ist Diensteanbieter, wer „[…] eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt […]". Damit ist die Definition sehr breit gehalten; die Websitebetreiber vermitteln mindestens den Zugang zu fremden Telemedien, indem sie das Social Plug-In auf ihrer Website einbinden.[690] Das bedeutet, dass die Regelungen der §§ 11 ff. TMG grundsätzlich Anwendung finden.[691]

Ferner ist auch der Anbieter des Social Plug-Ins selbst, etwa *Facebook* für den Like-Button, Diensteanbieter i. S. d. Vorschrift. Denn Social Plug-Ins werden nach deren Maßgaben in die Website eingebunden und stellen letztlich eine „Website in der Website" dar.[692]

5. Zwischenergebnis

Websitebetreiber, die Social Plug-Ins eines Betreibers eines sozialen Netzwerks – im vorliegenden Beispiel *Facebook* – in ihre Website integrieren, sind für die Einbindung dieser Social Plug-Ins datenschutzrechtlich Verantwortliche. Die Zulässigkeit der Einbindung muss demnach unter datenschutzrechtlichen Gesichtspunkten geprüft werden.[693]

---

690 *Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages*, "Facebook-Kampagne" des ULD, abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017), S. 10; *Piltz*, CR 2011, 657, 662; *Schröder/Hawxwell/Münzing*, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins, abrufbar unter https://www.datenschutzzentrum.de/uploads/facebook/WissDienst-BT-Facebook-ULD.pdf (abgerufen am 13.10.2017), S. 8; die Eigenschaft als Diensteanbieter jedenfalls voraussetzend *LG Düsseldorf,* Urt. v. 09.03.2016, Az. 12 O 151/15, ZD 2016, 231, 232, f. Rn. 47 ff; *Moos,* in: Taeger/Gabel, BDSG, TMG, § 13, Rn. 6; a. A. *Schleipfer*, DuD 2014, 318, 320, mit der Begründung, dass der Websitebetreiber von den Nutzungsvorgängen nichts mitbekäme.

691 Vgl. sogleich, Kap. 3 Pkt. C.II.1.a, S. 207; die telemedienrechtliche Verantwortlichkeit gem. §§ 7 ff. TMG ist hingegen für die vorliegende Klärung der datenschutzrechtlichen Verantwortlichkeit nicht relevant, da sie sich auf die Verantwortlichkeit für Inhalte des Angebots bezieht, vgl. schon Kap. 3 Pkt. A.II.2.b.bb, S. 103.

692 *Schleipfer*, DuD 2014, 318, 319.

693 Vgl. sogleich Kap. 3 Pkt. C.II, S. 207.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

II. Zulässigkeit der Einbindung von Social Plug-Ins am Beispiel von *Facebooks* „Like-Button"

1. Zulässigkeit durch gesetzlichen Erlaubnistatbestand

Zunächst soll die Zulässigkeit der Einbindung von Social Plug-Ins durch gesetzliche Erlaubnistatbestände untersucht werden. Bei dem Besuch von Websites, die ein Social Plug-In integriert haben, werden etwa die IP-Adresse übertragen[694] sowie verschiedene Cookies auf dem Nutzer-PC gesetzt.[695]

Im Folgenden muss für die Beurteilung der Zulässigkeit der Einbindung der Social Plug-Ins unterschieden werden zwischen der Art der Einbindung, in dem das Social Plug-In zeitgleich mit dem Aufrufen der Website aktiviert wird und den Fällen, in denen es erst mittels Klicks durch den Nutzer selbst aktiviert wird. Schließlich muss diskutiert werden, wie eine wirksame Einwilligung in die Datenverarbeitung, die durch das Social Plug-In ausgelöst wird, erzielt werden könnte.[696]

a) Zulässigkeit nach dem BDSG und dem TMG

Sofern es sich um die Verwendung von Inhaltsdaten oder der IP-Adresse handelt, richtet sich nach hier vertretener Ansicht auch bei Social Plug-Ins die Bewertung der Zulässigkeit der Erhebung, Verarbeitung und Nutzung nach dem BDSG.[697] Soweit es um das Setzen und Verwenden von Cookies geht, richtet sich die Zulässigkeit nach § 15 Abs. 1 S. 1 TMG.[698]

---

694 Vgl. *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 22.

695 Einen Überblick über die gesetzten Cookies bieten *O'Reilly*, Facebook Technical Analysis Report (16th December 2011), abrufbar unter https://dataprotection.ie/documents/facebook%20report/final%20report/Appendices.pdf (abgerufen am 13.10.2017), sowie *Acar/van Alsenoy/Piessens/Diaz/Preneel*, Facebook Tracking Through Social Plug-ins. Technical Report prepared for the Belgian Privacy Commission, abrufbar unter https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf (abgerufen am 13.10.2017).

696 Vgl. Kap. 3 Pkt. C.II.2, S. 211.

697 Vgl. Kap. 3 Pkt. B.I.1, S. 154.

698 Vgl. Kap. 3 Pkt. B.I.3.a.dd, S. 178.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aa) Zulässigkeit nach dem BDSG

Die Einbindung eines Plug-Ins nimmt der Websitebetreiber regelmäßig zu eigenen Geschäftszwecken i. S. d. § 28 BDSG vor. Selbst wenn eine Übermittlung an *Facebook* stattfindet, ist diese nicht Hauptzweck i. S. d. § 29 BDSG. Hauptzweck der Einbindung eines Social Plug-Ins ist vielmehr die Vermarktung des eigenen Produkts.

Soweit es sich um ein Plug-In handelt, das die Datenerhebung vornimmt, sobald der Nutzer eine Website öffnet, kann sich dieser Umgang mit personenbezogenen Daten nicht auf einen Zulässigkeitstatbestand stützen. Denn erstens ist die Einbindung eines Plug-Ins nicht zur Vertragserfüllung i. S. d. § 28 Abs. 1 S. 1 Nr. 1 BDSG erforderlich: Weder für den Websitebetreiber und erst recht nicht für *Facebook* ist die Verwendung der personenbezogenen Daten für die Begründung, Durchführung oder Beendigung eines Schuldverhältnisses erforderlich. Die Erforderlichkeit muss sich gerade auf die Erforderlichkeit zur Vertragserfüllung stützen und sowohl eine Website als auch ein soziales Netzwerk können ohne die Einbindung von Plug-Ins betrieben werden.[699] Etwas Anderes ergibt sich jedoch dann, wenn das Plug-In erst bei Klick durch den Nutzer aktiviert wird. In diesem Fall muss nicht auf die Erforderlichkeit für den Betrieb der Website, sondern auf die Erforderlichkeit für die Funktionalität des Plug-Ins selbst abgestellt werden.[700] Dann ist jedoch auch die Erforderlichkeit der Übertragung der IP-Adresse gegeben, um das Plug-In dem Nutzer richtig darzustellen.[701]

Auch kann sich die Einbindung, sofern das Plug-In automatisch bei Aufrufen der Website aktiviert wird, nicht auf berechtigte Interessen des Websitebetreibers oder *Facebooks* i. S. d. § 28 Abs. 1 S. 1 Nr. 2 BDSG stützen, die die Betroffeneninteressen überwiegen. Bei einem vom Nutzer nicht be-

---

699 *Piltz*, CR 2011, 657, 660; *Gennen/Kremer*, ITRB 2011, 59, 62; *Schröder/Hawxwell/Münzing*, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins, abrufbar unter https://www.datenschutzzentrum.de/uploads/facebook/WissDienst-BT-Facebook-ULD.pdf (abgerufen am 13.10.2017), S. 13; *Hullen*, MMR 2011, 387, 388; *Föhlisch/Pilous*, MMR 2015, 631, 633 f.; a. A. *Voigt/Alich*, NJW 2011, 3541, 3543.

700 *Kühnl,* Persönlichkeitsschutz 2.0, S. 149 f.

701 *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 22.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

merkbaren Umgang mit personenbezogenen Daten muss das Betroffeneninteresse als überwiegend angesehen werden: Schließlich ist das essentielle Verständnis des Datenschutzes, dass die Betroffene wissen, „[…] wer was wann und bei welcher Gelegenheit über sie weiß."[702] Dies gilt i. Ü. auch bei der Verarbeitung oder Nutzung personenbezogener Daten zu Werbezwecken i. S. d. § 28 Abs. 3 S. 2 bis 4 BDSG, da auch hierfür schutzwürdige Betroffeneninteressen nicht entgegenstehen dürfen, § 28 Abs. 3 S. 6 BDSG.

bb) Zulässigkeit nach dem TMG

Die Zulässigkeit des Setzens i. S. d. § 15 Abs. 1 S. 1 TMG von Cookies durch *Facebook* kommt nur dann in Betracht, wenn der Nutzer mit einem Klick das Plug-In selbsttätig aktiviert hat. Nur dann kann statt auf die Erforderlichkeit für die Inanspruchnahme der Website auf die Erforderlichkeit für die Funktionalität des Plug-Ins selbst abgestellt werden und erwogen werden, ob die Verwendung der Cookies erforderlich ist für die Inanspruchnahme der Telemedien i. S. d. § 15 Abs. 1 S. 1 TMG. Für die Erforderlichkeit der Cookies ist nach deren Funktion zu unterscheiden. So setzt *Facebook* sowohl bei Nicht-Nutzern als auch bei Nutzern den sogenannten „datr"-Cookie mit einer Dauer von zwei Jahren. Er soll der Identifikation des Browsers dienen und so missbräuchliche Anmeldungen auf *Facebook* verhindern.[703] Allerdings ist nicht ersichtlich, inwiefern dieser Cookie für die Inanspruchnahme des Plug-Ins erforderlich ist und zwar auch bei Nicht-Nutzern. Jedenfalls bei einem einmaligen Klick auf das Plug-In muss die Erforderlichkeit hierfür abgelehnt werden.[704] Andererseits kann ein Cookie, der der Identifikation bereits eingeloggter Mitglieder dient – im Fall von *Facebook* der sog. „c_user"-Cookie[705] – durchaus für die Inanspruchnahme

---

702 *BVerfG,* Urt. v. 15.12.1983, Az. 1 BvR 209/83, BVerfGE 65, 1, 43 – Volkszählung.

703 *O'Reilly*, Facebook Technical Analysis Report (16th December 2011), abrufbar unter https://dataprotection.ie/documents/facebook%20report/final%20report/Appendices.pdf (abgerufen am 13.10.2017), S. 176.

704 *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 25.

705 *O'Reilly*, Facebook Technical Analysis Report (16th December 2011), abrufbar unter https://dataprotection.ie/documents/facebook%20report/final%20report/Appendices.pdf (abgerufen am 13.10.2017), S. 178.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

des Telemediums erforderlich sein: Denn dieser Cookie ist nötig, damit die Daten mit dem Klick auf das Social Plug-In automatisch dem Mitgliedskonto zugeordnet werden können.[706] In diesem Fall sind jedoch die zusätzlichen Informationspflichten aus § 13 Abs. 1, 2 TMG bei einem automatisierten Verfahren, das eine spätere Identifikation des Nutzers ermöglicht, zu beachten.

b) Zulässigkeit nach der DSGVO und dem ePrivacy-VO-E

Dieselbe Argumentation gilt indes auch für eine gegebenenfalls in Betracht kommende Zulässigkeit nach Art. 6 Abs. 1 S. 1 lit. b DSGVO – die Verarbeitung ist weder für den Websitebetreiber noch für *Facebook* erforderlich zur Erfüllung eines Vertrags – sowie für eine Zulässigkeit gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO. Denn auch hier überwiegen bei einer von den Betroffenen unbemerkten Verarbeitung stets die Betroffeneninteressen; dies ergibt sich als Ausfluss des Rechts auf Schutz personenbezogener Daten aus Art. 8 GRCh.[707]

Auch für das Setzen von Cookies i. S. d. ePrivacy-VO-E[708] lässt sich auf die Argumentation verweisen: Das Setzen von Cookies ist gem. Art. 8 Abs. 1 lit. b ePrivacy-VO-E nur zulässig, sofern der Nutzer eingewilligt hat oder wenn das Setzen von Cookies erforderlich ist für die Bereitstellung des gewünschten Dienstes. Hinsichtlich der Erforderlichkeit kann auf die Argumentation zu den Ausführungen zur Zulässigkeit nach dem TMG verwiesen werden.[709]

2. Erlaubnis durch Einwilligung

Fraglich ist, ob das Einbinden von Social Plug-Ins vielleicht durch die Einwilligung des Betroffenen legitimiert ist. Dies ist nur dann der Fall, wenn

---

706 *Arbeitsgruppe des AK I "Staatsrecht und Verwaltung"*, Ergebnisbericht der Arbeitsgruppe AK I "Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017), S. 25.

707 Vgl. etwa *EuGH,* Urt. v. 08.04.2014, Rs. C-293/12, C-594/12, ECLI:EU:C:2014:238, Rn. 37 – Digital Rights Ireland und Seitlinger.

708 COM(2017) 10 final.

709 Kap. 3 Pkt. C.II.1.a.bb, S. 209.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

der Betroffene überhaupt die Gelegenheit zur Einwilligung erhält und die Verwendung der Daten nicht automatisch und ungefragt bereits beim Aufrufen der Website erfolgt.

a) Richtiger Empfänger der Einwilligungserklärung

Hierfür muss zunächst der richtige Einwilligungsempfänger benannt werden.[710] In Betracht kommen insoweit der Websitebetreiber, der das Social Plug-In einbindet sowie der Plattformbetreiber, im Fall des hier besprochenen Beispiels also *Facebook*. Hierbei muss zwischen den unterschiedlichen Handlungen der beiden Akteure unterschieden werden: Für das Einbinden des Social Plug-Ins verantwortlich ist, wie dargestellt,[711] der Websitebetreiber selbst. Die Verantwortlichkeit für die weiteren Verarbeitungsvorgänge durch *Facebook* liegt jedoch bei *Facebook*. Nötig ist daher eine gegenüber dem Websitebetreiber erfolgte Einwilligung durch den Betroffenen in die Aktivierung des Social Plug-Ins selbst; die Einwilligung für die Verarbeitung der Daten muss zudem gegenüber *Facebook* erfolgen. Nur bei Vorliegen einer solchen „Doppel-Einwilligung" ist das Vorgehen datenschutzrechtlich zulässig.

b) Keine Einwilligung durch *Facebooks* AGB

Aus dem zuvor gesagten folgt bereits, dass eine Generaleinwilligung durch *Facebooks* AGB ausgeschlossen ist. In Betracht kommt dies überhaupt nur für die Datenverarbeitung durch *Facebook* und auch nur für die Nutzer von *Facebook*. Die Datenverarbeitung betrifft jedoch auch Nicht-Nutzer von *Facebook*;[712] da diese nicht in die AGB von *Facebook* eingewilligt haben,

710 Diese Frage hat das *OLG Düsseldorf* dem *EuGH* zur Entscheidung vorgelegt, vgl. *OLG Düsseldorf,* Vorlagebeschl. v. 19.01.2017, Az. I-20 U 40/16, MMR 2017, 254, 255, Rn. 19; *EuGH,* Vorabentscheidungsersuchen des OLG Düsseldorf, Rs. C-40/17, ABl.EU L 281, 31 – Fashion ID.

711 Vgl. Kap. 3 Pkt. C.I, S. 201.

712 *Acar/van Alsenoy/Piessens/Diaz/Preneel*, Facebook Tracking Through Social Plug-ins. Technical Report prepared for the Belgian Privacy Commission, abrufbar unter https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf (abgerufen am 13.10.2017), S. 5 ff.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

entfällt die Einwilligung für diese Gruppe an Website-Besuchern von vornherein.[713]

Allerdings ist auch bei Nutzern eine Einwilligung in die AGB zweifelhaft. Denn es ist schon fraglich, ob der Nutzer tatsächlich damit rechnen muss, dass er mit seiner Einwilligung in die AGB und Datenschutzbestimmung *Facebooks* auch der Website-übergreifenden Verwendung seiner Daten zustimmt und zwar auch dann, wenn er gar nicht in *Facebook* eingeloggt ist. Dies gilt umso mehr, wenn man bedenkt, dass einige der von *Facebook* gesetzten Cookies eine Gültigkeit von zwei Jahren besitzen.[714] Daher könnte diese Bestimmung eine überraschende Klausel i. S. d. § 305c BGB darstellen.

Zudem könnte es an der hinreichenden Informiertheit der Einwilligung durch den Nutzer fehlen. Denn *Facebook* informiert nach aktuellem Stand in seiner Cookie-Richtlinie über die Setzung von Cookies beim Besuch von Websites, die Social Plug-Ins integriert haben, lediglich mit dem Hinweis, dass Cookies verwendet werden bei „[…] Dienste[n], die von anderen Unternehmen bereitgestellt werden, die die Facebook-Dienste nutzen (z. B. Unternehmen, die den „Like-Button" oder die Werbedienste von Facebook in ihre Webseiten und Apps integrieren)."[715] Allerdings enthält der Nutzer keine Information darüber, was der „Like-Button" ist; dass die Funktion und Bedeutung des „Like-Button"-Plug-Ins aber jedem *Facebook*-Nutzer bekannt ist, kann nicht ohne Weiteres angenommen werden.

Somit ist auch für *Facebook*-Nutzer die Einwilligung in die AGB nicht ausreichend als Einwilligung in die Datenverarbeitung durch *Facebook*, die mittels Social Plug-Ins auf Dritt-Websites ausgelöst wurde.

c) Ausgestaltung der Einwilligungserklärungen

Fraglich ist also, wie die Einwilligungserklärungen gegenüber dem Websitebetreiber und gegenüber dem Plattformbetreiber ausgestaltet sein sollten.

---

713 So auch *Ernst*, NJOZ 2010, 1917, 1918.

714 *Acar/van Alsenoy/Piessens/Diaz/Preneel*, Facebook Tracking Through Social Plug-ins. Technical Report prepared for the Belgian Privacy Commission, abrufbar unter https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf (abgerufen am 13.10.2017), S. 6, 14, 16.

715 *Facebook Inc.,* Cookies und andere Speichertechnologien, abrufbar unter https://www.facebook.com/policies/cookies/ (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Nach hier vertretener Ansicht ist bei elektronisch erklärter Einwilligung sowohl nach dem BDSG (beispielsweise im Fall der Übertragung von Inhaltsdaten und IP-Adressen)[716] sowie nach dem TMG (beispielsweise im Fall von Cookies)[717] eine „opt-in"-Einwilligung von Nöten, um sicherzustellen, dass der Betroffene über das nötige Einwilligungsbewusstsein verfügt.[718] Nach der DSGVO ist, wie dargestellt, die „opt-in"-Einwilligung obligatorisch; nach dem ePrivacy-VO-E der Kommission kann die Einwilligung in die Verwendung von Cookies zwar auch über die Browser-Einstellungen erfolgen, sie müsste sich dann allerdings auch ganz konkret auf Third Party-Cookies beziehen.

Fraglich ist in diesem Zusammenhang schon der Umfang der Informationen, die für eine wirksame Einwilligung nötig sind. Diese Frage geht zugleich einher mit den Informationspflichten aus § 13 TMG bzw. Art. 10 DSRL sowie Art. 13 DSGVO. Gem. § 13 Abs. 1 TMG hat der Diensteanbieter etwa über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu informieren. Dies ist insofern problematisch, als der Websiteanbieter selbst über diese Informationen regelmäßig keine Kenntnis haben wird.[719]

Fraglich ist demnach, wie dieser Informationspflicht nachgekommen werden kann und welchen Umfang die Einwilligungserklärung haben muss. Hierbei könnte eine Einwilligung durch den Betroffenen in zwei Schritten die zielführende Lösung sein: In einem ersten Schritt muss der Websitebetreiber darüber informieren, dass das Social Plug-In durch ihn eingebunden ist, jedoch weitgehend das Angebot eines Dritten – hier: *Facebook* – darstellt. Im Weiteren würde diese Informationspflicht umfassen, dass der Websitebetreiber die Funktionsweise des Plug-Ins und seinen fehlenden Einfluss auf die Verarbeitung offenlegt und hierbei auch kenntlich macht, dass ihm die genauen Verarbeitungsvorgänge nicht bekannt sind.[720] Wünschenswert wäre die Information der Nutzer in der gebotenen Kürze, um eine tatsächliche Kenntnisnahme durch die Nutzer zu gewährleisten. Mit Blick auf die insofern leicht erfassbare Tatsache, dass mit Klick auf das

716 Vgl. Kap. 3 Pkt. B.I.1, S. 154.
717 Vgl. Kap. 3 Pkt. B.I.3.a, S. 175.
718 Vgl. Kap. 3 Pkt. B.II.2, S. 190.
719 Das *OLG Düsseldorf* hat diese Frage inzwischen dem *EuGH* vorgelegt, *OLG Düsseldorf,* Vorlagebeschl. v. 19.01.2017, Az. I-20 U 40/16, MMR 2017, 254, 255, Rn. 20; *EuGH,* Vorabentscheidungsersuchen des OLG Düsseldorf, Rs. C-40/17, ABl.EU L 281, 31 – Fashion ID.
720 *Moos*, in: Taeger/Gabel, BDSG, TMG, § 13, Rn. 6.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Plug-In ein Angebot eines Dritten wahrgenommen wird und keine Einflussmöglichkeiten auf die dadurch ausgelöste Verarbeitung besteht, scheint dies durchaus realistisch umsetzbar. Nur bei einer aktiven Einwilligung des Nutzers nach dieser Information sollte in einem zweiten Schritt die Information zu Art, Umfang und Zweck der Erhebung durch *Facebook* selbst erfolgen.[721] Denn das Plug-In gestaltet sich als „Website in der Website" und öffnet damit ein eigenes Angebot durch *Facebook*.[722] Die Information muss dabei noch vor Datenverwendung und auf der aufgerufenen Website selbst erfolgen; eine Information auf der Website von *Facebook* selbst kann insofern nicht den Anforderungen an eine wirksame Einwilligung genügen, nach der die Information bereits vor Umgang mit personenbezogenen Daten zu erfolgen hat. Insbesondere muss aus der Information auch hervorgehen, für welchen Teil des Umgangs mit personenbezogenen Daten der Websitebetreiber und für welchen Teil der Anbieter des Social Plug-Ins verantwortlich ist, damit der Nutzer weiß, wem gegenüber er seine Betroffenenrechte geltend machen kann.[723] Nur wenn der Betroffene dann einwilligt, darf *Facebook* mit der Verwendung der personenbezogenen Daten beginnen. Darüber hinaus entfaltet diese zweistufige Information eine Warnfunktion für den Nutzer, dass mit seiner Zustimmung eine Verarbeitung seiner personenbezogenen Daten ausgelöst wird.

Der Websitebetreiber ist also verpflichtet, sicherzustellen, dass die „Website in der Website" erst nach erfolgter Einwilligung aufgerufen wird und die Einbindung in seine eigene Website mit einer vorherigen Information über die Verwendung der Daten einhergeht.[724] Dies liegt in seinen Fähigkeiten; die Garantie für die Richtigkeit der vorhergehenden Information durch den Plattformbetreiber, dessen Website automatisch aufgerufen wird, kann ihm indes nicht auferlegt werden. Solange der Nutzer klar erkennen kann, dass er mit seiner Bestätigung das Angebot eines Dritten aufruft und

---

721 Zuzugeben ist – mit Blick auf die Länge der Datenschutz- und Cookie-Richtlinie und AGB *Facebooks*, vgl. *Facebook Inc.,* Datenrichtlinie, abrufbar unter https://www.facebook.com/about/privacy (abgerufen am 13.10.2017); *Facebook Inc.,* Cookies und andere Speichertechnologien, abrufbar unter https://www.facebook.com/policies/cookies/ (abgerufen am 13.10.2017); *Facebook Inc.,* Erklärung der Rechte und Pflichten, abrufbar unter https://www.facebook.com/legal/terms (abgerufen am 13.10.2017) – dass diese Erklärung wohl deutlich länger ausfüllen dürfte als die Information durch den Websitebetreiber selbst. Dies ist jedoch kein spezifisches Problem von Plug-Ins, sondern der Erklärungen selbst.

722 *Schleipfer*, DuD 2014, 318, 319.

723 Vgl. Kap. 3 Pkt. C.II.2.c, S. 212.

724 Vgl. Kap. 3 Pkt. C.II.2, S. 211.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

freiwillig entscheidet, ob er dessen Informationen über die Datenerhebung Glauben schenken möchte, sollte dies im Sinne seines Rechts auf informationelle Selbstbestimmung möglich sein.

Einen ähnlichen Ansatz liefert die sog. „Zwei-Klick-Lösung" von *Heise*:[725] Die Plug-Ins werden dort erst aktiviert, wenn der Nutzer es aktiv betätigt. *Heise* geht davon aus, dass „[e]in Klick auf einen dieser Buttons bedeutet […], dass der Anwender seine Zustimmung erteilt, Daten an den jeweiligen Betreiber des sozialen Netzes zu übermitteln."[726] Allerdings sieht diese Lösung keine umfassende Information der Nutzer vor, sodass für den Nutzer nicht ersichtlich ist, dass er gerade eine datenschutzrechtliche Einwilligungserklärung abgibt. Eine „Zustimmung" durch den Nutzer ist nur durch den Klick auf das Plug-In nicht gegeben.

3. Umfang der Betroffenenrechte

Ergänzend sei auf den Umfang der Betroffenenrechte bei Social Plug-Ins hinzuweisen.[727] Denn die Betroffenenrechte – insbesondere das Auskunftsrecht aus § 34 BDSG bzw. Art. 12 lit. a DSRL sowie Art. 15 DSGVO bzw. § 34 BDSG-neu und das Recht auf Berichtigung, Löschung oder Sperrung der Daten i. S. d. § 35 BDSG bzw. Art. 12 lit. b DSRL sowie Art. 17 DSGVO bzw. § 35 BDSG-neu – müssen in ihrem Umfang den Möglichkeiten des Verantwortlichen angepasst sein. So kann sich das Auskunftsrecht über die Verarbeitung nur auf denjenigen erstrecken, der darüber Auskunft geben kann, d. h. im gewählten Beispiel auf *Facebook*. Die Art. 29-Datenschutzgruppe hat hierzu ausgeführt, dass „[i]n dieser Hinsicht […] der Rechtsrahmen flexibel ausgelegt werden [muss] […]".[728] Solange der Nutzer hinreichend über die Verantwortlichkeit in den verschiedenen Verwendungsstadien informiert wird,[729] ist dies auch interessengerecht und keine unzumutbare Belastung der Betroffenen.

---

725 *Heise Medien GmbH & Co. KG,* 2 Klicks für mehr Datenschutz, abrufbar unter https://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html (abgerufen am 13.10.2017).

726 *Heise Medien GmbH & Co. KG,* 2 Klicks für mehr Datenschutz, abrufbar unter https://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html (abgerufen am 13.10.2017).

727 Vgl. zu Betroffenenrechten Kap. 3 Pkt. D.I, S. 216.

728 *Art. 29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavorial Targeting. WP 171 (22.06.2010), S. 14.

729 Vgl. Kap. 3 C.I, S. 201.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

III. Zusammenfassung

Viele Social Plug-Ins werden vom Nutzer unbemerkt aktiviert und können sich deswegen nicht auf einen Zulässigkeitstatbestand stützen. Allein bei einem Klick durch den Nutzer auf ein Plug-In könnte die Übertragung einzelner Daten für die Darstellung des Angebots erforderlich sein. Die Zulässigkeit einer weitergehenden Datenverarbeitung ist jedoch dann ausgeschlossen, wenn dem Nutzer nicht bewusst ist, dass der Klick das Angebot eines Dritten aktiviert und eine solche Datenverarbeitung auslöst. Die Zulässigkeit der Einbindung von Social Plug-Ins muss also durch die Einwilligung des Website-Besuchers erreicht werden. Diese erfolgt dann informiert, wenn der Nutzer bei einem Klick auf das Plug-In zunächst informiert wird, dass damit das Angebot eines Dritten in Anspruch genommen wird und in einem nächsten Schritt der Dritte vor Datenverarbeitung über die Phasen der Datenverarbeitung aufklärt.

D. Betroffenenrechte und Durchsetzbarkeit

Den Betroffenen gestehen sowohl BDSG bzw. DSRL als auch DSGVO bzw. BDSG-neu einige Rechte zu, die den Schutz ihrer personenbezogenen Daten gewährleisten sollen. Im BDSG finden sie sich für den vorliegend relevanten nicht-öffentlichen Bereich in §§ 33 – 35, in der DSRL in Art. 10 – 12. In der DSGVO sind die Betroffenenrechte in Art. 12 – 22 zu finden, wobei Art. 23 DSGVO mögliche Beschränkungen durch Unionsrecht oder durch Mitgliedstaaten im Zuge von Öffnungsklauseln regelt. Diese finden sich in Deutschland in §§ 32 ff. BDSG-neu.[730]

I. Betroffenenrechte im BDSG und Änderungen durch die DSGVO

1. Betroffenenrechte im BDSG

Das BDSG sieht in § 33 BDSG Informationspflichten des Betroffenen durch die verantwortliche Stelle vor, sofern Daten erstmalig ohne Kenntnis des Betroffenen gespeichert werden (§ 33 Abs. 1 S. 1 BDSG) oder im Falle von § 29 BDSG erstmalig übermittelt werden (§ 33 Abs. 1 S. 2 BDSG). Dieses Recht soll also sichern, dass der Betroffene überhaupt Kenntnis von

730 Vgl. Kap. 3 Pkt. D.I.3, S. 223.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

dem Umgang mit seinen personenbezogenen Daten erfährt. Denn nur dann kann der Betroffene seine weiteren Rechte geltend machen. Ein solch weiteres Recht ist zum einen das Auskunftsrecht aus § 34 BDSG. Das Auskunftsrecht soll sicherstellen, dass der Betroffene Kenntnis darüber erlangen kann, welche Stellen welche personenbezogenen Daten über ihn haben.[731] Interessant ist hierbei insbesondere die Regelung des § 34 Abs. 1a BDSG, nach welcher der Betroffene, dessen personenbezogenes Datum i. S. d. § 28 Abs. 3 S. 4 BDSG übermittelt wurde,[732] Auskunft über die Herkunft der Daten erhalten kann. Schließlich sieht § 35 BDSG gewisse Berichtigungs- und Löschrechte des Betroffenen vor.

2. Änderungen durch die DSGVO

Diese Rechte finden sich ebenfalls in der DSGVO: Auch hier finden sich Informationspflichten (Art. 13 f. DSGVO), Auskunftsrechte (Art. 15 DSGVO) sowie Rechte auf Berichtigung, Löschung und Sperrung (in der Terminologie der DSGVO: Einschränkung der Verarbeitung) der Daten (Art. 16 – 18 DSGVO). Daneben kommen weitere Betroffenenrechte zum Tragen, etwa das Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO.

a) Betroffenenrechte bei der Verarbeitung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO

Die bisherigen Ergebnisse der Betrachtung zeigen, dass sich die Verarbeitung in den hier besprochenen Fällen beinahe immer auf Art. 6 Abs. 1 S. 1 lit. f DSGVO stützen wird. Da die Norm sehr breit ausgelegt werden kann, wohnt ihr ein besonderes Missbrauchsrisiko inne.[733] Dem steuert die DSGVO entgegen, indem sie für die Datenverarbeitung gem. Art. 6 Abs. 1 S. 1 lit. f DSGVO an verschiedenen Stellen zusätzliche Vorschriften zu den Betroffenenrechten vorsieht: Gem. Art. 13 Abs. 1 lit. d sowie Art. 14 Abs. 2 lit. d DSGVO muss der Verantwortliche den Betroffenen über das berechtigte Interesse, das er an der Verarbeitung hat, informieren.

731 *Kühling/Seidel/Sivridis,* Datenschutzrecht, Rn. 526, S. 223.
732 Vgl. Kap. 3 Pkt. B.I.b.aa.ii, S. 170.
733 Vgl. Kap. 3 Pkt. A.III.2.c.aa, S. 125.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aa) Widerspruchsrecht, Art. 21 DSGVO

Besonders wichtig ist zudem das Widerspruchsrecht i. S. d. Art. 21 Abs. 1 S. 1 DSGVO; es ist für den Betroffenen der erste Schritt, die Verarbeitung zu unterbinden (Art. 21 Abs. 1 S. 2, Abs. 3 DSGVO) und die Daten gegebenenfalls i. S. d. Art. 17 Abs. 1 lit. c DSGVO löschen zu lassen.[734]

Erfolgt die Verarbeitung aufgrund von Art. 6 Abs. 1 S. 1 lit. f DSGVO, darf die betroffene Person jederzeit „[…] aus Gründen, die sich aus ihrer besonderen Situation ergeben […]" der Verarbeitung widersprechen.

i) Verschobener Abwägungsmaßstab, Art. 21 Abs. 1 S. 1 DSGVO

Nach einem Widerspruch darf der Verantwortliche gem. Art. 21 Abs. 1 S. 2 DSGVO die Daten nicht mehr verarbeiten, „[…] es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen […]", die die Betroffeneninteressen überwiegen. Das bedeutet, dass auch das Widerspruchsrecht aus Art. 21 DSGVO eine Interessenabwägung zwischen den Verarbeiter- und den Betroffeneninteressen vorsieht. Allerdings verschiebt sich der Bewertungsmaßstab im Vergleich zu Art. 6 Abs. 1 S. 1 lit. f DSGVO: Während bei Art. 6 Abs. 1 S. 1 lit. f DSGVO auf die „[…] berechtigten Interessen des Verantwortlichen […]" abgestellt wird, sind nach erfolgtem Widerspruch zwingende schutzwürdige Interessen nötig. Zudem enthält Art. 21 Abs. 1 S. 2 DSGVO eine Beweislastumkehr zu Lasten des Verantwortlichen, der nun in der Pflicht ist, seine zwingend schutzwürdigen Interessen nachzuweisen.

ii) Widerspruchsgründe und entgegenstehende Verarbeiterinteressen, Art. 21 Abs. 1 S. 1 DSGVO

Fraglich ist, welche Gründe die betroffene Person zur Geltendmachung ihres Widerspruchsrechts anführen muss. Weder Art. 21 Abs. 1 S. 1 DSGVO noch die Erwägungsgründe präzisieren näher, was unter „[…] Gründen, die sich aus ihrer besonderen Situation ergeben […]" zu verstehen ist. Aus dem Wortlaut selbst geht jedenfalls hervor, dass es sich hierbei um eine atypische Situation handeln muss, die der Verantwortliche nicht vorhersehen musste und daher in die durch ihn selbst vorgenommene Verarbeitung nicht

734 Vgl. Kap. 3 Pkt. D.I.2.bb, S. 219.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

einbeziehen konnte,[735] etwa besondere familiäre Gründe des Betroffenen.[736]

Auch die „[…] zwingende[n] schutzwürdige[n] Gründe […]", die der Verantwortliche nachweisen muss, werden nicht näher definiert. Schutzwürdig sind die vom Unionsrecht anerkannten Gründe, etwa die Gründe aus Art. 23 Abs. 1 DSGVO.[737] Diese Gründe müssen zudem zwingender Natur sein, d. h., dass es keine anderen Möglichkeiten gibt, das Ziel der Verarbeitung, das in dem schutzwürdigen Grund liegt, zu erreichen.[738]

iii) Widerspruch bei Verarbeitung zu Zwecken der Direktwerbung, Art. 21 Abs. 1 S. 2 DSGVO

Erfolgt die Verarbeitung zu Zwecken der Direktwerbung, kann der Betroffene gem. Art. 21 Abs. 2 DSGVO widersprechen und zwar ohne Angabe von Gründen. Art. 21 Abs. 3 DSGVO stellt klar, dass der Verantwortliche sie dann nicht mehr verarbeiten darf und keine – auch keine erschwerte – Interessenabwägung möglich ist.

bb) Löschpflichten, Art. 17 DSGVO

Art. 17 DSGVO sieht ein Löschrecht für den Betroffenen vor. Noch in der Endfassung trägt dieses Recht den exklamatorischen Beinamen „Recht auf Vergessenwerden", umschreibt jedoch lediglich das bereits gem. Art. 12 lit. b Var. 2 DSRL existierende Recht auf Löschung.

Hat der Betroffene gem. Art. 21 Abs. 1 DSGVO Widerspruch eingelegt, so kann er die unverzügliche Löschung seiner personenbezogenen Daten i. S. d. Art. 17 Abs. 1 lit. c DSGVO verlangen, sofern „[…] keine vorrangigen berechtigten Gründe für die Verarbeitung [vorliegen] […]". Im Gegensatz zu Art. 21 Abs. 1 S. 2 DSGVO müssen die entgegenstehenden Verarbeiterinteressen hier also nicht zwingend schutzwürdiger Natur, sondern lediglich vorrangig berechtigter Natur sein. Klar ist jedoch insoweit, dass mit

735 *Martini*, in: Paal/Pauly, DSGVO, Art. 21, Rn. 30; *Herbst*, in: Kühling/Buchner, DSGVO, Art. 21, Rn. 15.
736 *Martini*, in: Paal/Pauly, DSGVO, Art. 21, Rn. 30.
737 *Martini*, in: Paal/Pauly, DSGVO, Art. 21, Rn. 38; *Herbst*, in: Kühling/Buchner, DSGVO, Art. 21, Rn. 20.
738 *Martini*, in: Paal/Pauly, DSGVO, Art. 21, Rn. 39; *Herbst*, in: Kühling/Buchner, DSGVO, Art. 21, Rn. 21.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

dem Begriff der „Verarbeitung" i. S. d. Art. 17 Abs. 1 lit. c DSGVO nur die Speicherung gemeint sein kann. Andernfalls könnte der Verantwortliche gestützt auf den Wortlaut den strengen Maßstab der entgegenstehenden zwingenden schutzwürdigen Verarbeiterinteressen i. S. d. Art. 21 Abs. 1 S. 2 DSGVO umgehen, obwohl er nach erfolgtem Widerspruch die Verarbeitung beenden muss, Art. 21 Abs. 1 DSGVO.

Erfolgt der Widerspruch gegen die Verarbeitung zu Zwecken der Direktwerbung, hat der Verarbeiter die Daten zu löschen, ohne dass eine Interessenabwägung möglich wäre.

b) Recht auf Datenübertragbarkeit

Grundsätzlich neu ist das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO.

aa) Zielsetzung des Art. 20 DSGVO

Gem. Art. 20 Abs. 1 DSGVO soll der Betroffene seine personenbezogenen Daten „[…] in einem strukturierten, gängigen und maschinenlesbaren Format […] erhalten […]". Zudem hat der Betroffene „[…] das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt werden, zu übermitteln […]". Voraussetzung ist hierfür, dass die Verarbeitung auf Art. 6 Abs. 1 S. 1 lit. a DSGVO beruht und es sich um eine Verarbeitung mithilfe automatisierter Verfahren handelt. Für die Verarbeitung durch soziale Netzwerke treffen diese Voraussetzungen grundsätzlich zu. Fraglich ist jedoch, wie wirksam ein solches Recht auf Datenübertragbarkeit in Bezug auf soziale Netzwerke ist; tatsächlich wird in der Diskussion um das Recht auf Datenübertragbarkeit der Wechsel von einem sozialen Netzwerk in ein anderes regelmäßig als Paradebeispiel angeführt.[739] Das Recht soll dem Betroffenen eine höhere Kontrolle über seine personenbezogenen Daten zugestehen, EG 68 S. 1 DSGVO, sowie sog. „lock-in"-Effekten[740] vorbeugen; der Nutzer soll also nicht gezwungen sein, bei einem bestimmten

739 *Hornung*, ZD 2012, 99, 103; *Jaspers*, DuD 2012, 571, 573; *Herbst*, in: Kühling/Buchner, DSGVO, Art. 20, Rn. 2; *Wedde,* DSGVO, S. 19.

740 *Herbst*, in: Kühling/Buchner, DSGVO, Art. 20, Rn. 2; *Roßnagel/Richter/Nebel*, ZD 2013, 103, 104; *Hornung*, ZD 2012, 99, 103.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Anbieter zu bleiben, nur weil der Wechsel durch die Bindung der Daten an einen bestimmten Anbieter erschwert wird.

bb) Schwierigkeiten der Umsetzbarkeit

Faktisch wirft diese Zielsetzung jedoch die Frage nach der technischen und praktischen Umsetzbarkeit auf.

i) Unterschiedliche Strukturen der sozialen Netzwerke

Gem. Art. 20 Abs. 2 DSGVO sollen die Daten vom ursprünglichen Verantwortlichen an den, vom Betroffenen ausgewählten, „neuen" Verantwortlichen übertragen werden. Allerdings hat jedes soziale Netzwerk eine ganz eigene Struktur. Vor diesem Hintergrund könnte die technische Realisierung der Datenübertragung zur Erreichung des Schutzes vor „lock-in"-Effekten Probleme bereiten.[741] Letztlich wird der Betroffene in jedem neuen sozialen Netzwerk sich wiederum ein neues Profil anlegen müssen und es entsprechend pflegen müssen, sodass sich das Recht aus Art. 20 Abs. 2 DSGVO als wenig praktikabel erweisen könnte.

ii) Praktische Umsetzbarkeit hinsichtlich Daten Dritter

Noch bedeutsamer ist jedoch der Hinweis auf die fehlende praktische Umsetzbarkeit hinsichtlich Daten Dritter. Denn sollten die Datensätze mehr als nur die Daten desjenigen Betroffenen, der sein Recht aus Art. 20 DSGVO geltend macht, betreffen, sollen die Grundrechte und Grundfreiheiten anderer Personen unberührt bleiben, EG 68 S. 6 DSGVO. Diese Klarstellung ist nur folgerichtig, da andernfalls die Herausgabe personenbezogener Daten anderer Personen wiederum eine – nicht legitimierte – Verarbeitung personenbezogener Daten darstellen würde. Soziale Netzwerke leben jedoch gerade vom Austausch der Nutzer untereinander, so dass es sich bei den Datensätzen regelmäßig um personenbezogene Daten nicht nur der Betroffenen, sondern auch anderer Nutzer handeln wird.[742] Die Gegenansicht, die

741 Ähnlich *Bräutigam/Schmidt-Wudy*, CR 2015, 56, 59 f.
742 Ebenso *Jülicher/Röttgen/Schönfeld*, ZD 2016, 358, 361.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

das Recht auf Übertragbarkeit auch auf Daten Dritter erstreckt sieht,[743] würde dazu führen, dass Art. 20 DSGVO zu einem weiteren Erlaubnistatbestand für die Verarbeitung personenbezogener Daten ausgeweitet würde, und Nutzer, die mit Einwilligung eines Anderen Fotos von sich selbst und dieser anderen Person hochgeladen haben, die Übertragung dieses Fotos an jeden beliebigen anderen Plattformbetreiber verlangen können. Allerdings erstreckt sich die Einwilligung, dass ein Foto in einem bestimmten sozialen Netzwerk hochgeladen wird, nicht notwendigerweise darauf, es auch in einem anderen Netzwerk hochzuladen. Diese Ansicht ist schon deswegen fragwürdig, weil sie das Bedürfnis des Nutzers nach einem unkomplizierten Anbieterwechsel pauschal höher gewichtet als das Recht auf informationelle Selbstbestimmung des Dritten. Selbst wenn man jedoch mit der Gegenmeinung davon ausginge, dass sich das Recht auf Daten Dritter erstreckt, bliebe die Wirkkraft des Rechts wohl begrenzt. Denn soziale Netzwerke entfalten ihre volle Funktionalität nur dann, wenn der Nutzer dort Kontakte hat, mit denen er kommunizieren kann. Das Recht aus Art. 20 DSGVO darf jedoch keinesfalls zu einer Verarbeitung personenbezogener Daten Dritter in dem Sinne führen, dass der Betroffene auch all seine Kontakte in das neue Netzwerk automatisch umzieht, also automatisch Profile für Dritte angelegt werden.

cc) Art. 20 DSGVO als Erweiterung des Auskunftsrechts

Sollte die Übertragung der personenbezogenen Daten des Betroffenen überhaupt ohne Weiteres möglich sein, ist angesichts der genannten Probleme hinsichtlich der praktischen Umsetzbarkeit mit Bezug auf die Daten Dritter die volle Wirkkraft des Rechts auf Datenübertragbarkeit und der erwünschte Schutz vor „lock-in"-Effekten wohl begrenzt. So ist zwar durchaus denkbar, dass der Betroffene vom Plattformbetreiber die personenbezogenen Daten herausverlangt, die er über ihn gespeichert hat. In diesem Fall würde Art. 20 Abs. 1 DSGVO eine Art erweiterten Auskunftsanspruch darstellen. Die Verwandtschaft zum Auskunftsanspruch zeigt sich bereits daran, dass in Art. 15 Abs. 2 des DSGVO-Entwurfs des Parlaments[744] das Recht auf Datenübertragbarkeit als „Recht auf Herausgabe der Daten" im

743 Vgl. *Schantz*, NJW 2016, 1841, 1845; *Herbst*, in: Kühling/Buchner, DSGVO, Art. 20, Rn. 3.

744 P7_TA(2014)0212.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Auskunftsanspruch verortet war. Die Wirkung des Art. 20 DSGVO hinsichtlich des erleichterten Wechsels von sozialen Netzwerken ist demgegenüber jedoch eingeschränkt.

3. Beschränkungen der DSGVO-Betroffenenrechte durch nationales Recht

Art. 23 DSGVO sieht schließlich die Möglichkeit vor, die Betroffenenrechte der DSGVO durch mitgliedstaatliches Recht zur Erreichung von in Art. 23 Abs. 1 DSGVO gelisteten Zielen zu beschränken.

a) Änderungen im BDSG-neu

Die in Art. 23 Abs. 1 DSGVO gelisteten Ziele, zu deren Zweck die Betroffenenrechte eingeschränkt werden können, umfassen etwa die nationale Sicherheit (lit. a), die Landesverteidigung (lit. b) und die Verfolgung von Straftaten (lit. d), jedoch auch den Schutz der betroffenen Person sowie der Rechte und Freiheiten anderer Personen (lit. i).[745] Im BDSG-neu[746], dem der Bundesrat am 12.05.2017 zugestimmt hat,[747] hat Deutschland von diesem Recht Gebrauch gemacht. Im Entwurf der Bundesregierung vom 24.02.2017[748] (im Folgenden: BDSG-neu-E) waren noch Beschränkungen der Informationspflicht bei der Datenerhebung bei dem Betroffenen im Fall der Zweckänderung (Art. 13 Abs. 3 DSGVO) gem. § 32 Abs. 1 Nr. 1 BDSG-neu-E bei unverhältnismäßigem Aufwand für den Datenverarbeiter sowie der Informationspflicht im Falle der Datenerhebung, die nicht beim Betroffenen erfolgt (Art. 14 Abs. 1, 2, 4 DSGVO) gem. § 33 Abs. 1 Nr. 2 lit. a BDSG-neu-E bei Gefährdung allgemein anerkannter Geschäftszwecke des Verantwortlichen, vorgesehen. Beide Normen sind in der endgültigen Fassung stark modifiziert worden. So ist in § 32 Abs. 1 BDSG-neu die Beschränkung bei unverhältnismäßigem Aufwand ersetzt worden durch eine

745 Ausführlich zu dieser Öffnungsklausel *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 68 ff.

746 Art. 1 DSAnpUG-EU, BGBl. 2017 I, 2097; vgl. auch Einleitung und Gang der Untersuchung, Pkt. B, S. 28.

747 BR-Drucks. 332/17 (Beschluss).

748 Art. 1 des Gesetzesentwurfs der Bundesregierung. Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 24.02.2017, BT-Drucks. 18/11325.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ganz andere Voraussetzung, sodass sie nun lediglich analog gespeicherte Daten betrifft. Damit ist die Beschränkung für die Verarbeitung im Rahmen von sozialen Online-Netzwerken kaum noch relevant. Auch § 33 Abs. 1 BDSG-neu-E wurde gänzlich ersetzt: Statt einer Beschränkung des Informationsrechts aus anerkannten Geschäftsgründen des Verarbeiters greift die Norm nun u. a. zur Verteidigung zivilrechtlicher Ansprüche.

Im Vergleich zum Entwurf der Bundesregierung ist die Beschränkung des Auskunftsrechts (Art. 15 DSGVO) im BDSG-neu nahezu unverändert geblieben. Es ist ausgeschlossen bei unverhältnismäßigem Aufwand für den Verantwortlichen, § 34 Abs. 1 Nr. 2 BDSG-neu, wobei jedoch kumulativ hinzutreten muss, dass „[…] [lit. a] die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsgemäßer Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder [lit. b] ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen […] und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist." Insofern erinnert der Ausschluss des Auskunftsrechts an die bislang bestehende Ausschlussmöglichkeit der Benachrichtigungspflicht des Betroffenen gem. § 33 Abs. 2 S. 1 Nr. 2 BDSG.

Während im Regierungsentwurf das Löschrecht des Betroffenen (Art. 17 Abs. 1 DSGVO) ebenfalls bei unverhältnismäßigem Aufwand für den Datenverarbeiter ausgeschlossen war und stattdessen durch eine Sperrung der Daten ersetzt werden sollte, § 35 Abs. 1 BDSG-neu-E, wurde die Norm in der endgültigen Fassung dahingehend eingeschränkt, dass dies nur für Fälle der nicht-automatisierten Datenverarbeitung gelten soll. Auch diese Beschränkung entfaltet damit bei Internetsachverhalten kaum Relevanz.

Besonders die geplanten und nun verworfenen Beschränkungen im Entwurf der Bundesregierung hätten eine Ausweitung der Beschränkungsmöglichkeiten von Betroffenenrechten im Vergleich zum BDSG bedeutet. So sieht der bereits genannte § 33 Abs. 2 Nr. 2 BDSG zwar auch einen Ausschluss der Benachrichtigungspflicht des Betroffenen bei unverhältnismäßig hohem Aufwand für den Verantwortlichen vor, jedoch nur, wenn die Daten „[…] aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen."

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Reichweite der Öffnungsklausel des Art. 23 Abs. 1 DSGVO

Insbesondere die recht pauschalen Beschränkungsgründe des „unverhältnismäßigen Aufwand[s]“ sowie der „allgemein anerkannten Geschäftsgründe“ warfen Zweifel daran auf, ob die Beschränkung aus diesen Gründen überhaupt noch von der Öffnungsklausel des Art. 23 Abs. 1 DSGVO gedeckt gewesen wäre.[749]

In Betracht kommt insofern zwar Art. 23 Abs. 1 lit. i DSGVO, der die Beschränkung der Betroffenenrechte zum „[…] Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen“ erlaubt, wobei mit einer anderen Person auch durchaus der Verantwortliche gemeint sein kann.[750] Ebenso lässt es sich grundsätzlich unter den Wortlaut subsumieren, einen „unverhältnismäßigen Aufwand“ als Beschränkungsgrund zum Schutz der Interessen des Verantwortlichen im BDSG-neu festzusetzen. Mit Blick auf die anderen Ziele des Art. 23 Abs. 1 DSGVO ist aber schon fraglich, ob diese Beschränkung tatsächlich „[…] in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt […]“ i. S. d. Art. 23 Abs. 1 DSGVO. Abgesehen von Art. 23 Abs. 1 lit. i DSGVO benennt die Norm überwiegend Gründe des öffentlichen Interesses, an welche die Beschränkung der Betroffenenrechte durch nationales Recht geknüpft werden kann – etwa aus Gründen der nationalen Sicherheit (lit. a) oder zum Schutz der Unabhängigkeit der Justiz (lit. f Alt. 1). Dies spricht dafür, dass Art. 23 Abs. 1 lit. i Alt. 2 DSGVO nicht unbegrenzt dahingehend ausgelegt werden sollte, dass jedes Interesse des Verantwortlichen für eine Beschränkung der Betroffenenrechte ausreicht. Schließlich bestünde bei einer zu großzügigen Auslegung des Art. 23 Abs. 1 lit. i Alt. 2 DSGVO die Gefahr, dass im Zusammenspiel mit Art. 6 Abs. 4 DSGVO die Norm

749 Vgl. etwa *Wolff*, Schriftliche Stellungnahme zu dem Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und - Umsetzungsgesetz EU – DSAnpUG-EU) – BT-Drs. Drucksache 18/11325, abrufbar unter http://www.cr-online.de/18-4-824-e-data.pdf (abgerufen am 13.10.2017), S. 14; *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts. Positionen der Bundesbeauftragten für den Datenschutz, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/DSAnpaUG_Positionspapier.html?cms_templateQueryString=dsanpug&cms_sortOrder=score+desc (abgerufen am 13.10.2017), S. 16 f.

750 Ebenso *Bäcker*, in: Kühling/Buchner, DSGVO, Art. 23, Rn. 32.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

genutzt werden könnte, um auch im privaten Bereich weitreichende nationale Zulässigkeitstatbestände zu schaffen. Denn Art. 6 Abs. 4 DSGVO enthält eine Öffnungsklausel für die Mitgliedstaaten, nationale Regelungen für zweckverändernde Verarbeitungen zu erhalten oder zu schaffen, sofern es einem der in Art. 23 Abs. 1 DSGVO gelisteten Ziele dient.[751] Eine sehr weite Interpretation des Art. 23 Abs. 1 lit. i Alt. 2 DSGVO könnte also zu einer Aushebelung der mit der DSGVO bezweckten unionalen Vereinheitlichung datenschutzrechtlicher Regelungen führen.[752]

Klargestellt werden muss zudem, dass die Beschränkung auch nicht auf Art. 14 Abs. 5 DSGVO gestützt werden könnte, der einen unverhältnismäßigen Aufwand für den Verantwortlichen als Beschränkungsgrund für Informationspflichten i. S. d. Art. 14 DSGVO nennt. Denn diese Norm stellt keine Öffnungsklausel dar,[753] erst recht nicht um Betroffenenrechte aus Art. 13 DSGVO einzuschränken.[754]

Keine andere Bewertung ergibt sich hinsichtlich des Beschränkungszwecks der „allgemein anerkannte[n] Geschäftszwecke" in § 33 Abs. 1 Nr. 2 lit. a BDSG-neu-E. Denn der Gesetzesentwurf stellte klar, dass damit das „Verständnis wie bisher" des Begriffs fortgetragen werden sollte,[755] eine Beschränkung also zu jedem geschäftlichen, beruflichen oder gewerblichen Zweck hätte erfolgen können, den der Verantwortliche selbst hätte festsetzen können.[756]

---

751 *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 38 ff.

752 Vgl. auch *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 428.

753 Vgl. zur Öffnungsklausel in Art. 14 DSGVO *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 56 f.

754 Der Referentenentwurf des Bundesministeriums des Innern zum DSAnpUG-EU v. 23.11.2016 stützte die Norm u. a. noch auf den Rechtsgedanken des Art. 14 Abs. 5 DSGVO, vgl. https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/12/161123_BDSG-neu-RefE_-2.-Ressortab-Verbaende-Laender.pdf (abgerufen am 13.10.2017).

755 Gesetzesentwurf der Bundesregierung. Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 v. 24.02.2017. BT-Drucks. 18/11325, S. 103.

756 Vgl. zum Begriff des Geschäftszwecks *Simitis*, in: Simitis, BDSG, § 28, Rn. 22 f.; kritisch zu § 33 Abs. 1 Nr. 2 BDSG-neu-E auch *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts. Positionen der Bundesbeauftragten für den Datenschutz, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/DSAnpaUG_Positionspapier.html?cms_templateQueryString=dsanpug&cms_sortOrder=score+desc (abgerufen am 13.10.2017), S. 16.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Die diskutierten Beschränkungen stellten also, insbesondere soweit sie nicht hinzutretenden spezifischen Voraussetzungen unterlagen, eine wohl vom Wortlaut der Öffnungsklausel gedeckte, hinsichtlich des Telos der Norm jedoch eher zweifelhafte Ausreizung der Öffnungsklausel dar.

Daher ist es erfreulich, dass sich die im Entwurf der Bundesregierung geplanten Beschränkungsmöglichkeiten nicht durchgesetzt haben. Zwar ist das Auskunftsrecht aus § 34 BDSG-neu weiterhin beschränkbar, sofern die Verarbeitung einen unverhältnismäßigen Aufwand für den Verantwortlichen darstellen würde; allerdings nur unter Hinzutreten weiterer, konkretisierter Voraussetzungen, etwa der Speicherung aufgrund von gesetzlichen Aufbewahrungsfristen. Die Norm begegnet daher nicht mehr denselben Bedenken hinsichtlich ihrer Unionskonformität wie noch die Vorgängervorschrift des Gesetzesentwurfs.

II. Durchsetzbarkeit des Datenschutzrechts

Fraglich ist, wie die datenschutzrechtlichen Bestimmungen durchgesetzt werden können und gegen datenschutzrechtliche Verstöße vorgegangen werden kann. Den Aufsichtsbehörden kommt hierbei eine zentrale Rolle zu (dazu 1.). Sowohl das BDSG als auch die DSGVO sehen zudem gewisse Sanktionierungsmöglichkeiten in Form von Bußgeldern oder gar Straftatbeständen vor (dazu 2.). Zudem sieht die DSGVO Präventivmaßnahmen vor, um Datenschutzverstößen schon im Vorfeld entgegenzuwirken (dazu 3.). Schließlich ist ein zivilrechtliches Vorgehen möglich (dazu 4.).

1. Aufsichtsbehörden

a) Rolle der Aufsichtsbehörden

Als „Hüter [der] Grundrechte und Grundfreiheiten“[757] spielen die Kontrollstellen eine zentrale Rolle bei der Durchsetzung der datenschutzrechtlichen Vorgaben. Primärrechtlich in Art. 8 Abs. 3 GRCh verankert, kommt ihnen gem. Art. 28 Abs. 1 DSRL die Aufgabe zu, „in völliger Unabhängigkeit“ die Umsetzung der mitgliedstaatlichen Vorschriften zu überwachen. Die

757 *EuGH,* Urt. v. 09.03.2010, Rs. C-518/07, ECLI:EU:C:2010:125, Rn. 23 – Kommission/Deutschland.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Befugnisse der Kontrollstellen finden sich in Art. 28 Abs. 3 DSRL und umfassen insbesondere Untersuchungs- sowie Einwirkungsbefugnisse. Im BDSG finden sich die Vorgaben zu den Aufsichtsbehörden für den nichtöffentlichen Bereich in § 38 BDSG. Gem. § 38 Abs. 1 BDSG kontrollieren sie die Ausführung des BDSG sowie weiterer datenschutzrechtlicher Bestimmungen. § 38 Abs. 5 BDSG gibt den Aufsichtsbehörden hierzu die Möglichkeit von Beseitigungsanordnungen (§ 38 Abs. 5 S. 1 BDSG) oder der Untersagung des Umgangs mit personenbezogenen Daten (§ 38 Abs. 5 S. 2 BDSG).

b) Zuständigkeit bei grenzüberschreitenden Sachverhalten

Grundsätzlich ist jede Aufsichtsbehörde für die Erfüllung ihrer Aufgaben in ihrem eigenen Hoheitsgebiet zuständig, vgl. Art. 55 Abs. 1 DSGVO. Fraglich ist, welche Datenschutzbehörde bei grenzüberschreitenden Sachverhalten für die Ausübung ihrer Befugnisse zuständig ist. Die Frage stellt sich für die vorliegende Thematik in besonderem Maße, da Internetsachverhalten die Grenzüberschreitung inhärent ist. Beispielhaft kann der Fall angeführt werden, dass ein Verantwortlicher nicht in dem Land des Nutzers niedergelassen ist und der Nutzer jedoch Beschwerde bei der Aufsichtsbehörde seines Mitgliedstaates einlegt.

aa) Zuständigkeit nach der DSRL

Gem. Art. 28 Abs. 6 S. 1 DSRL ist „[j]ede Kontrollstelle […] im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr […] übertragenen Befugnisse zuständig, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anwendbar ist.“ Art. 28 Abs. 4 S. 1 DSRL stellt zudem klar, dass jede Person sich an jede Kontrollstelle wenden kann, also nicht an eine bestimmte Kontrollstelle gebunden ist. Daraus geht zum einen hervor, dass die Zuständigkeit der Kontrollstellen dem territorial anwendbaren Recht nicht grundsätzlich folgt und zum anderen, dass der Betroffene nicht verpflichtet ist, die zuständige Kontrollstelle selbst zu identifizieren und sich gar an eine Kontrollstelle in einem fremden Mitgliedstaat zu wenden.

Der *EuGH* hat daher klargestellt, dass jede Kontrollstelle zumindest die Untersuchungsbefugnisse aus Art. 28 Abs. 3 Spiegelstr. 1 DSRL ausüben

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

darf.[758] Kommt sie im Rahmen dieser Untersuchungen jedoch zu dem Schluss, dass das Recht eines anderen Mitgliedstaats anwendbar ist, dann muss sie den Sachverhalt an die Kontrollstelle dieses Mitgliedstaats gem. Art. 28 Abs. 6 S. 2 DSRL überweisen. Insbesondere Sanktionen dürfen in diesem Fall nicht verhängt werden.[759]

bb) Zuständigkeit nach der DSGVO

Die Befugnisse der Aufsichtsbehörden finden sich in Art. 58 DSGVO. Im Vergleich zur DSRL sieht die DSGVO deutlich detailliertere Vorgaben zur Zuständigkeit und Zusammenarbeit der mitgliedstaatlichen Aufsichtsbehörden vor. So sieht zwar auch die DSGVO gem. Art. 55 Abs. 1 DSGVO im Grundsatz vor, dass jede Aufsichtsbehörde für die Ausübung ihrer Befugnisse auf dem Hoheitsgebiet ihres Mitgliedstaats zuständig ist. Für grenzüberschreitende Sachverhalte ist jedoch die Aufsichtsbehörde der Hauptniederlassung zuständig (sog. federführende Behörde), Art. 56 Abs. 1 DSGVO. Damit dieses sog. „One Stop-Shop"-Verfahren nicht dazu führt, dass der Betroffene sich an eine Behörde in einem fremden Mitgliedstaat wenden muss, räumt ihm Art. 77 Abs. 1 DSGVO das Recht ein, sich an jede Aufsichtsbehörde, insbesondere die seines Aufenthalts- oder Arbeitsortes, zu wenden.[760] Abweichend von Art. 56 Abs. 1 DSGVO ist die so befasste Aufsichtsbehörde zuständig, sich mit dieser Beschwerde zu befassen, Art. 56 Abs. 2 DSGVO. Die betroffene Behörde muss sich an die federführende Behörde wenden, die binnen drei Wochen entscheiden muss, ob sie sich mit dem Fall befasst oder nicht, Art. 56 Abs. 3 S. 1, 2 DSGVO. Sollte sie sich für eine Befassung mit dem Fall entscheiden, müssen die Aufsichtsbehörden nach dem Verfahren gem. Art. 60 ff. DSGVO zusammenarbeiten. Die Zusammenarbeit umfasst etwa den Austausch von Informationen (vgl. etwa Art. 60 Abs. 1, 3 DSGVO), die Gewährung gegenseitiger Amtshilfe (Art. 61 DSGVO) und sieht die Möglichkeit gemeinsamer Untersuchungs- sowie Durchsetzungsmaßnahmen vor (Art. 62 DSGVO). Erzielen die Aufsichtsbehörden in diesem Verfahren keine Einigung, wird das Kohärenzverfahren gem. Art. 63 ff. DSGVO eingeleitet.

---

758 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 54 – Weltimmo.

759 *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639, Rn. 55–58 – Weltimmo.

760 *Schantz*, NJW 2016, 1841, 1846 f.; kritisch zu den Entwürfen der DSGVO *Nguyen*, ZD 2015, 265, 266.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

2. Sanktionen

Die DSGVO normiert zudem die Möglichkeit empfindlicher Geldbußen. Diese sind im Vergleich zum BDSG deutlich gestiegen. § 43 Abs. 3 BDSG sieht Bußgelder i. H. v. maximal 50.000 bzw. 300.000 Euro vor. Die in Deutschland bisher verhängten Bußgelder waren vergleichsweise gering. Im Jahr 2011 verhängten Datenschutzbehörden von sieben Bundesländern insgesamt nur 66 Bußgelder i. H. v. insgesamt etwa 200.000 Euro.[761]

Im Vergleich sieht die DSGVO erheblich schärfere Geldbußen vor: Gem. Art. 83 Abs. 4 können Geldbußen i. H. v. 20 Millionen Euro oder für Unternehmen sogar i. H. v. 4 % des weltweiten Jahresumsatzes verhängt werden – und zwar des Mutterkonzerns und nicht etwa gewisser Tochterunternehmen.[762] Im Fall von *Facebook* wären das bei dem Jahresumsatz im Jahr 2016 von etwa 27 Mrd.[763] Bußgelder in Höhe von 1,08 Mrd. Im BDSG-neu finden sich die Bestimmungen in §§ 41 f. Insbesondere sieht § 42 BDSG-neu zusätzlich Strafvorschriften vor.

Es ist gerade die starke Erweiterung des möglichen Bußgeldrahmens, die dem Datenschutzrecht zu einer besseren Durchsetzbarkeit verhelfen kann.

3. Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung ist nicht ein Mittel zur Durchsetzbarkeit des Datenschutzrechts im klassischen Sinne, sondern viel mehr eine Präventionsmaßnahme zum Schutz gegen Datenschutzverstöße. Faktisch stellt sie jedoch ein weiteres Instrument dar, um die Einhaltung der Vorgaben der DSGVO sicherzustellen und dient der Durchsetzbarkeit damit mindestens im faktischen Sinne.

Gem. Art. 35 Abs. 1 DSGVO muss ein Verantwortlicher bei einer Form der Verarbeitung, die „[…] voraussichtlich ein hohes Risiko […]“ birgt, Art. 35 Abs. 1 S. 1 DSGVO, eine Abschätzung der Folgen dieser Datenverarbeitung für den Datenschutz durchführen. Art. 35 Abs. 3 DSGVO zählt

---

761 *Ashkar*, DuD 2015, 796, 797 m. w. N.

762 *Dietrich*, ZD 2016, 260, 264; *Faust/Spittka/Wybitul*, ZD 2016, 120, 120 f.; weiterführend zu Art. 83 DGSVO vgl. *Bergt*, DuD 2017, 555, 556 ff.

763 *Facebook Inc.,* Facebook Reports Fourth Quarter and Full Year 2016 Results, abrufbar unter https://investor.fb.com/investor-news/press-release-details/2017/facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results/default.aspx (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

nicht-abschließend Fälle einer solch risikobehafteten Datenverarbeitung auf: Für die Verarbeitung in sozialen Netzwerken ist besonders Art. 35 Abs. 2 lit. a DSGVO von Interesse, der als einen die Datenschutz-Folgenabschätzung auslösenden Fall die „[…] systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen […]" nennt; die Datenverarbeitung durch die Betreiber sozialer Netzwerke wird zumeist hierunter fallen. Darüber hinaus können auch die Aufsichtsbehörden eine Liste mit Verarbeitungen, bei denen eine Datenschutz-Folgenabschätzung erforderlich ist, erstellen, Art. 35 Abs. 4 DSGVO.

Der Mindestinhalt der Datenschutz-Folgenabschätzung ist schließlich in Art. 35 Abs. 7 DSGVO geregelt. So muss sie eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der Notwendigkeit sowie ihrer Risiken und sogleich Abhilfemaßnahmen für diese Risiken enthalten. Gem. Art. 36 Abs. 1 DSGVO muss der Verantwortliche ferner die Aufsichtsbehörde konsultieren, wenn er aufgrund der Datenschutz-Folgenabschätzung zu dem Ergebnis kommt, dass die geplante Datenverarbeitung besonders risikoreich für den Schutz personenbezogener Daten ist.

Die Datenschutz-Folgenabschätzung ist der Meldepflicht aus § 4d Abs. 5 BDSG ähnlich, wobei die Datenschutz-Folgenabschätzung inhaltlich weiter reicht und, anders als § 4d Abs. 5 BDSG, nicht in selbem Maße durch tatbestandliche Ausnahmen, wie etwa durch die Einwilligung des Betroffenen, ausgeschlossen ist.[764] Die Meldepflicht aus § 4d Abs. 5 BDSG entfaltete in der Praxis demnach kaum Relevanz.[765] Die Datenschutz-Folgenabschätzung könnte sich demgegenüber durchaus als wertvolles Mittel für den Datenschutz erweisen. Aus Betroffenensicht stellt sie grundsätzlich ein erfreuliches Instrument zur Prävention von Datenschutzverstößen dar. Allerdings sind die Vorgaben zur Erforderlichkeit einer Datenschutz-Folgenabschätzung, trotz der in Art. 35 Abs. 2 DSGVO enthaltenen Regelbeispiele, unpräzise. Aus Verantwortlichensicht dürften diese unpräzisen Vorgaben für Unsicherheit sorgen, insbesondere mit Blick auf die Möglichkeit der Sanktionierung[766] von Verstößen gegen die Vorgaben der Art. 35 f. DSGVO gem. Art. 84 Abs. 4 lit. a DSGVO mit Geldbußen in Höhe von bis zu 10 Mio. Euro oder bis zu 2 % des Jahresgesamtumsatzes.[767]

764 *Nolte/Werkmeister*, in: Gola, DSGVO, Art. 35, Rn. 5 ff.
765 *Martini*, in: Paal/Pauly, DSGVO, Art. 35, Rn. 74.
766 Vgl. bereits Kap. 3 Pkt. D.II.2, S. 230.
767 *Laue/Nink/Kremer,* Das neue Datenschutzrecht in der betrieblichen Praxis, S. 235.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Es ist durchaus denkbar, dass die Datenschutz-Folgenabschätzung dazu beiträgt, Datenschutzverstöße zu minimieren, indem sie Verantwortliche dazu verpflichtet, sich vor Durchführung der Verarbeitung mit der geplanten Verarbeitung auseinander zu setzen. Betroffene können damit insbesondere davor geschützt werden, dass Verantwortliche neue Technologien so lange austesten, bis Aufsichtsbehörden die Gelegenheit haben, darauf zu reagieren. Die Kehrseite der Medaille ist allerdings, dass dieses Instrument – insbesondere mit Blick auf die ungenauen Voraussetzungen der Norm – eine potentielle Bremswirkung auf den technologischen Fortschritt im Bereich der Datenverarbeitung haben könnte.

4. Zivilrechtliche Durchsetzung

a) Durchsetzung im nationalen Recht

Den Betroffenen stehen auch Ansprüche zur zivilrechtlichen Durchsetzung offen. Neben dem Unterlassungsanspruch aus § 1004 BGB sehen das BDSG sowie das BGB Schadensersatzmöglichkeiten für den Betroffenen vor. § 7 BDSG enthält eine Schadensersatzregelung im Falle des unzulässigen Umgangs mit personenbezogenen Daten. Gem. § 7 S. 2 BDSG kann sich der Verantwortliche exkulpieren, wenn ihm der Nachweis gelingt,[768] dass er die gebotene Sorgfalt im Umgang mit den personenbezogenen Daten beachtet hat. Im Gegensatz zu § 8 Abs. 2 BDSG, der nur auf öffentliche Stellen anwendbar ist, trifft § 7 BDSG keine Aussage zur Ersatzfähigkeit immaterieller Schäden. Daraus wird überwiegend geschlossen, dass § 7 BDSG nur auf materielle Schäden anwendbar ist.[769] Immaterielle Schäden sind aber unter Umständen über § 823 Abs. 1, 2 BGB i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG ersatzfähig. Zwar sieht § 253 Abs. 1 BGB die Ersatzfähigkeit immaterieller Schäden nur in den gesetzlich benannten Fällen vor. In § 253 Abs. 2 BGB ist das allgemeine Persönlichkeitsrecht jedoch nicht als ein solcher Fall benannt. Gleichwohl ist inzwischen anerkannt, dass bei schwerwiegenden Verletzungen des allgemeinen Persönlichkeitsrechts

768 Zu dieser Beweislastumkehr vgl. *Eßer*, in: Auernhammer, BDSG, § 7, Rn. 4.

769 *Simitis*, in: Simitis, BDSG, § 7, Rn. 32; *Däubler*, in: DKWW, BDSG, § 7, Rn. 19; *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 7, Rn. 12; *Quaas*, in: BeckOK DatenschutzR, BDSG, § 7, Rn. 55; *Eßer*, in: Auernhammer, BDSG, § 7, Rn. 5; a. A. *Bergmann/Möhrle/Herb,* BDSG, § 7, Rn. 12.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

auch ein Anspruch auf Geldentschädigung zusteht.[770] Allerdings muss der Betroffene hier das Verschulden des Datenverarbeiters nachweisen.[771] Damit erweist sich die Durchsetzung eines Schadensersatzanspruches für den Betroffenen als schwierig.

b) Durchsetzung in der DSGVO

Die DSGVO gibt dem Betroffenen eine Reihe von Ansprüchen an die Hand, die seine Position im Vergleich zur bisherigen Rechtslage stärken könnten. So sieht Art. 82 DSGVO eine Schadensersatzregelung vor und zwar nun explizit auch für immaterielle Schäden. Gem. Art. 82 Abs. 3 DSGVO kann sich der Verantwortliche durch den Nachweis, dass er für den eingetretenen Schaden nicht verantwortlich ist, exkulpieren. Der Schadensersatzspruch ist gem. EG 146 S. 4 DSGVO neben anderen Schadensersatzansprüchen, insbesondere also auch neben dem Ersatzanspruch aus § 823 Abs. 1, 2 i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG anwendbar. Der Schadensbegriff ist nach EG 146 S. 3 DSGVO weit auszulegen; die Norm soll einen „vollständigen und wirksamen Schadensersatz" gewährleisten, EG 146 S. 5 DSGVO.

Zudem sieht Art. 79 Abs. 1 DSGVO das Recht auf einen weiteren „wirksamen gerichtlichen Rechtsbehelf"[772] vor, wenn der Betroffene „[…] der Ansicht ist […]", dass seine aus der DSGVO gewährten Rechte durch eine nicht im Einklang mit der DSGVO stehende Verarbeitung verletzt wurden. Art. 79 DSGVO hält hierbei die nationalen Gesetzgeber an, entsprechende Rechtsbehelfe zu stellen.[773]

Art. 80 DSGVO sieht schließlich die Vertretung des Betroffenen durch Einrichtungen, Organisationen o. ä. vor. Art. 80 Abs. 2 DSGVO enthält eine Öffnungsklausel für die Mitgliedstaaten, nach der nationale Gesetzgeber Regelungen erlassen können, die den Einrichtungen o. ä. i. S. d. Art. 80 Abs. 1 DSGVO ein Klagerecht hinsichtlich der Rechte aus Art. 77 – 79

770 *BGH,* Urt. v. 15.11.1994, Az. VI ZR 56/94, BGHZ 128, 1, 12 f. – Caroline von Monaco; *BGH,* Urt. v. 17.12.2013, Az. VI ZR 211/12, BGHZ 199, 237, 256 f., Rn. 38 – Geldentschädigung wegen Internetveröffentlichung; *OLG Frankfurt a. M.,* Urt. v. 21.01.1987, Az. 21 U 164/86, NJW 1987, 1087, 1088; *OLG Köln,* Urt. v. 13.10.1988, Az. 18 U 37/88, NJW 1989, 720, 720 f.; *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 7, Rn. 19; *Simitis*, in. Simitis, BDSG, § 7, Rn. 33.

771 *Quaas*, in: BeckOK DatenschutzR, BDSG, § 7, Rn. 56 f.

772 Terminologisch wird im Folgenden der Begriff „Rechtsbehelf" i. S. d. Art. 79 DSGVO übernommen.

773 *Martini*, in: Paal/Pauly, DSGVO, Art. 79, Rn. 33; das wohl voraussetzend *Bergt*, in: Kühling/Buchner, Art. 79, Rn. 19 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

DSGVO (aber nicht des Rechts aus Art. 82 DSGVO, EG 142 DSGVO) ohne Beauftragung des Betroffenen gibt.[774] Im deutschen Recht gibt es seit dem 24. Februar 2016 mit § 2 UKlaG ein Recht, das diesen Spielraum teilweise ausfüllt.[775]

c) Änderungen hinsichtlich der gerichtlichen Zuständigkeit

Art. 79 Abs. 2 DSGVO enthält Vorgaben über die Zuständigkeit des Gerichts, die gem. Art. 82 Abs. 6 DSGVO auch auf Art. 82 DSGVO anwendbar sind. Grundsätzlich sind die Gerichte des Mitgliedstaates, in dem der Verantwortliche seine Niederlassung hat, anzurufen. Allerdings kann der Betroffene gem. Art. 79 Abs. 2 S. 2 DSGVO auch die Gerichte des Mitgliedstaates, in dem er selbst seinen Aufenthaltsort hat, anrufen, es sei denn, der Verantwortliche ist eine Behörde. Art. 79 Abs. 2 DSGVO ist lex specialis zu anderen Zuständigkeitsregelungen, insbesondere zu der EuGVVO, vgl. EG 147 DSGVO.[776]

Die Norm scheint jedoch nur die Fälle zu regeln, in denen der Betroffene gegen ein Unternehmen vorgeht. Das regelt die Norm zwar nicht ausdrücklich, erschließt sich jedoch aus der Formulierung des Art. 79 Abs. 1 DSGVO, der von der Niederlassung des Verantwortlichen einerseits und vom Aufenthaltsort[777] des Betroffenen andererseits spricht. Sachverhalte, in denen sich zwei natürliche Personen gegenüberstehen, regelt Art. 79 DSGVO demgegenüber nicht. Für sie ist daher weiterhin auf die allgemeinen Regelungen, insbesondere also die der EuGVVO, zurückzugreifen.

Die Regelung des Art. 79 Abs. 2 DSGVO könnte jedenfalls die Durchsetzung der Rechte von Betroffenen gegenüber Unternehmen erleichtern. Dies macht ein Rechtsstreit, der von dem österreichischen *OGH* inzwischen dem *EuGH* vorgelegt wurde,[778] deutlich: Der Datenschützer *Max Schrems*, der auch das Verfahren, das schließlich zur Ungültigkeit der Safe Harbor-

774 Ausführlich zur Öffnungsklausel *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 271 ff.

775 *Bergt*, in: Kühling/Buchner, DSGVO, Art. 78, Rn. 18 f.; kritisch *Schulz*, ZD 2014, 510, 512 ff.

776 *Bergt*, in: Kühling/Buchner, DSGVO, Art. 79, Rn. 15.

777 Der Begriff des „Aufenthaltsortes" ist in der DSGVO nicht näher definiert. Gemeint ist wohl der „gewöhnliche Aufenthaltsort", vgl. *Martini*, in: Paal/Pauly, DSGVO, Art. 79, Rn. 26 ff.

778 *OGH,* Beschl. v. 20.07.2016, Az. 6 Ob 23/16z, ZD 2017, 29.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Entscheidung führte,[779] in die Wege geleitet hatte, klagte vor österreichischen Gerichten auf Basis des Gerichtsstandes für Verbraucherregelungen i. S. d. Art. 16 Abs. 1 Alt. 2 EuGVVO a. F.[780] gegen *Facebook*. Aufgrund des Bekanntheitsgrades und Ausmaßes der datenschutzrechtlichen Aktivitäten, die *Schrems* zwischenzeitlich erreicht hatte, erhob *Facebook* u. a. die Einrede der fehlenden internationalen Zuständigkeit: *Schrems* fehle die Verbrauchereigenschaft.[781] Solchen Einwänden könnte die Regelung der gerichtlichen Zuständigkeit in Art. 79 Abs. 2 DSGVO künftig vorbeugen. Dies gilt insbesondere, wenn die Klage von erfahrenen Datenschützern in die Wege geleitet wird.

III. Zusammenfassung

Die Betroffenenrechte der DSGVO weisen viele Parallelen zu den Betroffenenrechten unter dem Regime der BDSG bzw. der DSRL auf. Grundlegend neu ist hingegen z. B. das Recht auf Datenübertragbarkeit, das den Nutzern den Anbieterwechsel erleichtern soll und ursprünglich gerade auf den Wechsel von einem sozialen Netzwerk zu einem anderen zugeschnitten war. Allerdings darf das Recht auf Datenübertragbarkeit sich nur auf die personenbezogenen Daten desjenigen, der das Recht in Anspruch nimmt, beziehen und nicht zu einem Zulässigkeitstatbestand für die Übertragung personenbezogener Daten anderer Personen ausgeweitet werden. Damit ist seine Wirksamkeit jedoch begrenzt, da soziale Netzwerke gerade von der Interaktion von Nutzern leben und die Datenverarbeitung oft die personenbezogenen Daten mehrerer Personen betreffen. Das BDSG-neu beschränkt die Betroffenenrechte der DSGVO teilweise aufgrund der in der DSGVO enthaltenen Öffnungsklausel des Art. 23 Abs. 1. Nachdem ursprünglich weitreichende Beschränkungen geplant waren, sind diese nun – für den vorliegend untersuchten Bereich – praktisch weniger relevant geworden.

Die DSGVO sieht mit der Datenschutz-Folgenabschätzung ein Instrument vor, das Datenschutzverstößen vorbeugen soll. Angesichts drohender

779 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems; *Kühling/Heberlein*, NVwZ 2016, 7; vgl. Kap. 4 Pkt. C, S. 276.

780 Verordnung (EG) Nr. 44/2001 des Rates vom 22. Dezember 2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, ABL.EG 2001 L 12, 1.

781 *OGH,* Beschl. v. 20.07.2016, Az. 6 Ob 23/16z, ZD 2017, 29; zur Anwendbarkeit der Regelungen für Verbrauchersachen in der EuGVVO bei *Facebook* vgl. *Dietrich*, ZD 2016, 260, 261 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Sanktionen ist es wahrscheinlich, dass die Verantwortlichen dieser Vorgabe Folge leisten werden und so gehalten sind, bereits im Vorfeld geplante Verarbeitungen zu analysieren. Während die Betroffenen davon durchaus profitieren können, besteht angesichts der recht unkonkreten Vorgaben der Norm die Gefahr, dass dadurch technologischer Fortschritt im Bereich der Datenverarbeitung behindert wird.

Für eine bessere Durchsetzbarkeit des Datenschutzes sieht die DSGVO die Möglichkeit der Verhängung empfindlicher Geldbußen vor. Sie können ein kraftvolles Mittel zur Durchsetzung der datenschutzrechtlichen Vorgaben der DSGVO darstellen, falls sie effektiv verhängt werden.

Sowohl nach der DSRL als auch nach der DSGVO hat der Betroffene das Recht, sich hierfür an die Aufsichtsbehörden seines Mitgliedstaates mit einer Beschwerde zu wenden. Anders als noch unter der DSRL sieht die DSGVO für diese Fälle der grenzüberschreitenden Sachverhalte ein austariertes System der Zusammenarbeit vor. Dieses System erlaubt die gemeinsame Durchsetzung von Maßnahmen gegen den Verantwortlichen und beschränkt sich nicht mehr alleine auf Verweisungen an andere Aufsichtsbehörden. Dadurch können die Rechte der Betroffenen gestärkt werden, da das System dazu beitragen kann, Maßnahmen effektiver durchzusetzen. Die Vorgaben der DSGVO über die Zusammenarbeit und das Kohärenzverfahren sind ein wichtiger Schritt zur besseren Durchsetzbarkeit des Datenschutzrechts – die Erprobung dieser Mechanismen in der Praxis darf mit Spannung erwartet werden.

In zivilrechtlicher Hinsicht ist vor allem die ausdrückliche Ersatzfähigkeit immaterieller Schäden aus Art. 82 Abs. 1 DSGVO erfreulich. Zwar konnte bei schwerwiegenden Beeinträchtigungen des allgemeinen Persönlichkeitsrechts im deutschen Recht schon bisher Ersatz für immaterielle Schäden gefordert werden, allerdings war die Haftung hierfür verschuldensabhängig, wofür der Betroffene die Beweislast trug. Demgegenüber sieht Art. 82 Abs. 3 DSGVO eine Beweislastumkehr vor.

Auch die Änderungen zur internationalen Zuständigkeit von Gerichten aus Art. 79 Abs. 2 DSGVO können dabei helfen, die Rechte der Betroffenen wirksam gegen Unternehmen durchzusetzen, indem sie sich an die Gerichte ihres Mitgliedstaates wenden können. Zwar sieht die EuGVVO für Verbrauchersachen diese Möglichkeit bereits vor. Die Praxis zeigt jedoch, dass dieser Gerichtsstand allzu leicht in Frage gestellt werden kann.

Diese Reihe an Veränderungen ist geeignet, die Durchsetzbarkeit des Datenschutzrechts zur bestehenden Rechtslage deutlich zu verbessern.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kapitel 4: Rechtsvergleich mit den USA vor dem Hintergrund des Datentransfers in die USA

> „Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual […] the right "to be let alone"".[782] (*Warren/Brandeis*, 1890)

Der Artikel „The Right to Privacy" von *Warren/Brandeis* aus dem Jahr 1890 wird als Ursprung der Idee des Datenschutzes in den USA begriffen.[783] Angesichts neuer Technologien und Geschäftsmodelle – insbesondere tragbare Fotoapparate und das Aufkommen von Papparazzi – argumentieren die Autoren, dass es ein Recht geben müsse „in Ruhe gelassen zu werden" („right to be let alone"). Diese Idee eines „right to privacy", das sich nicht aus vertraglichen Absprachen ergebe, sondern absolut wirkt, fand später Eingang in die Rechtsprechung des *Supreme Court*, als *Brandeis* dort Richter wurde.[784]

Obwohl damit in den USA datenschutzrechtliche Problemstellungen die juristische Debatte ebenfalls schon seit Langem durchdringen, lassen sich in den USA, insbesondere bei Internet-Sachverhalten, entscheidende Unterschiede zum europäischen Datenschutzverständnis beobachten. So wird das Recht auf informationelle Selbstbestimmung in den USA diskutiert, seine Existenz ist jedoch umstritten.[785] Das hat zur Folge, dass staatliche datenschützende Maßnahmen verfassungsrechtlich rechtfertigungsbedürftig sind – insbesondere am Maßstab des ersten Amendments –, den Verfassungsgütern bei einer Interessenabwägung jedoch kein Recht auf Datenschutz mit Verfassungsrang gegenübersteht. Einfachgesetzlich verfolgen die USA zudem einen vom europäischen Datenschutzverständnis grundlegend abweichenden Ansatz: Statt eines Verbots mit Erlaubnisvorbehalts ist in den USA

782 *Warren/Brandeis*, 4 Harv. L. Rev. 193 (1890).
783 Vgl. etwa Ausführungen bei Hall v. Post, 323 N.C. 259, 262 f.
784 Vgl. Kap. 4 Pkt. A.II, S. 243.
785 Vgl. Kap. 4 Pkt. A.I, S. 239.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

jeder Umgang mit personenbezogenen Daten erlaubt, sofern er nicht verboten ist.[786] Nach Aufstreben des Internets wurde ein Ansatz der Selbstregulierung vertreten, um das Wachstum nicht einzudämmen.[787]

Dieses Kapitel wird diese Unterschiede näher anhand der in Kapitel 3 analysierten Problemfelder beleuchten. Die USA sind Heimat der Mehrzahl der in Deutschland und der Europäischen Union genutzten größten sozialen Netzwerke[788] und spielen daher eine besondere Rolle im internationalen Datenverkehr zwischen der EU und Drittstaaten. Dies wird insbesondere vor dem Hintergrund des Transfers von personenbezogenen Daten von der EU in die USA relevant, da große soziale Netzwerke wie *Facebook*[789] oder *Snapchat*[790] die personenbezogenen Daten ihrer Nutzer in die USA übermitteln. Nach europäischer Konzeption dürfen personenbezogene Daten jedoch nur in Drittländer mit einem angemessenen Schutzniveau übermittelt werden, Art. 25 Abs. 1 DSRL bzw. Art. 45 Abs. 1 DSGVO. Dieses Kapitel wird die Voraussetzungen des Datentransfers in Drittländer und insbesondere die für den Transfer in die USA geschaffene „Sonderlösung" des EU-U.S.-Privacy Shield[791] im Lichte der *Schrems*-Entscheidung des *EuGH*[792] analysieren.

Zu diesem Zweck wird im Folgenden zunächst das verfassungsrechtliche (dazu A.) wie einfachgesetzliche (dazu B.) US-Bundesrecht mit Blick auf den Datenschutz im Social Web analysiert. Darauf aufbauend wird anschließend der Datenfluss von der EU in die USA diskutiert (dazu C.).

---

786 Ausführlich *Klar/Kühling*, AöR 2016, 165, 180 f.

787 *Eko*, 6 Comm. L. & Pol'y 445, 450 f.; *Clinton/Gore*, Framework for Global Electronic Commerce, abrufbar unter https://clinton4.nara.gov/WH/New/Commerce/read.html (abgerufen am 13.10.2017): „For [the internet's] […] to be realized fully, governments must adopt a non-regulatory, market-oriented approach […]".

788 Vgl. etwa *Facebook* mit 2,01 Mrd. monatlich aktiven Nutzern mit Hauptsitz in Kalifornien, *Facebook Inc.,* Company Info, abrufbar unter http://newsroom.fb.com/company-info/ (abgerufen am 13.10.2017).

789 Vgl. *Facebook Inc.,* Facebook Inc. and the EU-U.S. Privacy Shield, abrufbar unter https://www.facebook.com/about/privacyshield (abgerufen am 13.10.2017).

790 Vgl. *Snap Inc.,* Datenschutzbestimmungen, abrufbar unter https://www.snap.com/de-DE/privacy/privacy-policy (abgerufen am 13.10.2017).

791 Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes, C(2016) 4176, ABl.EU 2016 L 207, 1.

792 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

A. Verfassungsrechtliche Grundlagen

Zunächst werden die verfassungsrechtlichen Grundlagen des Schutzes personenbezogener Daten in den USA dargestellt. Zwar gelten die Grundrechte – die Bill of Rights, d. h. die ersten zehn Zusatzartikel der US-amerikanischen Verfassung (sog. Amendments) – nur im Verhältnis zwischen Staat und Bürger. Die US-amerikanische Verfassung kennt, mit wenigen Ausnahmen,[793] weder eine mittelbare noch eine unmittelbare Drittwirkung von Grundrechten. Gleichwohl soll eine Darstellung der verfassungsrechtlichen Grundlagen und der entsprechenden höchstrichterlichen Rechtsprechung dazu dienen, einen Überblick über die Stellung des Datenschutzes in den USA zu geben, da sich die aufzuzeigenden verfassungsrechtlichen Erwägungen in der Interpretation der vorliegend relevanten einfachgesetzlichen und gewohnheitsrechtlichen Ansprüche niederschlagen.

I. Das right to privacy und right to information privacy

1. Entwicklung des right to privacy

Obwohl die Verfassung der USA kein ausdrückliches right to privacy kennt, wurde durch richterliche Rechtsfortbildung ein solches Recht inzwischen als „fundamental right", also Grundrecht, anerkannt.[794] Es umfasst den Schutz des Einzelnen vor Eingriffen und auf Selbstbestimmung in Fragen, die grundsätzlich als besonders privat eingestuft werden, und wird etwa im

793 Wenn Private eine öffentliche Funktion ausüben oder wenn der Staat ein verfassungswidriges Verhalten gefördert hat, können daraus Ansprüche gegen Private aus der Verfassung erwachsen. Beispielhaft kann auf den Fall *Marsh v. State of Alabama* hingewiesen werden, Marsh v. State of Alabama, 326 U.S. 501 (1946), in dem eine gänzlich in Privateigentum stehende Stadt dennoch an den ersten Verfassungszusatz gebunden war. Allerdings sind Reichweite und Grenzen dieser Ausnahme bis heute nicht geklärt, vgl. *Chemerinsky,* Constitutional Law, Kap. 3 Pkt. C, S. 548 ff. m. w. N.

794 Vgl. Griswold v. Connecticut, 381 U.S. 479, 485 f. (1965).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kontext von Fällen zum Schwangerschaftsabbruch[795], dem Recht auf sexuelle Selbstbestimmung[796], aber auch bei der Beihilfe zur Selbsttötung[797] diskutiert.

Im Fall *Griswold*[798] aus dem Jahr 1965 urteilte der *Supreme Court* zum ersten Mal, dass sich aus der Verfassung ein right to privacy ergibt:

> „[…] specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. […] Various guarantees create zones of privacy."[799]

Über die Herleitung dieses Rechts bestand zwischen den Richtern indes Uneinigkeit. Nach der Mehrheitsentscheidung der *Griswold*-Entscheidung ist das right to privacy Ausfluss gewisser Rechte aus der Bill of Rights, im speziellen des ersten, dritten, vierten, fünften und neunten Amendments.[800] Andere Richter verorteten das right to privacy in ihren übereinstimmenden Anmerkungen zu der Entscheidung (sog. „concurring opinions") im neunten Amendment[801],[802] oder in der „substantive due process clause" des fünften und vierzehnten Amendments[803]. Die substantive due process clause sichert ein Recht auf ein faires Verfahren in materiell-rechtlicher Sicht[804] und schützt bestimmte persönliche Freiheiten des Einzelnen vor dem Eingriff des Bundes sowie der Staaten.[805] In folgenden Fällen wurde das right to

---

795 Vgl. Maher v. Roe, 432 U.S. 464 (1977); Webster v. Reproductive Health Services et al., 492 U.S. 490 (1989); Planned Parenthood v. Casey, 505 U.S. 833 (1992).

796 Vgl. Bowers v. Hardwick, 478 U.S. 186 (1986); Lawrence v. Texas, 539 U.S. 558 (2003).

797 Vgl. Washington v. Glucksberg, 521 U.S. 702 (1997); Vacco v. Quill, 521 U.S. 793 (1997).

798 Griswold v. Connecticut, 381 U.S. 479 (1965).

799 Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

800 Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

801 „The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

802 *Justice Goldberg*, übereinstimmende Meinung zum Fall Griswold v. Connecticut, 381 U.S. 479, 486 f. (1965).

803 *Justice Harlan*, übereinstimmende Meinung zum Fall Griswold v. Connecticut, 381 U.S. 479, 500 (1965).

804 Vgl. abweichende Meinung von *Justice Brandeis* im Fall New State Ice Co.: „(…) the due process clause has been held by the Court applicable to matters of substantive law as well as to matters of procedure.", New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932).

805 Vgl. Bolling v. Sharpe, 347 U.S. 497, 499 f. (1954); Aptheker v. Secretary of State, 378 U.S. 500, 505 ff. (1964); Kent v. Dulles, 357 U.S. 116, 125 f. (1958).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

privacy ebenso auf die substantive due process clause gestützt.[806] Allerdings sind gerade im Zusammenhang mit technologischem Fortschritt Fälle im Rahmen des vierten und fünften Amendment von großer Bedeutung.[807]

2. Das right to information privacy

Teilweise wird das „right to privacy" vom „right to information privacy" unterschieden. Die Unterscheidung zum „right to privacy" wurde erstmals im Jahr 1977 vom *Supreme Court* in der Entscheidung *Whalen v. Roe*[808] getroffen. Das right to information privacy meint nach dieser Entscheidung das Recht, private Angelegenheiten nicht offenlegen zu müssen.[809] Das right to information privacy ist also mit dem Recht auf informationelle Selbstbestimmung vergleichbar, seine Reichweite ist jedoch bislang noch ungeklärt. So ist bereits die Existenz eines right to information privacy umstritten: In mehr als vier Jahrzehnten seit *Whalen* wurden nur zwei weitere Fälle zum right to information privacy vor dem *Supreme Court* verhandelt.[810] Dabei kann festgestellt werden, dass im ersten Fall das right to information privacy hauptsächlich im Lichte des vierten und fünften Amendments diskutiert wurde und mit dem Informationsinteresse der Öffentlichkeit abgewogen wurde, wobei das Informationsinteresse der Öffentlichkeit als überwiegend angesehen wurde.[811] Im Jahr 2011 äußerte sich der *Supreme Court* im zweiten Fall zweifelnd gegenüber der Existenz eines right to information privacy: Der *Supreme Court* ging in dieser Entscheidung zwar von einem right to information privacy aus, drückte jedoch zugleich

806 Vgl. etwa Roe v. Wade, 410 U.S. 113 (1973); Lawrence v. Texas, 539 U.S. 558 (2003); Whalen v. Roe, 429 U.S. 589 (1977).
807 Vgl. Kap. 4 Pkt. A.II, S. 243.
808 Whalen v. Roe, 429 U.S. 589 (1977).
809 Whalen v. Roe, 429 U.S. 589, 598 f. (1977).
810 Nixon v. Administrator of General Services, 433 U.S. 425 (1977); NASA v. Nelson, 562 U.S. 134 (2011).
811 Der *Supreme Court* befasste sich mit der Frage, ob der ehemalige US-Präsident Nixon gewisse Unterlagen und Aufnahmen, die in seiner Funktion als Präsident angefertigt wurden, zur Archivierung an den Staat übergeben müsse. Das Gericht urteilte, dass das Interesse der Öffentlichkeit die Privatheitserwartung des ehemaligen Präsidenten überwiege, Nixon v. Administrator of General Services, 433 U.S. 425, 457 f. (1977).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

aus, dass die Entscheidung keine Aussage über das Bestehen eines solchen Rechts treffen sollte:

> „We assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*."[812]

Diese Formulierung wurde jedoch von Richtern des *Supreme Courts* selbst stark dahingehend kritisiert, dass der *Supreme Court* stattdessen hätte feststellen müssen, dass sich aus der Verfassung kein right to information privacy ergebe.[813] Der Einfluss dieser Entscheidung auf die Rechtsprechung anderer Gerichte ist dementsprechend als gering einzustufen. In knapp sechs Jahren seit der Entscheidung wurde der Fall in der Rechtsprechung nur etwa in 160 Fällen[814] zitiert, wovon sich nur wenige dezidiert mit der Entscheidung auseinandersetzten. Dabei wurde in fast allen Fällen nur die Feststellung getroffen, dass eine Entscheidung über das Bestehen des Rechts nicht getroffen wurde.[815] Nur in etwa einem duzend Fällen wurde die Aussage des *Supreme Courts* derart ausgelegt, dass ein right to information privacy bestehe.[816]

Zusammenfassend ist festzustellen, dass die USA ein Recht auf informationelle Selbstbestimmung mit einer Reichweite im deutschen bzw. europäischen Sinne nicht kennen. Zwar wird ein right to information privacy diskutiert, sein Schutzbereich ist ebenso wie seine Existenz jedoch unklar.

---

812 NASA v. Nelson, 562 U.S. 134, 138 (2011); ausführlich zum reasonable expectation of privacy-Test vgl. Kap. 4 Pkt. A.II.1.b, S. 245.

813 So äußerte *Justice Scalia* in seiner übereinstimmenden Meinung: „Courts should not use the Due Process Clause as putty to fill up gaps they deem unsightly in the protections provided by other constitutional provisions. In sum, I would simply hold that there is no constitutional right to "informational privacy. […] [The Court] states that it will "assume, without deciding" that there exists a right to informational privacy. […] The Court's sole justification for its decision to "assume, without deciding" is that the Court made the same mistake before — in two 33–year–old cases, *Whalen* […] and *Nixon […]*. […] *Whalen* and *Nixon* created an uncertainty that the text of the Constitution did not contain and that today's opinion perpetuates", NASA v. Nelson, 562 U.S. 134, 162 f. (2011).

814 Ergebnis der Suchen in den Datenbanken *Westlaw* und *LexisNexis* (Stand: 13.10.2017.)

815 Ismail v. Fulkerson, NO. SA CV 10-00901-VBF-AJW, 2014 WL 3962488, 13 f. (C.D. Cal, August 12, 2014); O'Neill v. Bannister, No. 3:12-cv-00030-LRH, 2012 WL 6968937, 9 (D. Nev., August 29, 2012).

816 Exemplarisch Warner v. Township of South Harrison, 885 F.Supp.2d 725, 739 (D.N.J. 2012); Reproductive Health Services v. Strange, 204 F. Supp. 3d 1300, 1335 f. (M.D. Ala. 2016); Lavender v. Koenig, No. C.A. No. 13-2042-LPS, 2015 U.S. Dist. LEXIS 34141 (D. Del., March 19, 2015).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

II. Das vierte Amendment

> „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated (…)."

Das vierte Amendment schützt das Recht der Bürger auf Sicherheit ihrer Person, Wohnung, Urkunden und des Eigentums gegen willkürliche Durchsuchung oder Beschlagnahmung. Das vierte Amendment spielt für den Datenschutz in den USA eine große Rolle, sodass es für das Verständnis der Entwicklung des US-amerikanischen Datenschutzes unerlässlich ist, ein besonderes Augenmerk auf das vierte Amendment zu legen. So wurde sein Schutzbereich im Lichte technologischen Fortschritts stets neu diskutiert und durch höchstrichterliche Rechtsprechung konkretisiert. Im Zuge dieser Rechtsprechung hat sich für das vierte Amendment eine eigene Dogmatik entwickelt, deren Grundgedanken auch bei der Interpretation der einfachgesetzlichen Grundlagen herangezogen werden.

Damit das Amendment anwendbar ist, muss eine Durchsuchung oder Beschlagnahmung („searches or seizures") stattgefunden haben (dazu 1.). Ferner müsste diese Durchsuchung oder Beschlagnahmung auch willkürlich („unreasonable") gewesen sein (dazu 2.).

1. Durchsuchung oder Beschlagnahme

Für die Anwendbarkeit des vierten Amendments stellt sich die Frage, wann staatliches Handeln als Durchsuchung oder Beschlagnahmung zu qualifizieren ist.

a) Schutzobjekt des vierten Amendments

Zunächst wurde das vierte Amendment in Bezug auf moderne Technologien restriktiv ausgelegt. Als Schutzobjekt des vierten Amendments wurden nur bestimmte Orte und Dinge anerkannt. So entschied in den 1920er Jahren der *Supreme Court* im Fall *Olmstead v. United States*[817], dass das Abhören des Heimtelefons eines Verdächtigen mangels Durchsuchung oder Beschlagnahmung keine Verletzung des vierten Amendments darstellt, da ein

817 Olmstead v. United States, 277 U.S. 438 (1928).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Telefon nicht vergleichbar mit einem Brief sei.[818] Justice *Brandeis*, der bereits 40 Jahre zuvor den Artikel "The Right to Privacy"[819] mitverfasste, schrieb hierzu eine abweichende Meinung (sog „dissenting opinion"). Er griff erneut die Idee des „right to be let alone" auf und leitete es aus dem vierten Amendment ab: Jedes Eindringen des Staates in die Privatsphäre des Bürgers sei eine Verletzung des vierten Amendments, unabhängig von den angewendeten Mitteln.[820] Die *Olmstead*-Entscheidung wurde schließlich in dem für das „right to privacy" wegweisenden Urteil *Katz v. United States*[821] revidiert. In diesem Fall wurden dem Gericht die Fragen vorgelegt, ob auch eine öffentliche Telefonzelle ein geschützter Ort nach dem vierten Amendment sein kann und ob zum Vorliegen einer Durchsuchung ein physisches Eindringen in das Schutzobjekt nötig ist. Der *Supreme Court* stellte klar, dass es bei der Anwendbarkeit des vierten Amendment nicht Orte schütze. Stattdessen nahm die Entscheidung die Gedanken der über 40 Jahre zuvor geschriebenen abweichenden Meinung von Justice Brandeis im Fall *Olmstead* auf:

> „[…] this effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. […] But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[822]

Im Vergleich zu *Olmstead* wechselte das Gericht also die Perspektive: Es ging nun nicht mehr um die Frage, wo der potentielle Eingriff in das vierte Amendment stattgefunden hat. Entscheidend ist stattdessen die Erwartungshaltung des Betroffenen dahingehend, ob seine Handlungen privat bleiben. Der Fall *Katz* bewirkte also eine Verschiebung des Schutzobjekts von bestimmten Orten auf den Menschen. Damit umfasst der Schutzbereich des

---

818 Olmstead v. United States, 277 U.S. 438, 466 (1928).

819 *Warren/Brandeis*, 4 Harv. L. Rev. 193 (1890).

820 „[…] [The makers of our Constitution] sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.", *Justice Brandeis*, abweichende Meinung im Fall Olmstead v. United States, 277 U.S. 438, 478 (1928).

821 Katz v. United States, 389 U.S. 347 (1967).

822 Katz v. United States, 389 U.S. 347, 351 (1967).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

vierten Amendments grundsätzlich elektronische Kommunikation jeglicher Art.

b) Reasonable expectation of privacy-Test

Im Rahmen von *Katz* wurde durch die von *Justice Harlan* geschriebene übereinstimmende Meinung (sog. „concurring opinion") der bis heute bei Rechtsfragen des vierten Amendments angewendete reasonable expectation of privacy-Test entwickelt. Für eine reasonable expectation of privacy müssen kumulativ zwei Dinge vorliegen: Erstens musste der Betroffene die Erwartung gehabt haben, dass sein Handeln im Privaten stattfindet (subjektives Element), und zweitens muss diese Erwartungshaltung von der Gesellschaft als vernünftig, also nachvollziehbar, angesehen werden (objektives Element).[823]

Der reasonable expectation of privacy-Test bereitet dahingehend Probleme, dass es den Schutz der Verfassung senken kann, wenn Bürger sich in bestimmten Situationen daran gewöhnt haben, dass ihr Handeln nicht privat oder jedenfalls Dritten zugänglich ist. Dies verdeutlich sich an der sog. third party-doctrine.

aa) Die third party-doctrine als Ausschlussgrund

Nach der third party-doctrine bietet das vierte Amendment keinen Schutz, wenn der Betroffene seine Daten freiwillig an Dritte weitergegeben hat.[824] Überdies erklärte der *Supreme Court*, dass, selbst wenn der Betroffene diese subjektive Erwartungshaltung gehabt habe, diese jedenfalls nicht objektiv von der Gesellschaft als nachvollziehbar angesehen werde.[825] Dies gilt auch

---

823 „[…] there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'", Katz v. United States, 389 U.S. 347, 361 (1967).

824 „This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.", United States v. Miller, 425 U.S. 435, 443 (1976); vgl. auch Smith v. Maryland, 442 U.S. 735, 742 (1979).

825 Smith v. Maryland, 442 U.S. 735, 744 (1979).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

dann, wenn den Nutzern keine andere Wahl bleibt, als ihre Daten einem Dritten anzuvertrauen.[826]

Das bedeutet, dass das vierte Amendment immer dann keinen Schutz gewährt, wenn ein Dritter in die Daten involviert ist, sei es die Bank in Bezug auf die Kontoauszüge[827] oder die Telefongesellschaft in Bezug auf die Verbindungsdaten[828]. Dieser Schluss bereitet Probleme in einer Zeit, in der insbesondere Internetdiensteanbietern von einem breiten Spektrum an Daten profitieren, die die Nutzer ihnen entweder freiwillig mitteilen oder mittels Tracking Tools aggregiert werden. Denn damit können die Geschäftspraktiken privater Akteure den Schutzbereich des vierten Amendments verändern. Indem sie Daten sammeln, senkt sich die Erwartung des durchschnittlichen Nutzers, dass sein Handeln im Social Web privat ist. In der Konsequenz bestehen sie dann den reasonable expectation of privacy-Test nicht mehr. Durch die third party-doctrine werden Rechtsgüter von Verfassungsrang zur Disposition von außerstaatlichen Akteuren gestellt. Das kann dazu führen, dass nicht allein die Verfassung das maßgebende Mittel dessen ist, was geschützt werden sollte, sondern beispielsweise auch die Praxis der privaten Online-Diensteanbieter.

bb) Schutz von Daten auf mobilen Endgeräten

Die dargestellte third party-doctrine wirft die Frage nach dem Schutz von Daten, die in mobilen Endgeräten wie Handys gespeichert sind, unter dem vierten Amendment auf. Wie gezeigt stellte der *Supreme Court* in *Katz* klar, dass das vierte Amendment hauptsächlich dem Schutz der Menschen zugutekommt und nicht nur bestimmte Orte unter seinen Schutz stellt. Infolgedessen haben verschiedene Gerichte bestätigt, dass Daten auf Datenträ-

826 Vgl. die abweichende Meinung von *Justice Brennan* im Fall Smith v. Maryland: „It is idle to speak of "assuming" risks in contexts where, as a practical matter, individuals have no realistic alternative. More fundamentally, to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections. For example, law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications. (…)", Smith v. Maryland, 442 U.S. 735, 749 (1979).

827 United States v. Miller, 425 U.S. 435 (1976).

828 Smith v. Maryland, 442 U.S. 735 (1979).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

gern unter dem Schutz des vierten Amendments stehen. Hierbei wurde teilweise die Analogie zu einem geschlossenen Behältnis gezogen,[829] obwohl der *Supreme Court* urteilte, dass ein geschlossenes Gefäß bei einer rechtmäßigen Durchsuchung der Person, seines Autos oder seiner Wohnung ebenfalls ohne gesonderten Durchsuchungsbeschluss geöffnet werden darf.[830] Im Jahr 2014 urteilte der *Supreme Court* schließlich im Fall *Riley*, dass eine gerechtfertigte Privatheitserwartung in Handys bestehe. Damit umfasst ein Durchsuchungsbeschluss für eine Wohnung oder eine rechtmäßige Durchsuchung einer Person nicht mehr automatisch auch deren Handy. Da der *Supreme Court* moderne Handys als „Minicomputer" bezeichnet,[831] ist davon auszugehen, dass sich dieses Urteil auf jegliche moderne Endgeräte erstrecken lässt.

Fraglich ist, ob *Riley* damit als eine Abkehr der third party-doctrine bewertet werden kann. Der *Supreme Court* befand in diesem Fall, dass ein Handy nicht ohne Durchsuchungsbeschluss durchsucht werden dürfe. Er stellte dabei vor allem den Zugriff auf eine Vielzahl von Daten in den Vordergrund, wenn hierfür kein Durchsuchungsbeschluss verlangt werde.[832] Allerdings zählt der *Supreme Court* auch eine Vielzahl von Daten auf, die klassischerweise unter die third party-doctrine fallen, wie Daten, die in einer Cloud gespeichert sind.[833] Gleichzeitig betont der *Supreme Court* aber, dass auch Handys nicht immun gegen die Durchsuchung sein sollten und es natürlich auch hier Ausnahmen zu dem Erfordernis eines Durchsuchungsbeschlusses gebe.[834] Der *Supreme* Court erwähnt die third party-doctrine aber nicht explizit. In einer Gesamtschau des Falles ist davon auszugehen, dass der *Supreme Court* die third party-doctrine nicht aushebeln wollte, sondern nur die Erstreckung eines Durchsuchungsbeschlusses

---

829 United States v. Barth, 26 F.Supp.2d 929, 936 f. (W.D. Tex. 1998); United States v. Conklin, 63 M.J. 333, 337 (C.A.A.F. 2006), unter der Annahme, dass jede Datei für sich ein geschlossenes Behältnis darstellt.

830 United States v. Ross, 456 U.S. 798 (1982); das Urteil hob den Grundsatz, dass geschlossene Behälter immer einen gesonderten Durchsuchungsbeschluss benötigen aus der Entscheidung Robbins v. California, 453 U.S. 420 (1981) auf.

831 Riley v. California, 134 S.Ct. 2473 (2014).

832 „One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. […] But the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones.", Riley v. California, 134 S.Ct. 2473, 2489 (2014).

833 Riley v. California, 134 S.Ct. 2473, 2491 (2014).

834 Riley v. California, 134 S.Ct. 2473, 2493 (2014).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

auf mobile Endgeräte verhindern wollte. Dafür spricht auch, dass der *Supreme Court* klarstellt, dass das Urteil keine Entscheidung darüber treffe, wann eine Durchsuchung im Hinblick auf die Einsicht in gespeicherte digitale Daten vorliege.[835]

2. Willkürliche („unreasonable") Durchsuchung oder Beschlagnahme

Ferner muss die Durchsuchung oder Beschlagnahme auch willkürlich („unreasonable") erfolgt sein.

Grundsätzlich ist eine Durchsuchung oder Beschlagnahme dann nicht willkürlich im Sinne des vierten Amendments, wenn sie mittels eines Durchsuchungsbeschlusses erfolgt. Für einen Durchsuchungsbeschluss müssen die Polizeibeamten hierzu bei einem Richter vortragen, dass „probable cause" für die Durchsuchung oder Beschlagnahme gegeben ist.[836] Probable cause bedeutet das Vorliegen einer berechtigterweise vertrauenswürdigen Information, die ausreichend ist um einen Menschen in dem Glauben, dass er ein Vergehen begangen hat oder begeht, zu durchsuchen.[837]

Die Rechtsprechung des *Supreme Court* hat einige Ausnahmen vom Erfordernis eines Durchsuchungsbeschlusses erarbeitet.

a) Einwilligung durch den Gesprächspartner (misplaced trust-doctrine)

Kein Durchsuchungsbeschluss ist etwa erforderlich, wenn der Kommunikationspartner der Überwachung eines Gesprächs zustimmt. Denn das vierte Amendment gewährt keinen Schutz davor, der falschen Person sein Vertrauen zu schenken.[838] Diese Ausnahme ist deswegen interessant, weil sie sich auch in einfachgesetzlichen Rechtsgrundlagen, die sowohl für öffentliche als auch private Stellen gelten, niederschlägt. So sieht der Wiretap Act eine sog. one consent-rule vor, d. h., wenn einer der Gesprächspartner dem Abfangen einer Kommunikation zustimmt, ist dieses Abfangen zulässig.[839]

---

835 Riley v. California, 134 S.Ct. 2473, Fn. 1 (2014).
836 Federal Rules of Criminal Procedure, Rule 41 (d)(1).
837 Carroll v. United States, 267 U.S. 132, 162 (1925).
838 United States v. White, 401 U.S. 745, 749 ff. (1971).
839 Vgl. Kap. 4 Pkt. B.I.1.a.aa.iii, S. 258.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Einwilligung in die Durchsuchung

Ferner ist dann kein Durchsuchungsbeschluss nötig, wenn in die Durchsuchung eingewilligt wurde, wobei die Einwilligung nicht notwendigerweise vom Betroffenen selbst stammen muss. Diese Fallgruppen weisen insofern also Ähnlichkeit zu der misplaced trust-doctrine auf. Für die Durchsuchung einer Wohnung reicht es aus, wenn ein anderer Bewohner derselben Wohnung den Behörden Zutritt gewährt.[840] Dies gilt auch dann, wenn die Behörden fälschlicherweise annehmen, dass die zustimmende Person zur Einwilligung befugt ist.[841] Zwar erstreckt sich der Durchsuchungsbeschluss für die Wohnung, wie gezeigt, nicht mehr auf die Durchsuchung mobiler Endgeräte. Fraglich ist jedoch, wie sich die Einwilligung in die Durchsuchung eines mobilen Endgeräts durch einen Dritten auswirkt. Es gibt bislang keine Rechtsprechung des *Supreme Court* zu diesem besonderen Fall. Der *Wisconsin Supreme Court* hat in einem Fall entschieden, dass die Einwilligung der Freundin eines Betroffenen ausreicht, um dessen Computer zu durchsuchen. Allerdings hatte die Freundin für wenige Stunden Zugang zu dem Computer durch den Betroffenen erhalten.[842]

Ob der Fall auch ähnlich entschieden worden wäre, wenn die Freundin keine ausdrückliche Genehmigung zur Nutzung des Computers durch den Betroffenen erhalten hätte, bleibt offen. Aus einer Gesamtschau der dargestellten Fälle kann man schließen, dass die Durchsuchung ohne Durchsuchungsbeschluss dann rechtmäßig ist, wenn sich die Situation für die Behörden dergestalt darstellt, als sei die einwilligende Person zur Nutzung des Computers berechtigt. Selbiges dürfte gelten, wenn der Computer dem Einwilligenden nur kurzzeitig überlassen wurde. Je länger der Dritte Zugriff auf das Gerät hatte, desto schwerer dürfte die Vermutung wiegen, dass dieser auch in dessen Durchsuchung einwilligen durfte. Damit bleiben allerdings solche Fälle außer Betracht, in denen der Einwilligende offensichtlich in keinerlei Besitzverhältnis zu dem zu durchsuchenden Gerät steht.

c) Weitere Ausnahmen

Ergänzend sei ferner noch auf weitere Ausnahmen vom Erfordernis eines Durchsuchungsbeschlusses hingewiesen. Ein Durchsuchungsbeschluss ist

840 United States v. Matlock, 415 U.S. 164, 177 (1974).
841 Illinois v. Rodriguez, 497 U.S. 177, 198 f. (1990).
842 State v. Sobczak, 347 Wis.2d 724, 749 ff. (2013).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

nicht nötig für Dinge, die bei rechtmäßiger Anwesenheit mit bloßem Auge erkennbar sind (sog. plain view-doctrine)[843], oder wenn besondere Gründe, die ein sofortiges Handeln ohne Durchsuchungsbeschluss rechtfertigen, vorliegen (special needs-doctrine).[844]

III. Das fünfte Amendment

> „No person shall be held […] in any criminal case to be a witness against himself […]"

Im fünften Amendment ist das Recht auf Selbstbelastungsfreiheit niedergeschrieben. Zusammen mit dem vierten Amendment soll damit verhindert werden, dass zu Unrecht erlangte Beweisstücke in den Prozess gegen den Angeklagten eingeführt werden können.

Im digitalen Kontext stellt sich die Frage, ob das fünfte Amendment auch dagegen schützt, bestimmte Informationen wie Passwörter oder Verschlüsselungs-Codes herausgeben zu müssen. Im 19. Jahrhundert sah die Rechtsprechung des *Supreme Court* vor, dass das vierte und fünfte Amendment einer Klausel entgegenstehen, nach der die Beweiswirkung eines Dokuments, das ein Angeklagter eines Strafprozesses nicht herausgibt, gegen ihn vermutet wird.[845] Dieser Grundsatz wurde allerdings durch verschiedene Urteile aufgeweicht. In *Shapiro* urteilte der *Supreme Court* etwa, dass solche Dokumente jederzeit heraus verlangt werden können, die nach Maßgabe von einfachgesetzlichen Grundlagen archiviert werden müssen.[846] Weigert sich der Angeklagte, die geforderten Informationen preiszugeben, droht ihm eine Verurteilung wegen Missachtung des Gerichts („contempt"), was unter bestimmten Voraussetzungen eine Straftat für sich darstellen kann[847] und mit Geld- oder Freiheitsstrafe geahndet werden kann.[848]

---

843 Vgl. Harris v. United States, 390 U.S. 234, 236 (1968).

844 Hier werden die Interessen des Betroffenen mit den Interessen der Behörden an einer Durchsuchung abgewogen, vgl. *Justice Blackmun,* Concurring Opinion zum Fall New Jersey v. T.L.O., 469 U.S. 325, 351 (1985).

845 Boyd v. United States, 116 U.S. 616, 621 f. (1886).

846 Shapiro v. United States, 335 U.S. 1, 17 f. (1948).

847 Für einen ausführlichen Überblick über die verschiedenen Arten von contempt vgl. *Grote*, 88 Wash. U. L. Rev. 1247.

848 18 U.S.C. § 401 (3).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

1. Vergleichbarkeit mit Zeugenaussagen

Grundsätzlich können solche Informationen vom Angeklagten heraus verlangt werden, die nicht von Natur aus als Zeugenaussage („testimonial") eingestuft werden.[849] Für die Herausgabe von Passwörtern für technische Geräte ist demnach die Frage, ob diese als „Zeugenaussage" zu werten sind. Hierbei handelt es sich um einen substantiellen Wahrnehmungsgehalt, nämlich um solche Aussagen mit Wahrheitsgehalt, die von den Aussagenden getroffen werden.[850] So wurden etwa die Abgabe von Fingerabdrücken oder die Abnahme von Blut nicht als zeugenaussageähnlich gewertet,[851] da diese ohne Zutun des Betroffenen erlangt werden können. Ob die Herausgabe von Passwörtern eine Zeugenaussage darstellt, wurde vom *Supreme Court* noch nicht entschieden. In anderen Gerichten wurde der Frage jedoch nachgegangen, wobei die Urteile uneinheitlich ausfielen. So wurde die Herausgabe des Passwortes als problemlos zeugenaussageähnlich eingestuft.[852] Die Eingabe des Passwortes bereitete einem Gericht größere Probleme, da es sich hier um ein Tun und nicht um eine Aussage handelte. Das Gericht kam jedoch auch hier zu dem Ergebnis, dass die erzwungene Eingabe des Passwortes der Erfragung des Passwortes gleichstehe.[853] Anders liegt der Fall jedoch, wenn der Angeklagte eine unverschlüsselte Kopie des Datenträgers herausgeben sollte. Denn nach US-amerikanischer Rechtsprechung sind nicht die Dateien selbst, sondern nur der Akt der Herausgabe derselben als zeugenaussageähnlich einzustufen.[854]

2. Die foregone conclusion-doctrine als Ausschlussgrund

Ferner erlaubt die sog. „foregone conclusion-doctrine" einen Angeklagten dazu anzuhalten, solche Dokumente herauszugeben, deren Existenz sowie

849 Baltimore City Dept. of Social Services v. Bouknight, 493 U.S. 549, 554 f. (1990) zu der Frage, ob die Herausgabe eines Kindes vom fünften Amendment erfasst ist, m. w. N.
850 *Allen/Mace*, 94 J. Crim. L. & Criminology 243, 246 f.
851 Schmerber v. California, 384 U.S. 757, 764 (1966) m. w. N.
852 United States v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010).
853 In re: Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mj-91, 2007 WL 4246473, 3 (D. Vt. November 29, 2007)
854 United States v. Hubbell, 530 U.S. 27, 35 f. (2000).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Ort den Behörden bekannt ist und die beinahe nichts zu den bereits vorliegenden Beweisen gegen den Angeklagten hinzufügen.[855] Mit dieser Begründung wurde im Fall *In re Boucher* zwar davon abgesehen, den Angeklagten zur Eingabe des Passwortes zu zwingen, jedoch musste er eine Kopie des verschlüsselten Datenträgers zur Verfügung stellen, da die Behörden im Vorfeld bereits kleine Bilder erkennen konnten, die auf den Besitz von Dateien mit kinderpornographischem Inhalt schließen ließen.[856] Mit anderen Worten kann ein Angeklagter sich dann nicht auf das fünfte Amendment berufen, wenn die Behörden mit einer gewissen Sicherheit wissen, dass sich auf dem Datenträger belastendes Beweismaterial befindet. In einem Fall, in dem dafür keinerlei Anhaltspunkte bestanden, hat das Gericht die Pflicht zur Bereitstellung einer unverschlüsselten Kopie abgelehnt.[857] Dennoch wirft die foregone conclusion-doctrine gewisse Fragen auf. Erstens ist die Reichweite dieser Ausnahme unklar und wird von Gerichten unterschiedlich angewendet.[858] Ferner ist es regelmäßig schwierig, die Grenze zu ziehen, ab wann die Behörden Kenntnis von der Existenz und dem Ort des belastenden Beweismaterials haben und wann dahingehend nur eine bloße Vermutung besteht. Die Kenntnis dürfte „kaum etwas oder nichts“[859] zu den bereits vorhandenen Informationen beitragen. Zudem unterscheidet sich die Herausgabe des Passworts von der Herausgabe einer unverschlüsselten Kopie des Datenträgers kaum, da sie zum selben Ergebnis führen: Der Gewährung des Zugangs zu dem Gerät, auf dem sich nach Vermutung der Ermittlungsbehörden belastende Beweisstücke befinden.

IV. Erstes Amendment

> „Congress shall make no law […] abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.“

Das erste Amendment sichert den Bürgern unter anderem Meinungs-, Presse- und Versammlungsfreiheit zu. Es hat einen hohen Stellenwert im

855 Fisher v. United States, 425 U.S. 391, 411 (1976).
856 In re: Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mj-91, 2009 WL 424718, 3 f. (D. Vt. Februar 19, 2009).
857 In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1346 ff. (11th Cir. 2012).
858 *Mohan/Villasenor*, 15 U. Pa. J. Const. L. Height. Scrutiny 11, 15 f.
859 Vgl. Fisher v. United States, 425 U.S. 391, 411 (1976).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Rechtsgefüge der USA und ist besonderer Ausdruck der US-amerikanischen Freiheitskultur. Das erste Amendment wurde als Reaktion auf die Einschränkungen der Meinungs- und Pressefreiheit im England des 16. und 17. Jahrhunderts erlassen.[860] Es ist zweifellos ein *fundamental right*, seine Schutzwirkung variiert jedoch je nach Inhalt der Meinungsäußerung. Demnach genießen politische Meinungsäußerungen etwa den höchsten Schutz.[861] Gewisse Meinungsäußerungen von „geringem sozialen Wert"[862] genießen keinerlei Schutz, etwa „obscenity" (Obszänitäten, worunter etwa Kinderpornographie fällt) oder „fighting words" (Kampfparolen, d.h. solche Meinungsäußerungen, die darauf ausgerichtet sind, eine gewaltsame Reaktion eines anderen hervorzurufen[863]).[864] Das erste Amendment schützt anonyme Meinungsäußerungen ebenso wie offene Meinungsäußerungen.[865] Ferner entfaltet das erste Amendment seine Schutzwirkung auch im Internet.[866]

Das erste Amendment wirkt auch als Abwehrrecht gegen datenschützende Maßnahmen. So wird etwa das „Recht auf Vergessenwerden" als Verstoß gegen das erste Amendment gesehen.[867] Teilweise wird vertreten, dass das erste Amendment datenschützende Maßnahmen generell überwiege.[868] Da das right to information privacy keinen Verfassungsrang genießt,[869] ist die Rechtfertigung von Eingriffen in das erste Amendment jedenfalls schwierig.[870]

B. Einfachgesetzliche Regelungen

Das US-amerikanische Datenschutzrecht unterscheidet sich in wesentlichen Punkten von den Datenschutzregelungen in Deutschland und der EU.

Wie eingangs dargestellt, kennt das US-amerikanische Datenschutzrecht kein Verbot mit Erlaubnisvorbehalt. Demnach lässt sich die Regel in den

860 *Chemerinsky*, Constitutional Law, S. 1197 f..
861 Meyer v. Grant, 486 U.S. 414, 420 (1988).
862 Chaplinsky v. New Hampshire, 315 U.S. 568, 572 (1942).
863 R. A. V. v. St. Paul, 505 U.S. 377, 391 (1992).
864 R. A. V. v. St. Paul, 505 U.S. 377, 382 (1992).
865 McIntyre v. Ohio Elections Commission, 514 U.S. 334, 357 (1995).
866 Reno v. ACLU, Reno v. ACLU, 521 U.S. 844, 885 (1997).
867 Vgl. *Lee*, 12 J. L. Pol'y for Info. Soc'y 85, 85 f.
868 *Lee*, 12 J. L. Pol'y for Info. Soc'y 85, 86 m. w. N.
869 Vgl. Kap. 4 Pkt. A.I, S. 239.
870 Ebenso *Klar/Kühling*, AöR 2016, 165, 180.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

USA für den Umgang mit personenbezogenen Daten vereinfacht so ausdrücken: Erlaubt ist alles, was nicht ausdrücklich verboten wurde.[871]

Ferner ist der Anknüpfungspunkt nicht wie in Deutschland und der EU das personenbezogene Datum. Vielmehr lässt sich kein gemeinsamer Anknüpfungspunkt für die verschiedenen Regelungen finden, was auch daran liegt, dass sich die datenschutzrechtlichen Regelungen punktuell in verschiedenen Gesetzen finden.

Drittens sind die Bundesgesetze von der sog. one consent-rule geprägt: Viele Regelungen sehen vor, dass eine datenschutzrechtlich relevante Handlung rechtmäßig ist, wenn einer der beteiligten Gesprächspartner zustimmt. Dabei wurden von Gerichten teilweise gerade diejenigen, gegen deren Zugriffe der Betroffene sich zu wehren versuchte, als Gesprächspartner definiert.[872]

Außerdem gibt es im US-Bundesrecht keinen Anspruch auf Datenlöschung oder Höchstspeicherfristen.[873]

Im Folgenden werden die für diese Untersuchung relevanten Bundesgesetze und das Deliktsrecht der USA vorgestellt und ihre Anwendbarkeit auf die datenschutzrechtlich relevanten Handlungen von sozialen Netzwerken geprüft.

I. Datenschutzrechtliche Bestimmungen im Anbieter-Nutzer-Verhältnis

Im Folgenden werden zunächst datenschutzrechtliche Bestimmungen im Anbieter-Nutzer-Verhältnis dargestellt[874]. Dabei wird zunächst auf die Datenverarbeitung mittels Tracking Tools eingegangen, um das relevante Bundesrecht darzustellen. In einem nächsten Schritt wird die Zulässigkeit der Verarbeitung von durch den Nutzer selbst bereitgestellten Informationen eingegangen.

---

871 Vgl. auch *Klar/Kühling*, AöR 2016, 165, 179; *Kranig*, ZD-Aktuell 2012, 02910.

872 Vgl. Kap. 4 Pkt. B.I.1.a, S. 255.

873 *Tsesis*, 49 Wake Forest Law Review 433, 441.

874 Terminologisch kann dabei nicht, wie in Kapitel 3, auf die Zulässigkeit der Verarbeitung personenbezogener Daten abgestellt werden, da das US-amerikanische Datenschutzrecht nicht das personenbezogene Datum ins Zentrum der datenschutzrechtlichen Diskussion stellt, sondern andere Anknüpfungskriterien hat.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

1. Datenschutzrechtliche Bestimmungen hinsichtlich Tracking Tools

a) Wiretap Act

Der Wiretap Act[875] ist einer von drei Teilen des Electronic Communications Privacy Act (ECPA).[876] Das Gesetz ist auf öffentliche wie private Stellen gleichermaßen anwendbar. Regelungsgegenstand ist die Übertragung bestimmter Kommunikationsformen von ihrem Anfang bis zu ihrem Ende. Der Wiretap Act enthält sowohl Straftatbestände als auch zivilrechtliche Schadensersatzbestimmungen. Gem. 18 U.S.C. § 2511 (1) i. V. m. 18 U.S.C. § 2511 (4)(a) wird das Abfangen bestimmter Kommunikationen sowie das Benutzen oder Weitergeben von Kommunikationsinhalten mit Geld- oder Freiheitsstrafe von bis zu fünf Jahren bestraft. Geschützt sind drei Kommunikationsformen: Drahtkommunikationen („wire communication"), das heißt gem. 18 U.S.C. § 2510 (1) i. V. m. 18 U.S.C. § 2510 (18) solche Kommunikationen, die die menschliche Stimme beinhalten und unter Nutzung von Kabel- oder ähnlichen Vorrichtungen zwischen dem Ursprungs- und dem Empfangsort übertragen werden; mündliche Kommunikationen („oral communication"), das heißt gem. 18 U.S.C. § 2510 (2) eine mündliche Unterhaltung, in der die Beteiligten die gerechtfertigte Erwartung haben, dass ihre Unterhaltung nicht abgefangen werden; und elektronische Kommunikationen („electronic communication"), die gem. 18 U.S.C. § 2510 (12) ganz oder teilweise in der Übertragung von Zeichen, Signalen, Schrift, Bildern, Ton, Daten oder sonstigem Gedankengut über Kabel-, Radio-, Elektromagnetwellen-, Photoelektronik- oder Photooptiksysteme besteht, ohne Draht- oder mündliche Kommunikation i. S. d. ECPA zu sein.

aa) Datenerhebung mittels Tracking Tools

Im Folgenden soll untersucht werden, ob und wie die Datenerhebung mittels technischer Hilfsmittel unter dem Wiretap Act reguliert ist.

Maßgeblich ist hierfür zunächst die Bestimmung des 18 U.S.C. § 2511 (1)(a):

> „Except as otherwise specifically provided in this chapter any person who--

875 18 U.S.C. §§ 2510 – 2522.

876 Die beiden anderen Teile sind der Stored Communications Act, 18 U.S.C. §§ 2701 – 2712, und der Pen Register Act, 18 U.S.C. §§ 3121 – 3127.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

> intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; […] shall be punished […]."

Näher untersucht werden müssen die Begriffe der Kommunikation („communication") (dazu i.) und des Abfangens („intercept") (dazu ii.)

i) Kommunikationsbegriff ("communication")

Da Draht- und mündliche Kommunikationen als Voraussetzung haben, dass mindestens ein Teil der Kommunikation die menschliche Stimme beinhalten muss, kommt für die klassische Verwendung von sozialen Netzwerken nur die elektronische Kommunikation in Betracht. Das ist gem. 18 U.S.C. § 2510 (12) die Übertragung von Zeichen, Signalen, Schrift, Bildern, Ton, Daten oder sonstigem Gedankengut, die ganz oder teilweise über Kabel-, Radio-, Elektromagnetwellen-, Photoelektronik- oder Photooptiksysteme erfolgt, ohne Draht- oder mündliche Kommunikation i. S. d. ECPA zu sein.

Fraglich ist, auf welchen Kommunikationsvorgang beim Platzieren von Tracking Tools abzustellen ist. In Betracht kommt der Kommunikationsvorgang zwischen Nutzerbrowser und Server, auf dem die Daten der Website platziert sind, wenn der Nutzer die Website besucht. Bei dem Einsatz von Tracking Tools durch Dritte, wie etwa im Fall von Social Plug-Ins,[877] kommt zudem die Kommunikation zwischen Nutzerbrowser und dem Dritt-Server, also demjenigen, der die Platzierung von Tracking Tools auf dem Endgerät des Nutzers vornimmt, in Betracht. In beiden Fällen stellen die Anfragen und Antworten durch den Nutzerbrowser und die entsprechenden Server eine elektronische Kommunikation i. S. d. 18 U.S.C. § 2510 (12) dar, da die Kommunikation bestehend aus Anfragen und Antworten zwischen Nutzerbrowser und Server eine Übertragung von Daten über eines oder mehrerer der in 18 U.S.C. § 2510 (12) genannten Systeme darstellt. Teilweise stellen die Gerichte eben auf diese Kommunikation bei der Platzierung der Tracking Tools ab.[878] Dies ist deswegen problematisch, weil aufgrund der one consent-rule bereits die Einwilligung eines Kommunikationspartners ausreicht, um einem Eingreifen der Bestimmungen nach

877 Vgl. Kap. 3 Pkt. C, S. 199.
878 Vgl. z. B. In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434 (D. Del. 2013).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

18 U.S.C. § 2511 (1)(a) entgegenzustehen. Diese Einwilligung könnte durch die besuchte Website gegeben werden.[879]

ii) Abfangen von Inhalten

(1) Abfangen

Die Kommunikation müsste auch abgefangen werden. Gem. 18 U.S.C. § 2510 (4) bedeutet Abfangen die akustische oder anders geartete Beschaffung von Inhalten einer Draht-, elektronischen, oder mündlichen Kommunikation unter Nutzung irgendeines elektrischen, mechanischen oder anders gearteten Hilfsmittels. Es muss also nicht notwendigerweise ein Dritter sein, der die Kommunikation abfängt; es genügt hierfür jegliche Beschaffung von Kommunikationsinhalten. Fraglich ist jedoch der Inhaltsbegriff.

(2) Inhalte

Inhalte sind gem. 18 U.S.C. § 2510 (8) alle Informationen, die die Substanz, den Tenor oder die Bedeutung der Kommunikation betreffen. In einer alten Fassung enthielt der Passus außerdem noch die Identität der Person; dieser Passus wurde jedoch in der neuen Fassung von 1986 gestrichen.[880] Dies wurde von den Gerichten so definiert, dass Informationen, die die Person identifizierbar machen, jedoch nicht die Substanz der Kommunikation selbst betreffen, keine Inhalte i. S. d. Wiretap Act sind.[881] Hier unterscheidet sich das US-amerikanische Recht in einem wesentlichen Punkt zum europäischen und unionalen Recht, in dem der Anknüpfungspunkt das personenbezogene Datum ist: Inhalte i. S. d. Wiretap Act sind nur die Informationen, die der Nutzer bewusst kommunizieren will, wie das gesprochene

879 Vgl. Kap. 4 Pkt. B.I.1.a.aa.iii, S. 258.
880 In re iPhone Application Litigation, 844 F.Supp2d 1040, 1062 (N.D. Cal. 2012).
881 Graf v. Zynga Game Network, Inc., 750 F.3d 1098, 1105 f. (9th Cir. 2014); In re iPhone Application Litigation, 844 F.Supp2d 1040, 1062 (N.D. Cal. 2012); Sams v. Yahoo!, Inc., No. CV–10–5897–JF(HRL), 2011 WL 1884633, 7 (N.D. Cal., May 18 2011); In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 444 (D. Del. 2013).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Wort bei einem Telefonat.[882] Mit diesem Argument wurde die Anwendbarkeit des Wiretap Act auf die Verwendung von Cookies,[883] IP-Adressen,[884] Standortdaten[885] und persönliche Daten, wie etwa Adressen,[886] abgelehnt, selbst wenn die Substanz der Kommunikation zwischen Nutzerbrowser und Plattformserver üblicherweise gerade diese Daten betreffen. Anders liegt der Fall nur, wenn die Nutzer gerade bewusst durch Vornahme einer Kommunikationshandlung diese Daten übermitteln, etwa wenn die IP-Adresse Inhalt einer Nachricht ist.[887] Damit ist der Wiretap Act nicht gegen die klassischen Tracking Tools anwendbar.

iii) Die one consent-rule als Hindernis der Durchsetzbarkeit

Selbst wenn der Einsatz von diversen Tracking Tools unter den Wiretap Act fiele, sehen dessen Vorschriften Ausnahmen vor, die seiner Durchsetzbarkeit im Wege stehen können.

Die größte Ausnahme bildet die one consent-rule in 18 U.S.C. § 2511 (2)(d). Danach ist das Abfangen der Kommunikationen dann rechtmäßig, wenn *einer* der Kommunikationspartner dem Abfangen zustimmt.[888] Damit kommt es auch bei der Platzierung von Tracking Tools durch Dritte bezüglich des Abfangens nicht darauf an, ob auf die Kommunikation zwischen dem Nutzerbrowser und dem Server der besuchten Website oder auf die Kommunikation zwischen dem Nutzerbrowser und dem Server des Dritten, der die Tracking Tools einsetzt, abgestellt wird. Die Konsequenz lässt sich am Beispiel von Social Plug-Ins verdeutlichen: Selbst wenn man auf die

882 In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 444 (D. Del. 2013); United States v. Reed, 575 F.3d 900, 916 (9th Cir. 2009).

883 In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 443 f. (D. Del. 2013).

884 Sams v. Yahoo!, Inc., No. CV–10–5897–JF(HRL), 2011 WL 1884633, 7 (N.D. Cal. May 18, 2011).

885 In re iPhone Application Litigation, 844 F.Supp2d 1040, 1061 f. (N.D. Cal. 2012).

886 In re iPhone Application Litigation, 844 F.Supp2d 1040, 1061 f. (N.D. Cal. 2012).

887 Vgl. Blumofe v. Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003).

888 Einige Staaten haben demgegenüber Gesetze, die die Einwilligung aller an der Kommunikation Beteiligten erfordern, wie etwa Kalifornien, vgl. Cal. Pen. Code § 632.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Kommunikation zwischen dem Nutzerbrowser und dem Server der besuchten Website abstellte, kann der Websitebetreiber in die Platzierung der Tracking Tools durch einen Dritten einwilligen. Wenn die Gerichte stattdessen auf die Kommunikation zwischen dem Dritten und dem Nutzerbrowser abstellen, kann der Platzierende der Tracking Tools in das Abfangen einwilligen. Dies gilt nur dann nicht, wenn die Browsereinstellungen des Nutzers sich eindeutig gegen das konkrete Tracking Tool richten und diese Einstellungen gezielt umgangen werden.[889]

bb) Datenverwendung und Datenweitergabe

Gem. 18 U.S.C. § 2511 (1)(c) bzw. (d) ist auch die Verwendung von Kommunikationsinhalten sowie die Weitergabe derselben verboten. Allerdings wird eine Anwendung gegen die Betreiber von sozialen Netzwerken an den oben dargelegten Gründen scheitern.

b) Stored Communications Act

aa) Platzieren von Cookies

> „Except as provided in subsection (c) of this section whoever—
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; […]
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section."[890]

Der Stored Communications Act (SCA) verbietet zwar nicht ausdrücklich die Datenerhebung, könnte aber auf das Platzieren von Tracking Tools auf dem Nutzerrechner anwendbar sein. Gem. 18 U.S.C. § 2711 (1) gelten die Definitionen des Wiretap Act auch für den SCA. Der SCA untersagt den unautorisierten Zugriff auf eine Einrichtung durch die ein Dienst zur Erbringung von elektronischer Kommunikation i. S. d. 18 U.S.C. § 2510 (14) bereitgestellt wird, wenn hierdurch autorisierter Zugang zu einer Draht- oder elektronischen Kommunikation erlangt, verändert oder verhindert wird,

889 In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 443 (D. Del. 2013).
890 18 U.S.C. § 2701(a).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

während sie sich in elektronischer Speicherung („electronic storage") befindet. Elektronische Speicherung wird nach 18 U.S.C § 2510 (17) als vorübergehende, zwischenzeitliche Speicherung von elektronischer Kommunikation bezeichnet, die der elektronischen Übertragung inhärent ist. Fraglich ist, was als Einrichtung i. S. d. 18 U.S.C. § 2701(a) zu definieren ist und wann ein Zugriff auf diese nicht autorisiert ist.

i) Einrichtung i. S. d. Norm

Erste Voraussetzung für das Eingreifen der Norm ist das Vorliegen einer Einrichtung, durch die ein Dienst, der den Nutzern die Möglichkeit gibt elektronische Kommunikationen zu versenden oder zu empfangen, bereitgestellt wird. Da viele Tracking Tools auf dem Nutzerrechner platziert werden,[891] müsste dieser als Einrichtung i. S. d. 18 U.S.C. § 2701 (a) gelten. Teilweise wurde der Rechner des Nutzers als Einrichtung i. S. d. Norm qualifiziert.[892] Dies wurde jedoch in zahlreichen Gerichtsurteilen bezweifelt, da der Nutzerrechner vielmehr Dienste, um Kommunikationen zu versenden und empfangen, in Anspruch nimmt, als diese bereitzustellen.[893] Die wohl überwiegende Meinung in den USA geht daher davon aus, dass die Nutzerrechner schon das erste Merkmal nicht erfüllen. Dies gilt auch deswegen, weil diese Definition sonst darin resultieren könnte, dass Serviceprovider aufgrund der Ausnahme in 18 U.S.C. § 2701 (c) vorbehaltslos Zugriff auf Nutzerrechner gewähren könnten.[894]

---

891 Vgl. Kap. 1 Pkt. C.II, S. 40.

892 In re Doubleclick Privacy Litigation, 154 F.Supp.2d 497, 509 (S.D.N.Y. 2001); In re Toys R Us, Inc., Privacy Litigation, No. C 00-2746 MMC, 2001 WL 34517252, 5 (N.D. Cal. October 9, 2001).

893 In re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp. 2d 4, 13 f. (D. Mass. 2002); In re iPhone Application Litigation, 844 F.Supp2d 1040, 1058 (N.D. Cal. 2012); In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 446 (D. Del. 2013); In re Nickelodeon Consumer Privacy Litigation, MDL No. 2443 (SRC), 2014 WL 3012873, 16 (D.N.J. July 2, 2014); Cousineau v. Microsoft Corp., 6 F. Supp. 3d 1167, 1174 f. (W.D. Wash. 2014); Morgan v. Preston, No. 3:13-00403, 2013 WL 5963563, 5 (M.D. Tenn. November 7, 2013).

894 In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 445 f. (D. Del. 2013) m w. N..; In re Nickelodeon Consumer Privacy Litigation, MDL No. 2443 (SRC), 2014 WL 3012873, 16 (D.N.J. July 2, 2014); vgl. Kap. 4 Pkt. B.I.1.b.aa.iii, S. 261.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ii) Elektronische Speicherung

Selbst wenn man davon ausgeht, dass der Nutzerrechner eine Einrichtung im Sinne der Norm ist, muss geklärt werden, ob sich die Kommunikation in elektronischer Speicherung befindet. Viele Tracking Tools werden gerade langfristig auf dem Endgerät des Nutzers abgelegt. Gem. 18 U.S.C. § 2510 (17) ist elektronische Speicherung die vorübergehende, zwischenzeitliche Speicherung von elektronischer Kommunikation, die der elektronischen Übertragung inhärent ist. Für die Zeit, in der die Dateien auf der Festplatte der Nutzerrechner gespeichert sind, wird die Platzierung von Tracking Tools demnach nicht durch den SCA reguliert. Einige Gerichte stellten jedoch klar, dass dies nicht gilt, solange die Cookies sich im sog. Random-Access Memory (RAM) befinden.[895]

iii) Ausschluss durch die one consent-rule

Für die Fälle, in denen die Gerichte davon ausgingen, dass ein Zugriff auf eine Einrichtung i. S. d. SCA erfolgte und sich die angegriffene Kommunikation ferner in einem Zustand der elektronischen Speicherung befand, musste ferner geklärt werden, ob das Platzieren eines Tracking Tools auf dem Nutzerrechner ein unerlaubter Zugriff auf diesen i. S. d. Norm ist. Dabei sind Zugriffe dann vom Tatbestand von vornherein ausgenommen, wenn eine Person oder ein Unternehmen, die einen Draht- oder elektronischen Kommunikationsdienst („wire or electronic communication service“)[896] bereitstellen oder von einem Nutzer derselben hinsichtlich einer Kommunikation, an der dieser beteiligt ist, in den Zugriff einwilligen, 18 U.S.C. § 2701 (a) i. V. m. 18 U.S.C. § 2701 (c). Der Begriff des elektronischen Kommunikationsdienstes wurde teilweise sehr weit als das Internet an sich definiert.[897] Als Nutzer des Internets i. S. d. 18 U.S.C. § 2701 (c)(2) wurden die besuchten Websites eingestuft, mit der Begründung, dass Nut-

895 In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 447 (D. Del. 2013); In re Toys R Us, Inc., Privacy Litigation, No. C 00-2746 MMC, 2001 WL 34517252, 3 (N.D. Cal. October 9, 2001); In re iPhone Application Litigation, 844 F.Supp2d 1040, 1059 (N.D. Cal. 2012).

896 Definition s. 18 U.S.C. § 2510 (15).

897 In re Doubleclick Privacy Litigation, 154 F.Supp.2d 497, 508 (S.D.N.Y. 2001).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

zer i. S. d. Norm nicht notwendigerweise Personen sein müssen und Websites Anfragen an Server stellen können.[898] Damit konnten die besuchten Websites als Kommunikationspartner des Nutzerbrowsers dem Zugriff der Dritten auf die Nutzerrechner zustimmen. Wenn man auf die Kommunikation zwischen dem Nutzerbrowser und dem Dritten abstellt, kann der Dritte unproblematisch der Platzierung der Tracking Tools selbst zustimmen. Dies führt zu dem Ergebnis, dass nach der derzeitigen Gesetzeslage ein dem Nutzer unbekannter Dritter auf seinem Rechner Tracking Tools installieren kann, weil der Zugreifende und nicht der Nutzer selbst dem Zugriff zugestimmt hat.

Insgesamt stellt sich die Rechtslage so dar, dass – wenn auch durch verschiedene Interpretationen der Norm – die Anwendbarkeit des SCA auf die Fälle der Datenerhebung mittels Tracking Tools als unanwendbar befunden wurde.

bb) Weitergabe von gespeicherten Nachrichten

> „[…] (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service […].“[899]

Der SCA bestraft ferner die Weitergabe von Kommunikationsinhalten gem. 18 U.S.C. § 2702. Fraglich ist daher, ob es sozialen Netzwerken oder Dritten gestattet ist, die erhobenen Daten miteinander auszutauschen oder an andere Personen oder Unternehmen weiterzugeben. Personen oder Unternehmen, die einen elektronischen Kommunikationsdienst für die Öffentlichkeit anbieten, dürfen nach Vorschriften der Norm keine Kommunikationsinhalte preisgeben. Der Inhaltsbegriff ist dabei derselbe wie der des Wiretap Act, vgl. 18 U.S.C. § 2711. Inhalte sind wie dargelegt nur die Informationen, die der Nutzer bewusst kommunizieren will.[900] Damit greift die Regelung von vornherein nicht für die Weitergabe von Daten, die mittels Tracking Tools erhoben wurden. Ferner enthält der SCA mit 18 U.S.C. § 2702 (b)(3) wiederum eine Vorschrift, die die Weitergabe von Daten mit

---

898 In re Doubleclick Privacy Litigation, 154 F.Supp.2d 497, 508 ff. (S.D.N.Y. 2001); In re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp. 2d 4, 13 f. (D. Mass. 2002).

899 18 U.S.C. § 2702 (a)(1).

900 Vgl. Kap. 4 Pkt. B.I.1.a.aa.i, S. 256; In re Google Inc. Cookie Placement Consumer Privacy Litigation, 988 F.Supp.2d 434, 444 (D. Del. 2013); United States v. Reed, 575 F.3d 900 (9th Cir. 2009).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Einwilligung *einer* der Parteien der Kommunikation gestattet; gleichgültig ob die Daten von dem sozialen Netzwerk oder dem Dritten erhoben werden, ist diese Norm für diese Fälle nicht anwendbar.

c) Deliktsrecht

Datenschutzrechtsverstöße können auch deliktsrechtlich durch die gewohnheitsrechtlich anerkannten „privacy torts" verfolgt werden.

aa) Intrusion upon seclusion

> „One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[901]

Der intrusion upon seclusion Anspruch gibt Verletzten einen Rechtsanspruch gegen das Eindringen Anderer in ihre Privatsphäre.

Voraussetzung hierfür ist zunächst das Eindringen in die Privatsphäre, das heißt in einen Ort, in den der Kläger sich bewusst zurückgezogen hat, um Privatsphäre genießen zu können. Das Eindringen in die Privatssphäre kann dabei physischer Natur sein oder mittels technischer Erweiterung seiner natürlichen Sinne.[902] Ferner müsste das Eindringen auch nach objektiven Maßstäben anstößig sein. Dieser objektive Maßstab ergibt sich aus den Worten „reasonable person".

Das Merkmal der Anstößigkeit setzt einen Schweregrad des Eindringens in die Privatsphäre fest. Ähnlich wie unter dem vierten Amendment kommt es darauf an, was ein objektiver Beobachter vernünftigerweise als besonders schweres Eindringen in seine Privatsphäre beurteilen würde. Dieses Merkmal wandelt sich jedoch mit gesellschaftlichen Veränderungen. Letztlich haben auch hier die Diensteanbieter populärer sozialer Netzwerke die Möglichkeit über ihr Verhalten die Durchsetzung von Rechtsansprüchen zu steuern. Je üblicher und akzeptierter die Erhebung und Verarbeitung von personenbezogenen Daten ist, desto höher sind die Hürden für eine Durch-

901 *The American Law Institute,* Restatement of the Law Second, Torts, § 652B.
902 *The American Law Institute,* Restatement of the Law Second, Torts, § 652B, comment b.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

setzung des intrusion upon seclusion-Anspruchs. Entsprechend wurde weder die Vernetzung von Nutzerdaten über verschiedene Dienste und Geräte hinweg noch die Weitergabe der Daten an Dritte für objektiv anstößig befunden.[903] Auch die Platzierung von Cookies auf den Rechnern von minderjährigen Nutzern wurde nicht als objektiv anstößig angesehen,[904] genauso wenig wie das Hochladen eines Bildes eines Familienhauses in dem online-Kartenservice *Google Street View*[905].[906] Stattdessen wurde die Norm derart ausgelegt, dass nur besonders außergewöhnliche und schwerwiegende Fälle unter die Norm fallen sollen,[907] etwa heimliche Videoaufnahmen im Badezimmer eines Anderen.[908]

Damit erweist sich der intrusion upon seclusion-Anspruch nicht als wirksamer Anspruch gegen das Platzieren von Tracking Tools oder Verarbeitung von Daten.

bb) Appropriation of name or likeness

> „One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[909]

Der appropriation of name or likeness-Anspruch soll die Identität der Betroffenen vor einer Verwendung durch einen Anderen schützen und gewährt Betroffenen einen Schadensersatzanspruch für psychische Belastungen, die durch die Verwendung ihrer Identität entstanden sind.

Interessant ist dieser Anspruch für solche Fälle, in denen soziale Netzwerke den Namen ihrer Nutzer in einem bestimmten Kontext anzeigen, etwa im Falle von *Facebooks* sog. *Sponsored Stories*, in denen anderen Nutzern bestimmte Werbeeinblendungen angezeigt werden unter dem Hinweis,

---

903 In re Google, Inc. Privacy Policy Litig., 58 F.Supp.3d 968, 987 f. (N.D. Cal. 2014).

904 In re Nickelodeon Consumer Privacy Litigation, MDL No. 2443 (SRC), 2014 WL 3012873, 19 (D.N.J. July 2, 2014) und 2015 WL 248334, 5f. (D.N.J. January 20, 2015).

905 *Google Inc.,* Google Street View, abrufbar unter http://www.google.com/maps/streetview/ (abgerufen am 13.10.2017).

906 Boring v. Google Inc., 362 Fed. Appx. 273 (3rd Cir. 2010).

907 In re Nickelodeon Consumer Privacy Litigation, 2015 WL 248334, 6 (D.N.J. January 20, 2015) m. w. N.

908 Soliman v. Kushner Companies, Inc., 433 N.J. Super. 153 (N.J. Super. Ct. App. Div. 2013).

909 *The American Law Institute,* Restatement of the Law Second, Torts, § 652C.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

dass ein bestimmter anderer Nutzer dieses Produkt mit der *Facebook*-eigenen Funktion „gefällt mir" markiert hat.

Der Anspruch ist nicht anwendbar, wenn der Name für Nachrichten von öffentlichem Interesse genutzt wird. Dabei müssen jedoch die Nachrichten in Kausalzusammenhang mit dem Namen stehen; es kommt dabei gerade auf den journalistischen Hintergrund der Namensnutzung an.[910] Entsprechend wurde das Eingreifen der Ausnahme bei einer Verwendung des Namens rein zu Werbezwecken im Falle der *Sponsored Stories* abgelehnt.[911]

Allerdings ist der Anspruch dann nicht durchsetzbar, wenn die Nutzer ihre Einwilligung zur Verwendung ihres Namens gegeben haben. Die AGB müssen explizit auf die Verwendung des Namens zu Werbezwecken hinweisen; ein bloßer Hinweis darauf, dass der Name keinen Privatsphäreeinstellungen unterliegen kann, wurde demnach nicht als ausreichend angesehen.[912]

Insgesamt betrachtet erweist sich der Anspruch damit als ein wirkungsvolles Mittel gegen die Verwendung der eigenen Identität zu Werbezwecken durch die sozialen Netzwerke. Dies gilt jedoch nur, wenn die AGB nicht entsprechende ausdrückliche Regelungen enthalten.

2. Datenschutzrechtliche Bestimmungen hinsichtlich vom Nutzer selbst bereitgestellter Daten

Für vom Nutzer selbst bereit gestellte Fälle kommen die dargelegten Gesetzeswerke überwiegend nicht in Betracht. Soweit die Plattformbetreiber die bereitgestellten Informationen in einer Art zweckentfremden, die irreführend ist, kommt u. U. eine Regulierung durch die FTC in Betracht.[913]

Denkbar ist aber eine Anwendbarkeit des SCA für die Auswertung der Nachrichteninhalte nach 18 U.S.C. § 2701 (a)(1) auf Postings auf Profilen. Sowohl private Nachrichten, also Nachrichten zwischen zwei oder mehreren Personen, als auch Postings im eigenen Profil oder Profilen Anderer fallen unter die Definition der elektronischen Kommunikation. Fraglich ist jedoch, ob sich diese auch in elektronischer Speicherung gem. 18 U.S.C.

910 *The American Law Institute,* Restatement of the Law Second, Torts, § 652C, comment d.
911 Fraley v. Facebook, Inc., 830 F.Supp.2d 785, 804 f.(N.D. Cal. 2011).
912 Cohen v. Facebook, Inc., 798 F.Supp.2d 1090, 1094 ff.(N.D. Cal. 2011).
913 Vgl. dazu Kap. 4 Pkt. B.I.3, S. 267.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

§ 2510 (17)(A) befinden, da diese endgültig auf den Servern der Plattformbetreiber verbleiben und damit nicht das Element der zeitlichen Begrenzung erfüllen. Allerdings liegt eine elektronische Speicherung auch dann vor, wenn die Plattformbetreiber die Nutzerinformationen zu Zwecken der Datensicherung speichern, 18 U.S.C. § 2510 (17)(B). Soweit dies bei sozialen Netzwerken der Fall ist, befinden sich die Nutzerinformationen demnach in elektronischer Speicherung i. S. d. SCA. Für *Facebook* hat ein Gericht bereits festgestellt, dass auch die zeitlich unbegrenzte Datensicherung der Nutzerinformationen das Tatbestandsmerkmal erfüllt.[914] Postings fallen nach einem Gerichtsurteil trotz 18 U.S.C. § 2511 (g), der für den gesamten ECPA eine Ausnahme für öffentlich zugängliche elektronische Kommunikationen bildet, dann in den Schutzbereich des SCA, wenn die Postings nur einem begrenzten Publikum zur Verfügung stehen.[915] Solange Postings also mittels der Funktionen des jeweiligen sozialen Netzwerks nicht jedem Internetnutzer, sondern nur dem eigenen Freundesnetzwerk angezeigt werden, sind sie nicht öffentlich zugänglich i. S. d. Norm. Im Lichte von Netzwerken, in denen Nutzer bisweilen eine Kontaktanzahl in vierstelliger Höhe haben, ist es jedoch durchaus möglich, dass dies von anderen Gerichten anders entschieden würde.

Fraglich ist jedoch wiederum das Merkmal der Einrichtung, durch die ein elektronischer Kommunikationsdienst bereit gestellt wird i. S. d. 18 U.S.C. § 2702 (a)(1). Um eine Anwendbarkeit zu konstruieren, müsste vorliegend das Nachrichtenfach oder das Nutzerprofil als eine solche Einrichtung angesehen werden.[916] Nach dem oben dargelegten Einrichtungsbegriff[917] erscheint zweifelhaft, inwiefern ein Nachrichtenfach oder ein Profil eine Einrichtung ist, durch die ein elektronischer Kommunikationsdienst bereitgestellt wird. Selbst wenn man davon ausginge, dass der elektronische Kommunikationsdienst die Dienste des sozialen Netzwerks an sich sind, werden diese ebenso wenig *durch* das Nachrichtenfach oder durch das Profil bereitgestellt wie durch den Computer. Darüber hinaus würde diese Interpretation wieder zu dem fragwürdigen Ergebnis führen, dass die Betreiber der sozialen Netzwerke als Betreiber des Kommunikationsdienstes gem. 18 U.S.C.

914 Ehling v. Monmouth-Ocean Hospital Service Corporation, 961 F.Supp.2d 659, 667 f. (D.N.J. 2013).

915 Ehling v. Monmouth-Ocean Hospital Service Corporation, 961 F.Supp.2d 659, 668 (D.N.J. 2013).

916 So wohl die Interpretation in Ehling v. Monmouth-Ocean Hospital Service Corporation, 961 F.Supp.2d 659 (D.N.J. 2013).

917 Vgl. Kap. 4 Pkt. B.I.1.b.aa.i, S. 260.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

§ 2701 (c)(1) Anderen den Zugriff auf das Nachrichtenfach und das Profil erlauben könnten, und zwar ohne Einwilligung des Nutzers.

Daher eignet sich die Norm nicht dazu, die Auswertung von Nachrichteninhalten der Nutzer durch die Betreiber der sozialen Netzwerke zu reglementieren.

3. Regulierung durch die Federal Trade Commission

> "(a)(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful. […]
>
> (n) Definition of unfair acts or practices. The Commission shall have no authority under this section or section 18 [15 USCS § 57a] to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."[918]

Wie dargestellt greifen das einschlägige Bundesrecht und das Deliktsrecht weder bei dem Umgang mit durch den Einsatz von Tracking Tools gewonnenen Informationen noch bei freiwillig bereitgestellten Informationen hinreichend ein. Allerdings könnte das Vorgehen gegen 15 U.S.C § 45 verstoßen, wenn es sich dabei um „[…] unfair and deceptive acts […]" i. S. d. Norm handelt. Die Federal Trade Commission (FTC) ist eine unabhängige Bundesbehörde der USA, die für Wettbewerbsregulierung und Verbraucherschutz zuständig ist. In dieser Funktion geht sie auch gegen soziale Netzwerkbetreiber vor.[919]

---

918 15 U.S.C. § 45 (a)(1); 15 U.S.C. § 45 (n).

919 Vgl. etwa *FTC*, GeoCities, abrufbar unter https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities (abgerufen am 13.10.2017); *FTC*, Myspace LLC, In the Matter of, abrufbar unter https://www.ftc.gov/enforcement/cases-proceedings/102-3058/myspace-llc-matter (abgerufen am 13.10.2017)*; FTC*, Facebook, Inc., abrufbar unter https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

a) „Unfair and deceptive“

Die Bewertung, ob die angewandten Methoden „unfair“ sind, erfolgt dabei anhand drei Kriterien: Erstens soll die FTC in Betracht ziehen, ob es sich dabei um Methoden handelt, die geeignet sind, den Verbrauchern starken Schaden zuzufügen, zweitens, ob dieser Schaden nicht von den Verbrauchern selbst vermieden werden konnte, und drittens, ob die Methoden nicht Vorteile für den Verbraucher oder den Wettbewerb haben, die den Verstoß aufwiegen, 15 U.S.C. § 45 (n). Bei der Beurteilung, ob Methoden „deceptive“ sind, bezieht die FTC in die Beurteilung ein, ob eine Aussage getroffen wurde, ob diese Aussage mit gewisser Wahrscheinlichkeit irreführend war und ob die Aussage wesentlich („material“) war,[920] wobei eine wesentliche Aussage Informationen enthält, die Wichtigkeit für die Verbraucher haben und daher mit Wahrscheinlichkeit ihre Wahl oder ihr Verhalten hinsichtlich des Produkts beeinflussen.[921]

b) Datenschutzrechtliche Durchsetzung durch die FTC

Die FTC geht demnach hauptsächlich gegen missverständliche oder falsche Angaben in den Datenschutzrichtlinien der Diensteanbieter vor. Zwar empfiehlt die FTC dahingehend die Einhaltung von Vorgaben zu Nutzerinformation, Wahlmöglichkeiten, Zugangsmöglichkeiten für Nutzer zu den über sie gespeicherten Daten und Datensicherheit (sog. „fair information practices“).[922] Es handelt sich hierbei jedoch nur um Empfehlungen und nicht um verbindliche Vorgaben. Tatsächlich gibt es auf Bundesebene keine Pflicht, Datenschutzrichtlinien bereit zu halten. Auf Landesebene verpflichtet etwa Kalifornien Unternehmen, die ihren Sitz in Kalifornien haben oder personenbezogene Daten von kalifornischen Bewohnern sammeln, dazu, eine Datenschutzrichtlinie zu erstellen.[923] Die Kompetenzen der FTC unter

---

920 Novartis Corp. v. FTC, 223 F.3d 783, 786 (D.C. Cir. 2000).

921 Bildstein v. MasterCard Int'l Inc, 329 F. Supp. 2d 410, 414 (S.D.N.Y. 2004).

922 *FTC*, Privacy Online: Fair Information Practices. A Report to Congress, abrufbar unter https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (abgerufen am 13.10.2017).

923 California Business and Professions Code, Division 8, Chapter 22.1, Section 22575 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

dem FTCA sind umstritten.[924] So wurde argumentiert, dass die FTC gar nicht gegen Websitebetreiber vorgehen könne, die keine Datenschutzrichtlinien bereitstellen, da dann den Nutzern keine falschen Angaben gemacht würden.[925]

Faktisch geht die FTC trotz ungeklärter Kompetenzen gegen Datenschutzverstöße vor. Dabei ergibt sich aus einer Gesamtschau der Fälle, dass die FTC hauptsächlich gegen große Unternehmen vorzugehen scheint,[926] allerdings mit durchaus wirkungsvollen und empfindlichen Bußgeldern in Millionenhöhe.[927] Bußgelder in solcher Höhe sind dem deutschen Datenschutzrecht, das gem. § 43 Abs. 3 BDSG Bußgelder bis zu 300.000 € vorsieht,[928] bislang fremd. Die FTC geht damit härter gegen Datenschutzverstöße vor als deutsche Aufsichtsbehörden und Gerichte.

c) Einwilligung nach den fair information practice-Grundsätzen

Schließlich ist noch ein Augenmerk auf die Anforderungen der Einwilligung nach den fair information practice-Grundsätzen zu legen. In den dargestellten Bundesgesetzen finden sich keine den europäischen Vorgaben

---

924 Vgl. etwa die Fälle FTC v. Wyndham Worldwide Corp., *FTC*, Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk, abrufbar unter https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment (abgerufen am 13.10.2017); LabMD v. FTC, LabMD, Inc. v. Federal Trade Commission, Case-No. 16-16270, abrufbar unter https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-v-federal-trade-commission (abgerufen am 13.10.2017)*; Reidenberg*, 38 Hous. L. Rev. 717, 740 ff. für einen Überblick über die Kompetenzen der FTC hinsichtlich der Safe Harbor-Regelungen.

925 *Schwartz*, 52 Vand. L. Rev. 1607, 1638; *Kühnl,* Persönlichkeitsschutz 2.0, S. 257 m. w. N.

926 vgl. *FTC*, Enforcing Privacy Promises, abrufbar unter https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (abgerufen am 13.10.2017) für einen aktuellen Überblick der Maßnahmen der FTC gegen verschiedene Unternehmen.

927 So zahlte *Apple* in einem Settlement etwa 22,5 Mio. USD, *FTC*, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, abrufbar unter https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (abgerufen am 13.10.2017).

928 Gem. § 43 Abs. 3 S. 2 BDSG könnten allerdings höhere Bußgelder verhängt werden.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

ähnliche Anforderungen an die Einwilligung. Nach den fair information practice-Grundsätzen sollen die Verbraucher einwilligen können, ob und wie personenbezogene Daten über den Zweck hinaus, für den sie bereitgestellt wurden, verwendet werden dürfen.[929] Es handelt sich dabei also um eine Einwilligung in die Zweckänderung nach europäischem Verständnis. In der Literatur werden jedoch zusätzlich die Voraussetzungen der Informiertheit und teilweise auch der Freiwilligkeit diskutiert.[930] Insbesondere das Problem der (fehlenden) Informiertheit ist Gegenstand der Forschung,[931] da sie als „notice" Bestandteil der genannten Grundsätze ist.

Anders als nach europäischem Recht ist die Einwilligung aber nicht bei Nichtvorliegen der Voraussetzungen ex tunc nichtig. Vielmehr handelt es sich, abgesehen vom Einwilligungserfordernis durch die Eltern unter COPPA, um ein Instrument zur Selbstregulierung.[932] Daher gestaltet sich die Durchsetzung bei fehlenden inhaltlichen Voraussetzungen der Einwilligung im US-amerikanischen Datenschutzrecht als schwierig.[933]

---

929 *FTC*, Privacy Online: Fair Information Practices. A Report to Congress, abrufbar unter https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (abgerufen am 13.10.2017), S. 4.

930 *Sloan/Warner*, Beyond Notice and Choice: Privacy, Norms, and Consent, abrufbar unter http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1567&context=fac_schol (abgerufen am 13.10.2017), S. 7 ff.

931 Vgl. etwa *Sloan/Warner*, Beyond Notice and Choice: Privacy, Norms, and Consent, abrufbar unter http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1567&context=fac_schol (abgerufen am 13.10.2017); *Barocas/Nissenbaum*, On Notice: The Trouble with Notice and Consent, abrufbar unter http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf (abgerufen am 13.10.2017); *Strahilevitz/Kugler*, Is Privacy Policy Language Irrelevant to Consumers?, 45 J. Legal Stud. S69.

932 *Schwartz/Solove*, Notice and Choice:Implications for Digital Marketing to Youth, abrufbar unter http://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf (abgerufen am 13.10.2017), S. 2.

933 *Schwartz/Solove*, Notice and Choice:Implications for Digital Marketing to Youth, abrufbar unter http://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf (abgerufen am 13.10.2017), S. 2.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

4. Weitere datenschützende Normen

a) Computer Fraud and Abuse Act

Der Computer Fraud and Abuse Act (im Folgenden: CFAA) bestraft u. a. den vorsätzlichen Zugriff auf einen Computer und Erhalt von Informationen von einem geschützten Computer, 18 U.S.C. § 1030 (a)(2)(C), sowie die vorsätzliche Übermittlung von Programmen, Informationen u. a. und den vorsätzlichen unerlaubten Zugriff auf einen geschützten Rechner, wenn hierdurch vorsätzlich Schaden und Verlust verursacht wurde, 18 U.S.C. § 1030 (a)(5)(A),(C), oder, in den Fällen des § 1030 (a)(5)(B), grob fahrlässig ein Schaden verursacht wurde. Schaden bedeutet gem. 18 U.S.C. § 1030 (e)(8) eine Beeinträchtigung der Integrität oder Verfügbarkeit von Daten, eines Programms, Systems oder Informationen; Verlust ist gem. § 1030 (e)(11) definiert als jede Art von Kosten, die mit dem Verstoß gegen die Norm einhergehen. Als zusätzliche Voraussetzung für zivilrechtliche Klagen muss unter dem CFAA ein wirtschaftlicher Schaden eine Höhe von 5.000 USD innerhalb eines Jahres erreichen, 18 U.S.C. § 1030 (g) i. V. m. 18 U.S.C. § 1030 (c)(4)(A)(i)(I). Dabei ist es aufgrund der immateriellen Natur von Datenschutzrechtsverletzungen schwierig für den Kläger, eine Schadenszufügung in dieser Höhe nachzuweisen. Auch tatsächliche Beeinträchtigungen der Funktionalität der Nutzersysteme oder Nutzerrechner erfüllen die Anforderungen der Norm regelmäßig nicht.[934]

Der CFAA ist damit kein vielversprechender Ansatzpunkt für ein Vorgehen gegen das Platzieren von Tracking Tools oder die Weitergabe von Daten.

---

934 Als nichtausreichend wurden u. a. angesehen: Beanstandung einer generellen Beeinträchtigung der Funktionalität des Rechners, Bose v. Interclick, Inc., No. 10 Civ. 9183 (DAB), 2011 WL 4343517, 3 f. (S.D.N.Y. August 17, 2011); Unterbrechung von Dateienübertragungen, Fink v. Time Warner Cable, No. 08 Civ. 9628 (LTS)(KNF), 2009 WL 2207920, 4 (S.D.N.Y. July 23, 2009); Bereinigung des Computers von Cookies und sowie wirtschaftlicher Wert der Daten zur Verwendung für Werbeschaltung, In re Doubleclick Privacy Litigation, 154 F.Supp.2d 497, 524 (S.D.N.Y. 2001); Verlangsamte Funktionalität eines Mobilfunktelefons durch Erhalt unerwünschter SMS, Czech v. Wall St. on Demand, Inc., 674 F.Supp.2d 1102, 1114 ff. (D. Minn. 2009).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Regelungen für Kinder: Children's Online Privacy Protection Act

> „(a) Acts prohibited.
>
> In general. It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b). […]"[935]

Der Children's Online Privacy Protection Act[936] (im Folgenden: COPPA) schützt bestimmte personenbezogene Daten von Kindern, indem er unter anderem Websitebetreibern auferlegt, auf ihrer Website, wenn sie sich an Kinder unter 13 Jahren richtet, anzugeben, welche Informationen über die Kinder gesammelt werden und in welcher Art diese üblicherweise weitergegeben werden und dass die Eltern in das Sammeln, Nutzen und Weitergeben dieser Informationen einwilligen.

Allerdings ist der überwiegende Teil der sozialen Netzwerke nicht ausdrücklich an Kinder unter 13 Jahren gerichtet. Die Regelungen des COPPA richten sich jedoch gem. 15 U.S.C. § 6502 (a)(1) nur an „[…] an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, […]". Gem. der Definition aus 15 U.S.C. § 6501 (10)(A) bedeutet "[…] directed to children […]", dass die Seite auf Kinder unter 13 Jahren gezielt ausgerichtet sein muss oder jedenfalls Teile der Seite gezielt auf Kinder ausgerichtet sein müssen. Bei der Bewertung sollen Faktoren wie die Nutzung von animierten Charakteren, Musik oder das Alter von Modellen in Betracht gezogen werden, 16 C.F.R. § 312.2 (1). Zudem soll die Regelung keine Anwendung auf Websites finden, die vor der Eingabe des Alters keine personenbezogene Daten sammeln, 16 C.F.R. § 312.2 (3). In einer Antwort auf die häufigsten Fragen stellt die FTC zudem klar, dass COPPA von sog. „general audience websites", also Websiten, die auf ein bestimmtes Publikum ausgerichtet sind, nicht verpflichtet werden, das Alter der Besucher abzufragen und COPPA nur dann greift, wenn der Websitebetreiber tatsächliches Wissen davon erhält, dass ein Besucher unter 13 Jahre ist.[937]

Die Regelungen des COPPA erinnern damit an Art. 8 Abs. 1 DSGVO, bleiben aber in ihrer Schutzwirkung hinter dieser Regelung zurück. [938]

---

935 15 U.S.C. § 6502 (a)(1).

936 15 U.S.C. § 6501 ff.

937 *FTC*, Complying with COPPA: Frequently Asked Questions, abrufbar unter https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Audience (abgerufen am 13.10.2017).

938 Vgl. Kap. 3 Pkt. B.II.3, S. 194.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

II. Datenschutzrechtliche Bestimmungen im Nutzer-Nutzer-Verhältnis

Fraglich ist, welche Ansprüche den Nutzern von sozialen Netzwerken gegen andere Nutzer bei Datenschutzrechtsverstößen zur Verfügung stehen. Denkbar wäre etwa das Hochladen von Informationen oder Bildern Anderer auf dem eigenen Profil oder die Weitergabe von Informationen, die ein Nutzer auf seinem Profil geteilt hat an Personen außerhalb des Netzwerks.

1. Public disclosure of private facts[939]

> „One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
> (a) would be highly offensive to a reasonable person, and
> (b) is not of legitimate concern to the public."[940]

Der *public disclosure of private facts*-Anspruch gibt den Geschädigten einen Anspruch gegen die Veröffentlichung von Informationen, die die Privatsphäre betreffen. Von Interesse könnte dieser Anspruch sein, wenn die Plattform eines sozialen Netzwerks genutzt wird, um private Dinge von Anderen zu veröffentlichen, etwa bei dem durchaus üblichen Hochladen von Fotos anderer Nutzer ohne deren vorherige ausdrückliche Einwilligung oder bei dem Posten von Fakten über einen Anderen. Auch hier ist aus der Sicht eines objektiven Beobachters zu bewerten, ob die Veröffentlichung der Information anstößig ist. Ferner dürfen diese Dinge nicht von Belang für die Öffentlichkeit sein. Das Merkmal des „Öffentlichmachens" ist erfüllt, wenn die private Information einem größeren Publikum zugänglich gemacht wurde oder so vielen Leuten, dass es wahrscheinlich ist, dass die Information öffentlich wird.[941] Dies gilt etwa für die Verbreitung einer Information in einem Schaufenster eines kleinen Ladens.[942] Somit ist fraglich,

---

939 In Betracht kommen ferner auch hier die torts intrusion upon seclusion und appropriation of name or likeness nach den oben dargelegten Maßstäben. Der vierte tort, „false light", wird vorliegend nicht besprochen, da es sich hierbei mehr um ein persönlichkeitsschützenden als datenschutzrechtlichen Anspruch handelt, *The American Law Institute,* Restatement of the Law Second, Torts, § 652E.

940 *The American Law Institute,* Restatement of the Law Second, Torts, § 652D.

941 *The American Law Institute,* Restatement of the Law Second, Torts, § 652D, comment a.

942 *The American Law Institute,* Restatement of the Law Second, Torts, § 652D, comment a, illustration 2.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

was für die Verbreitung auf einem Profil gilt. Einerseits sind Profile klassischerweise nur einem begrenzten Personenkreis zugänglich; allerdings kann dieser Personenkreis je nach Nutzer vierstellige Ausmaße annehmen. Damit würde die Information unter Umständen mehr Personen zugänglich gemacht als bei einem Aushang in einem Schaufenster eines kleinen Ladens. Allerdings unterscheidet sich der Aushang von dem Profil dahingehend, dass bei dem Aushang im Schaufenster jeder potentiell die Möglichkeit hätte, die Information wahrzunehmen, während die Information auf dem Profil beschränkt ist. So wurde in einem Fall etwa das Öffentlichmachen von Informationen auf einem Profil eines sozialen Netzwerks bejaht, auch wenn geschätzt nur sechs Menschen die Information wahrgenommen haben. Allerdings war das entsprechende Profil nicht durch entsprechende Aktivierung von Funktionen für die Öffentlichkeit verborgen.[943] Letztlich wird das Öffentlichmachen einer Einzelfallentscheidung unterliegen, wobei die Entscheidung davon abhängig gemacht werden muss, wie vielen Leuten die Information tatsächlich zugänglich war und ob darauf basierend eine weitergreifende Verbreitung der Information wahrscheinlich ist.

Ferner müsste die Information auch privat i. S. d. Norm sein. Privat sind jedenfalls keine Fotos von vollständig bekleideten Personen, die in der Öffentlichkeit aufgenommen werden.[944] Es muss sich damit um Bilder oder Informationen handeln, die eindeutig privat sind.

Hinzu kommend muss die öffentlich gemachte Information nach objektiven Maßstäben anstößig sein. Dieses Merkmal ist von gesellschaftlichen Gepflogenheiten abhängig und wandelbar. Das bloße Posten von wahren Informationen kann nicht darunter fallen, auch wenn der Andere sie gerne geheim gehalten hätte, wie etwa das Datum seiner Hochzeit.[945]

Der Anspruch erweist sich folglich nur dann als wirkungsvoll, wenn eine eindeutig private Information, die darüber hinaus objektiv als anstößig empfunden wird, auf einem Profil veröffentlich wird. Das Hochladen von gewöhnlichen Fotos oder Informationen anderer fällt damit nicht unter diesen Anspruch.

---

943 Yath v. Fairview Clinics, N. P., 767 N.W.2d 34, 43 f. (Minn. Ct. App. 2009).

944 *The American Law Institute,* Restatement of the Law Second, Torts, § 652D, comment b.

945 *The American Law Institute,* Restatement of the Law Second, Torts, § 652D, comment c.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

2. Stored Communications Act

Ein Anspruch unter dem SCA aufgrund von einem Zugriff auf Informationen in einem Profil und der anschließenden Weitergabe von Informationen an Dritte außerhalb des Netzwerks wird schon an der Voraussetzung scheitern, dass ein Profil keine Einrichtung i. S. d. 18 U.S.C. § 2701 (1)(a) ist.[946] Selbst wenn man davon ausginge, dass das Merkmal der Einrichtung i. S. d. Norm erfüllt ist, da durch die Profile der Dienst des sozialen Netzwerks angeboten wird, wären andere Nutzer, sofern die Informationen ihnen durch die entsprechenden Einstellungen des sozialen Netzwerks zugänglich sind, berechtigt, auf diese Informationen zuzugreifen und diese weiterzugeben, 18. U.S.C. § 2701 (c)(2).[947] Auch ein Anspruch gem. 18 U.S.C. § 2702 (a)(1) kommt nicht in Betracht, da Nutzer eines sozialen Netzwerks keine Anbieter eines elektronischen Kommunikationsdienstes sind.

III. Zusammenfassung

Das einfachgesetzliche US-amerikanische Datenschutzrecht folgt einem grundsätzlich anderen Ansatzpunkt als das europäische Datenschutzrecht. Statt eines grundsätzlichen Verbots jeglicher Verarbeitung personenbezogener Daten ist die Verarbeitung personenbezogener Daten grundsätzlich erlaubt und nur teilweise begrenzt.

Die Durchsetzbarkeit der Normen, soweit sie anwendbar sind, wird durch die Möglichkeit der einseitigen Einwilligung in die Datenverarbeitung durch den Datenverarbeiter selbst begrenzt. Ebenso wenig bietet das Deliktsrecht hinreichenden Schutz personenbezogener Daten, da die von den Gerichten aufgestellten Maßstäbe einen sehr starken Datenschutzeingriff fordern.

Diesem „Minus" an datenschützenden Regelungen steht das Vorgehen der FTC gegen Plattformbetreiber, die irreführende Maßnahmen mit den Daten der Nutzer vornehmen, gegenüber. Zwar erfolgt dieses Vorgehen nur punktuell gegen große Plattformbetreiber, dafür aber mit empfindlichen Strafen, die dem deutschen Datenschutzrecht bislang fremd sind. Hier lässt sich also sogar ein stärkerer Vollzug gegen zweifelhafte Geschäftsmodelle beobachten als diesseits des Atlantiks.

---

946 Kap. 4 Pkt. B.I.1.b.aa.i, S. 260.

947 Ehling v. Monmouth-Ocean Hospital Service Corporation, 961 F.Supp.2d 659, 670 (D.N.J. 2013).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

C. Datentransfer in die USA

Nach der Konzeption der DSRL sowie der DSGVO bilden die EU und der EWR einen datenschutzrechtlichen Binnenraum, in dem personenbezogene Daten frei fließen können (vgl. Art. 1 Abs. 2 DSRL; Art. 1 Abs. 3 DSGVO).[948] Sollen personenbezogene Daten jedoch die „Datenburg" Europa verlassen, ist dies nur unter den besonderen Voraussetzungen der Art. 25 f. DSRL bzw. Art. 44 ff. DSGVO möglich. Dies betrifft auch die Betreiber großer sozialer Netzwerke, die die Daten ihrer Nutzer von der EU in die USA transferieren.[949] Im Folgenden wird auf die Vorgaben der DSRL und der DSGVO unter ihrer Interpretation durch den *EuGH* eingegangen (dazu I.), bevor der Datentransfer in die USA dargestellt wird (dazu II.). Hierbei wird insbesondere auf die nach den vom *EuGH* ungültig erklärten[950] Safe Harbor-Grundsätze[951] sowie deren Nachfolger, das EU-U.S.-Privacy Shield[952], einzugehen sein.

I. Die Angemessenheit des Schutzniveaus

Wie dargestellt, folgt das Datenschutzrecht in den USA einem ganz anderen Ansatz als das Datenschutzrecht in der EU. Voraussetzung für die Zulässigkeit der Übermittlung von personenbezogenen Daten in ein Drittland ist gem. Art. 25 Abs. 1 DSRL jedoch, dass das Drittland ein „angemessenes" Schutzniveau gewährleistet. Das Vorliegen des angemessenen Schutzniveaus kann die Kommission i. S. d. Art. 25 Abs. 6 i. V. m. Art. 31 Abs. 2 DSRL feststellen. Liegt kein angemessenes Schutzniveau vor, muss auf die Ausnahmeregelungen des Art. 26 DSRL zurückgegriffen werden. Eine

---

948 *Kühling/Seidel/Sivridis,* Datenschutzrecht, S. 37 ff.

949 Vgl. etwa *Facebook Inc.,* Facebook Inc. and the EU-U.S. Privacy Shield, abrufbar unter https://www.facebook.com/about/privacyshield (abgerufen am 13.10.2017); *Snap Inc.,* Datenschutzbestimmungen, abrufbar unter https://www.snap.com/de-DE/privacy/privacy-policy (abgerufen am 13.10.2017).

950 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems.

951 Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des "sicheren Hafens" und der diesbezüglichen "Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, K (2000) 2441, Abl.EG 2000 L, 7.

952 C(2016) 4176, ABl.EU 2016 L 207, 1.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Ausnahme vom Angemessenheitserfordernis stellt etwa die Einwilligung durch den Betroffenen dar, Art. 26 Abs. 1 lit. a DSRL.

Die DSGVO verlangt ebenfalls ein angemessenes Schutzniveau im Drittland des Empfängers, das die Kommission gem. Art. 45 Abs. 1 DSGVO feststellen kann. Ausnahmen hiervon finden sich in Art. 46 f. DSGVO sowie Art. 49 DSGVO.

Die Frage, wie der Angemessenheitsbegriff zu definieren ist, wurde in der Literatur bis zur *Schrems*-Entscheidung des *EuGH*[953], in dem dieser die Safe Harbor-Entscheidung der Kommission für ungültig erklärte, stark diskutiert. Dabei ging es um die Frage, ob ein gleichwertiges Datenschutzniveau verlangt werden soll,[954] oder eines, das dem Kernbestand der DSRL gerecht werden soll.[955] Einigkeit bestand jedoch dahingehend, dass keine Deckungsgleichheit gefordert ist.[956]

1. Auslegung durch den *EuGH*

Im Fall *Schrems* zur Safe Harbor-Entscheidung der Kommission befasste sich der *EuGH* mit dem Angemessenheitsbegriff. Nach Ansicht des *EuGH* müsse das Schutzniveau im Drittland zwar nicht identisch, jedoch „[…] der Sache nach gleichwertig […]" sein.[957] Sekundärrechtlich macht der *EuGH* dieses Erfordernis an dem Wortlaut des Art. 25 Abs. 6 DSRL fest, nachdem das Drittland das angemessene Schutzniveau „gewährleistet" und zwar „[…] hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen […]".[958] Zudem verankert der *EuGH* diese Argumentation primärrechtlich in der GrCh: Art. 25 Abs. 6 DSRL setze die in Art. 8 Abs. 1 GrCh ausdrücklich vorgesehene Pflicht zum Schutz personenbezogener Daten um. Damit soll die Norm den „[…] Fortbestand des hohen Niveaus dieses Schutzes im Fall der Übermittlung personenbezogener Daten in ein Drittland gewährleisten."[959]

---

953 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems.
954 *Simitis*, BDSG, § 4b Rn. 52.
955 *Klug/Körffer/Gola*, in: Gola/Schomerus, BDSG, § 4b Rn. 12; *Däubler*, in: DKWW, BDSG, § 4b Rn. 12; Gabel, in: Taeger/Gabel, BDSG, § 4b Rn. 21.
956 *Simitis*, BDSG, § 4b Rn. 52.
957 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 73 – Schrems.
958 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 73 – Schrems.
959 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 72 – Schrems.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

2. Konsequenzen der Auslegung durch den *EuGH*

Mit dieser Argumentation wird der Einschätzungsspielraum der Kommission bei der Beurteilung der Angemessenheit des Schutzniveaus, der in Art. 25 Abs. 2, 6 DSRL angelegt ist, stark beschränkt.[960] Gleichzeitig gibt der *EuGH* aber keine klar definierten Parameter vor, wann das Schutzniveau als gleichwertig (aber noch nicht identisch) gilt.

Eine allzu einseitige Fokussierung auf die Grundrechte aus Art. 7, 8 GrCh versperrt jedoch möglicherweise der Abwägung mit widerstreitenden, letztlich ebenso grundrechtlich verankerten Interessen, den Weg. Diese in Sachverhalten zwischen Privaten nicht unproblematische Bevorzugung des Schutzes personenbezogener Daten lässt damit einerseits das Recht auf informationelle Selbstbestimmung der Betroffenen und andererseits die Verarbeiterinteressen außer Acht.[961] Zudem ist diese Interessenabwägung auch sekundärrechtlich durch die DSRL vorgegeben: So weist etwa EG 56 DSRL auf die Bedeutsamkeit des grenzüberschreitenden Datenverkehrs für den internationalen Handel hin.

3. Beurteilungsmaßstab der DSGVO

Die DSGVO konkretisiert die in der DSRL angelegten und recht pauschalen Kriterien zur Bewertung der Angemessenheit i. S. d. Art. 25 Abs. 2 DSRL. So sieht Art. 45 Abs. 2 DSGVO diverse Bewertungskriterien vor, wie etwa wirksame Betroffenenrechte i. S. d. Art. 45 Abs. 2 lit. a DSGVO, die Existenz unabhängiger Aufsichtsbehörden im Drittland i. S. d. Art. 45 Abs. 2 lit. b DSGVO, oder die vom betreffenden Drittland eingegangenen internationalen Verpflichtungen in Bezug auf den Schutz personenbezogener Daten i. S. d. Art. 45 Abs. 2 lit. c DSGVO. Gleichwohl zeigt ein Vergleich mit den Vorgaben der DSRL, dass die DSGVO hier keine grundsätzlich neuen Maßstäbe zur Bewertung der Angemessenheit des Schutzniveaus aufstellen will, sondern die Maßstäbe der DSRL lediglich näher ausdifferenziert. So gleicht etwa Art. 45 Abs. 2 lit. a DSGVO dem knapperen, aber in der Sache ähnlichen Art. 25 Abs. 2 DSRL, während Art. 45 Abs. 2 lit. c DSGVO teilweise dieselben Kriterien aufstellt wie bereits Art. 25 Abs. 6 DSRL. Für die

960 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 78 – Schrems.

961 Dazu kritisch *Kühling/Heberlein*, NVwZ 2016, 7, 9.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Bewertung der Angemessenheit des Schutzniveaus eines Drittlands stellt die DSGVO damit keinen grundsätzlich neuen Maßstab auf.

II. Regelungen für den Transfer in die USA

Liegt kein Angemessenheitsbeschluss vor, so kann der Datentransfer etwa auf Grundlage von Standardvertragsklauseln (Art. 26 Abs. 4 DSRL bzw. Art. 46 Abs. 2 lit. c DSGVO) oder verbindlicher interner Datenschutzvorschriften (Art. 26 Abs. 2 DSRL bzw. Art. 47 DSGVO) oder aufgrund der Einwilligung des Betroffenen (Art. 26 Abs. 1 lit. a DSRL bzw. Art. 49 Abs. 1 S. 1 lit. a DSGVO) erfolgen. Für den Transfer in die USA wurden zusätzlich besondere Regelungen geschaffen. Vom Jahr 2000 bis zum Jahr 2015 konnten Datentransfers in die USA auf Grundlage der Safe Harbor-Entscheidung durch die Kommission stattfinden. Die Safe Harbor-Entscheidung stellte an sich keine Entscheidung über die Angemessenheit des Schutzniveaus in den USA dar; vielmehr bezog sich die Angemessenheit nur auf die am Safe Harbor-Programm teilnehmenden Organisationen.[962] Nach dem *Schrems*-Urteil des *EuGH*, in dem der *EuGH* die Grundsätze für ungültig erklärte, hat die Kommission gemeinsam mit dem US-amerikanischen Department of Commerce das EU-U.S.-Privacy Shield erarbeitet, das seit Juli 2016 in Kraft ist. Diese „Sonderregelungen" entfalten besondere Relevanz, da sie die Legitimationsgrundlage für die Datenübermittlung von der EU in die USA durch zahlreiche namenhafte US-amerikanische Unternehmen bilden. So nahmen Betreiber sozialer Netzwerke wie *Facebook*, *Twitter* oder *Snapchat* bereits an dem Safe Harbor-Programm[963] teil und haben sich nunmehr auch den Prinzipien des EU-U.S.-Privacy Shield[964] unterworfen.

962 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 83 – Schrems; *Borges*, NJW 2015, 3617, 3618; *Petri*, DuD 2015, 801.

963 Vgl. *Department of Commerce,* U.S.-EU Safe Harbor List, abrufbar unter https://safeharbor.export.gov/list.aspx (abgerufen am 13.10.2017) und *Twitter Inc.,* Twitter Datenschutzrichtlinie, abrufbar unter https://twitter.com/privacy/previous/version_10?lang=de (abgerufen am 13.10.2017).

964 *Department of Commerce,* Privacy Shield List, abrufbar unter https://www.privacyshield.gov/list (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

1. Safe Harbor-Entscheidung der Kommission

a) System der Selbstzertifizierung

Die Safe Harbor-Grundsätze funktionierten nach dem Selbstzertifizierungsprinzip: Unternehmen, die an dem Programm teilnehmen wollten, mussten dem US-amerikanischen Department of Commerce ein Schreiben mit grundsätzlichen Informationen zum Unternehmen und dem Umgang mit personenbezogenen Daten von EU-Bürgern sowie näheren Informationen zur Umsetzung der Safe Harbor-Grundsätze zukommen lassen. Seit Inkrafttreten der Entscheidung bis zu ihrer Ungültigkeitserklärung war der Missbrauch des Selbstzertifizierungsvorgangs über drei Duzend mal Gegenstand von Maßnahmen der FTC gegen Unternehmen, die sich fälschlicherweise als Teilnehmer am Safe Harbor-Programm ausgaben.[965] Eine Studie aus dem Jahr 2013 zeigte jedoch, dass die tatsächliche Anzahl von falsch zertifizierten Unternehmen wohl deutlich höher lag.[966] Das Handelsministerium veröffentlichte eine Liste von teilnehmenden Unternehmen,[967] ohne Garantie für die Richtigkeit und Vollständigkeit der Liste oder die Übereinstimmung der Angaben der Unternehmen zur Teilnahme an dem Safe Harbor-Programm zu übernehmen.[968] Zudem sollten Mitteilungen über fortgesetzte Verstöße in die Liste aufgenommen werden – gem. FAQ 11 der Grundsätze allerdings nur aufgrund einer Meldung der Unternehmen selbst, oder aufgrund der Meldung von Selbstregulierungs- oder staatliche Kontrollorganen. Da die Grundsätze aber dem Wortlaut nach weder für die FTC noch die Selbstregulierungsorgane eine Pflicht zur Überwachung der Einhaltung der Safe Harbor-Grundsätze vorsahen,[969] beruhte der Inhalt dieser Liste beinahe ausschließlich auf den Angaben der Unternehmen selbst.

---

965 Vgl. *FTC*, U.S.-EU Safe Harbor compliance: Don't run aground, abrufbar unter https://www.ftc.gov/news-events/blogs/business-blog/2015/08/us-eu-safe-harbor-compliance-dont-run-aground (abgerufen am 13.10.2017).

966 Vgl. *Galexia*, EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance, abrufbar unter http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf (abgerufen am 13.10.2017), S. 4.

967 *Department of Commerce,* U.S.-EU Safe Harbor List, abrufbar unter https://safeharbor.export.gov/list.aspx (abgerufen am 13.10.2017).

968 *Department of Commerce,* U.S.-EU Safe Harbor List, abrufbar unter https://safeharbor.export.gov/list.aspx (abgerufen am 13.10.2017).

969 Vgl. K (2000) 2441, Abl.EG 2000 L, 7, FAQ 11: „Hat die FTC Grund zu der Annahme, dass ein solcher Verstoß vorliegt, *kann* [Hervorh. durch die Verf.] sie

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Grundsätze und Ungültigkeit

Die in Anhang I der Entscheidung festgelegten Grundsätze umfassten Informationspflichten, Regelungen über die Wahlmöglichkeit zur Verarbeitung personenbezogener Daten, über die Weitergabe von personenbezogenen Daten, deren Sicherheit, zur Datenintegrität, Auskunftsrechte und Regelungen zur Durchsetzbarkeit der Safe Harbor-Grundsätze. Die Grundsätze wurden in der deutschen Literatur als unzureichend kritisiert. So wurde der Zweckbindungsgrundsatz nur im Wege eines „opt-outs" in die Grundsätze eingebunden und damit vom Regelfall zur Ausnahme verkehrt.[970]

Der *EuGH* erklärte die Safe Harbor-Entscheidung im Oktober 2015 für ungültig.[971] Maßgeblich waren dafür weniger die materiellen Grundsätze als die weitreichenden Ausnahmen von ihrer Gültigkeit.[972] Denn die Grundsätze galten nur für Unternehmen, die sich selbst zertifizierten, und entfalteten keine Wirkung gegenüber Behörden.[973] Hinzu kamen die Möglichkeiten, die Gültigkeit der Grundsätze zu „[…] Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen […]" i. S. d. Anhang I, Abs. 4 der Safe Harbor-Entscheidung zu begrenzen.[974] Außerdem beanspruchte gem. Anhang IV, Abschnitt B der Safe Harbor-Entscheidung US-amerikanisches Recht Vorrang vor den Safe Harbor-Grundsätzen.[975] Der *Gerichtshof* bemängelte zudem die Durchsetzungsmöglichkeiten der Grundsätze. So legte die Safe Harbor-Entscheidung weder fest, ob US-amerikanisches Recht Möglichkeiten zur Begrenzung von Eingriffen in Grundrechte vorsieht, noch ob gegen solche Eingriffe wirksamer Rechtsschutz bestünde.[976] Eine Regelung, die aber den generellen Zugriff durch Behörden auf personenbezogene Daten vorsehe, ver-

---

eine behördliche Anordnung erwirken, die die beanstandete Praxis untersagt, oder sie *kann* [Hervorh. durch die Verf.] vor einem Bezirksgericht klagen.".

970 Simitis, BDSG, § 4b, Rn. 73.

971 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650 – Schrems.

972 Ausführlich *Kühling/Heberlein*, NVwZ 2016, 7, 9 ff.

973 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 82 – Schrems.

974 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 84 – Schrems.

975 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 85 f. – Schrems.

976 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 88 ff. – Schrems.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

stoße gegen den Wesensgehalt des Art. 7 GRCh und eine Regelung, die keinen Rechtsbehelf auf Zugang und Löschung der Daten vorsieht, verstoße gegen den Wesensgehalt des Art. 47 GrCh.[977]

Über die Angemessenheit des Schutzniveaus in den USA traf der *EuGH* indes keine Aussage.[978]

2. EU-U.S.-Privacy Shield

Nach der *Schrems*-Entscheidung des *EuGH* waren Datentransfers auf Grundlage der Safe Harbor-Entscheidung der Kommission unzulässig. Die Kommission erarbeitete daher gemeinsam mit dem US-amerikanischen Department of Commerce den EU-U.S.-Privacy Shield als Nachfolger der Safe Harbor-Grundsätze.

a) Grundsätze

Das EU-U.S.-Privacy Shield bietet in materieller Sicht keine grundsätzlichen Neuerungen gegenüber den Safe Harbor-Grundsätzen. Das System beruht weiterhin auf dem Selbstregulierungsprinzip,[979] wobei die Schritte zur Selbstzertifizierung denen zu Safe Harbor ähnlich sind.[980] Die Grundsätze decken sich in den Grundzügen mit denen der Safe Harbor Entscheidung: Vorgesehen sind Regelungen zur Informationspflicht, Datenintegrität, Wahlmöglichkeit, Sicherheit, Auskunftsrecht, Weitergabe und der Durchsetzung. In der Ausgestaltung unterscheiden sich die Grundsätze jedoch teilweise. So ist der Zweckbindungsgrundsatz nun ausdrücklich erwähnt, allerdings weiterhin im Wege eines „opt-out".[981]

977 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 94 f. – Schrems.

978 *Kühling/Heberlein*, NVwZ 2016, 7, 9; *Piltz*, K&R 2016, 1, 2; *Moos/Schefzig*, CR 2015, 625, 630.

979 C(2016) 4176, ABl.EU 2016 L 207, 1, Rn. 14.

980 *Department of Commerce*, Privacy Shield Program, abrufbar unter https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 (abgerufen am 13.10.2017).

981 C(2016) 4176, ABl.EU 2016 L 207, 1, Rn. 21 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

b) Kritische Würdigung der Änderungen durch das EU-U.S.-Privacy Shield

Der *EuGH* hatte die weitreichenden Ausnahmen in den Safe Harbor-Grundsätzen und den potentiellen Zugriff durch Behörden sowie fehlenden Rechtsschutz gegen diesen Zugriff bemängelt. Diese Lücken versucht das EU-U.S.-Privacy Shield mit einer Reihe von Maßnahmen zu schließen.

aa) Ausnahmen vom EU-U.S.-Privacy Shield und Begrenzung behördlicher Zugriffe

Hinsichtlich der weitreichenden Ausnahmen von den Grundsätzen lässt sich konstatieren, dass sich diese auch im EU-U.S.-Privacy Shield finden.[982] Der behördliche Zugriff auf Daten wird nunmehr zwar durch die Presidential Policy Directive-28 (PPD-28) auf bestimmte Zwecke begrenzt.[983] Allerdings wird ihre Wirkung wegen der schnellen Änderbarkeit – insbesondere hinsichtlich eines neuen amtierenden US-Präsidenten – und fehlender einklagbarer Rechte in Frage gestellt.[984]

bb) Wirksame Rechtsbehelfe

Auch finden sich weiterhin keine wirksamen Rechtsbehelfe gegen behördliche Zugriffe. Zwar zählt der Durchführungsbeschluss der Kommission in Frage kommende Rechtsbehelfe auf: So nennt er Rechtsbehelfe aus dem Foreign Intelligence Surveillance Act (FISA), dem Freedom of Information Act (FOIA) oder dem ECPA,[985] geht jedoch ebenso auf die Schwierigkeiten der Rechtsdurchsetzung ein.[986] Hierfür muss der Betroffene nämlich seine Klagebefugnis darlegen können, was voraussetzt, dass er einen Zugriff auf seine Daten nachweisen kann (sog. standing).[987]

---

982 *Weichert*, ZD 2016, 209, 216 m. w. N.
983 C(2016) 4176, ABl.EU 2016 L 207, 1, Anhang VI, Pkt. I.b.
984 *Schröder*, in: Kühling/Buchner, DSGVO, Art. 45, Rn. 43.
985 C(2016) 4176, ABl.EU 2016 L 207, 1, Rn. 116.
986 C(2016) 4176, ABl.EU 2016 L 207, 1, Rn. 115.
987 Vgl. etwa Clapper v. Amnesty International USA, 133 S. Ct. 1138, 1147 ff. – Clapper v. Amnesty International USA; vgl. *Kühling/Heberlein*, NVwZ 2016, 7, 11 m. w. N.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Aus diesem Grund[988] sieht das EU-U.S.-Privacy Shield die Installation einer unabhängigen[989] Ombudsperson vor, deren Aufgabe die Prüfung von Beschwerden ist. Betroffene können sich dabei an zuständige Kontrollstellen ihres Mitgliedstaates wenden. Die Einreichung des Antrags bei der Ombudsperson erfolgt durch eine zentrale EU-Stelle.[990] Die Ombudsperson soll mit Prüfungsbefugnissen ausgestattet sein und bestätigen, dass US-amerikanische Rechtsvorschriften eingehalten wurden oder dass die Verstöße beseitigt wurden. Allerdings wird durch die Ombudsperson weder bestätigt noch verneint, dass ein Zugriff auf die personenbezogenen Daten des Betroffenen erfolgte und es werden auch keine Aussagen über eventuell zur Abhilfe ergriffenen Maßnahmen getroffen.[991] Zudem ist die Reichweite der tatsächlichen Investigationsbefugnisse der Ombudsperson nicht hinreichend geklärt.[992]

cc) Anforderungen des Art. 25 Abs. 6 DSRL

Nicht zuletzt bleiben weiterhin berechtigte Zweifel daran, ob das EU-U.S.-Privacy Shield den Anforderungen des Art 25 Abs. 6 DSRL gerecht wird. Zwar kann man in dem Durchführungsbeschluss noch das von Art. 25 Abs. 6 DSRL geforderte Kriterium, dass die Angemessenheit tatsächlich festgestellt werden müsse, sehen.[993] Ob dem Kriterium der „[…] innerstaatlichen Rechtsvorschriften oder internationale[n] Verpflichtungen […]“

988 C(2016) 4176, ABl.EU 2016 L 207, 1, Rn. 111 ff.

989 Die Unabhängigkeit der Ombudsperson, die als Under Secretary formell dem Außenministerium zugeordnet ist, vom U.S. Präsidenten nominiert wird und vom U.S. Senat bestätigt werden muss, wird teilweise in Zweifel gezogen, vgl. *Art. 29-Datenschutzgruppe*, Opinion 01/2016 on the EU - U.S. Privacy Shield draft adequacy decision. WP 238 (13.04.2016), S. 49 f.

990 C(2016) 4176, ABl.EU 2016 L 207, 1, Anhang III, Anlage A, Pkt. 3.a.

991 C(2016) 4176, ABl.EU 2016 L 207, 1, Anhang III, Anlage A, Pkt. 4.e.; kritisch *Weichert*, ZD 2016, 209, 216.

992 *Grau/Granetzny*, NZA 2016, 405, 406; *Art. 29-Datenschutzgruppe*, Opinion 01/2016 on the EU - U.S. Privacy Shield draft adequacy decision. WP 238 (13.04.2016), S. 50.

993 *v. Lewinski*, EuR 2016, 405, 416.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

durch das EU-U.S.-Privacy Shield Genüge getan wird, wird jedoch unterschiedlich bewertet.[994] Teilweise wird die Verbindlichkeit im Zusammenhang mit einer Veröffentlichung im U.S. Federal Register diskutiert.[995] Das EU-U.S.-Privacy Shield wurde inzwischen im U.S. Federal Register veröffentlicht,[996] allerdings als „Notice", d. h. eine Anzeige der Existenz eines Dokuments, das für die Öffentlichkeit bedeutsam ist, und nicht als Gesetz.[997] Daraus kann kaum Aussagekraft gewonnen werden. Bei der Debatte um den „Bindungswillen" auf Seiten der USA ist jedoch zu bedenken, dass aus US-amerikanischer Perspektive ebenso an der Bindung der EU an das EU-U.S.-Privacy Shield gezweifelt werden kann. Dies vor allem mit Blick auf die Tatsache, dass bereits die Safe Harbor-Regelung vom *EuGH* für ungültig erklärt wurde und nunmehr gegen das EU-U.S.-Privacy Shield beim *EuG* eine Nichtigkeitsklage anhängig ist.[998] Zudem war kürzlich die Drohung der Kündigung des EU-U.S.-Privacy Shields von EU-Seiten verlautbar[999] angesichts einer Executive Order des U.S.-Präsidenten, die Behörden anwies, Nicht-U.S.-Bürger von behördlichen Datenschutzrichtlinien auszuklammern[1000]. Die Anforderungen des Art. 25 Abs. 6 DSRL sollten vor diesem Hintergrund nicht allzu streng interpretiert werden. Art. 45 Abs. 2 lit. c

994 Zustimmend wohl *v. Lewinski*, EuR 2016, 405, 416; kritisch *Weichert*, ZD 2016, 209, 214; *Schreiber/Kohm* verlangen eine „verbindliche Bekanntmachung" im U. S. Federal Register, *Schreiber/Kohm*, ZD 2016, 255, 258.

995 *v. Lewinski*, EuR 2016, 405, 416; *Weichert*, ZD 2016, 209, 214; *Schreiber/Kohm*, ZD 2016, 255, 258.

996 81 FR 51041; es handelt sich beim U.S. Federal Register um das US-amerikanische Amtsblatt, in dem Gesetze, Gesetzesvorschläge und Notizen veröffentlicht werden.

997 Vgl. *National Archives,* Federal Register Tutorial, abrufbar unter https://www.archives.gov/federal-register/tutorial/online-html.html (abgerufen am 13.10.2017).

998 *EuG,* Nichtigkeitsklage, eingereicht am 16.09.2016, Rs. T-670/16, Abl.EU 2016 C 410, 26 – Digital Rights Ireland/Kommission.

999 So die Äußerung von *Jourova*, vgl. *Bodoni,* If Trump Spoils Privacy Pact, We'll Pull It, EU Official Warns, abrufbar unter https://www.bloomberg.com/news/articles/2017-03-02/if-trump-spoils-privacy-pact-we-ll-pull-it-eu-official-warns (abgerufen am 13.10.2017).

1000 Sec. 14 der Executive Order: Enhancing Public Safety in the Interior of the United States v. 25.01.2017, abrufbar unter https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united (abgerufen am 13.10.2017); eine neue Executive Order vom März 2017 enthält die Passage nicht, vgl. Executive Order Protecting The Nation From Foreign Terrorist Entry Into The United States v. 06.03.2017, abrufbar

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

DSGVO sieht in ähnlicher Weise wie Art. 25 Abs. 6 DSRL vor, dass internationale Verpflichtungen des Drittlands in die Bewertung der Angemessenheit einfließen sollen. Darüber hinaus sind nach Art. 45 Abs. 2 lit. c DSGVO auch „[…] andere Verpflichtungen, die sich aus rechtsverbindlichen Übereinkünften oder Instrumenten sowie aus der Teilnahme des Drittlands […] an multilateralen oder regionalen Systemen insbesondere in Bezug auf den Schutz personenbezogener Daten ergeben […]" in die Bewertung mit aufzunehmen. Das EU-U.S.-Privacy Shield genügt damit nach hier vertretener Ansicht auch den Anforderungen des Art. 45 DSGVO.

III. Zusammenfassung

1. Keine Datentransfers in die USA als drohende Konsequenz

Der *EuGH* hat strenge Kriterien für den Drittlandtransfer aufgestellt. Diese umfassen einen straff angelegten Maßstab für die Bewertung der Angemessenheit, den der *Gerichtshof* mit einem Fokus auf Art. 7, 8 GrCh argumentativ untermauert. Zudem sieht der *Gerichtshof* den Wesensgehalt von Art. 7 und Art. 47 GrCh verletzt angesichts behördlicher Zugriffsmöglichkeiten aus personenbezogene Daten ohne wirksame Rechtsbehelfe.

Legt man diesen Maßstab dem EU-US-Privacy Shield zugrunde, wird man zu dem Schluss kommen, dass auch die neue Regelung, aller Änderungen zum Trotz, nicht diesem Maßstab genügen kann. Denn faktisch umfasst das EU-U.S.-Privacy Shield weiterhin weitreichende Ausnahmen, während der Rechtsschutz, wie dargestellt, wohl nicht den Wirksamkeitskriterien entspricht.

Das bedeutet allerdings, dass den eingangs genannten anderen Möglichkeiten der Übertragung, etwa mittels Standardvertragsklauseln (Art. 26 Abs. 4 DSRL bzw. Art. 46 Abs. 2 lit. c DSGVO), ebenfalls der Weg versperrt ist, besteht die Gefahr behördlicher Zugriffe dort doch in selbem Maße. Teilweise wird den Betroffenen angesichts der (vermeintlichen) Ver-

---

unter https://www.whitehouse.gov/the-press-office/2017/03/06/executive-order-protecting-nation-foreign-terrorist-entry-united-states (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

letzung des Wesensgehalts der Grundrechte gar die Möglichkeit der Einwilligung abgesprochen.[1001] Über die Sinnhaftigkeit einer solchen Begründung angesichts der Diskussion um heimliche Zugriffe europäischer Nachrichtendienste auf personenbezogene Daten,[1002] lässt sich trefflich streiten.

2. Notwendigkeit ausgewogener Interessenabwägungen

Die Konsequenz wäre, dass Datentransfers in die USA faktisch nicht möglich sind und damit ein Großteil der Kommunikation in sozialen Netzwerken mit US-amerikanischem Sitz – was den Großteil der stark frequentierten sozialen Netzwerke darstellt – nicht möglich sein wird. Die Möglichkeit staatlicher Zugriffe auf personenbezogene Daten wird also zum Anlass genommen, den freien Fluss von Daten – und mit ihm die Kontaktaufnahme zu Freunden (jedenfalls, soweit sich diese in den USA befinden) und den Meinungsaustausch – zu begrenzen. In diesem Sinne ist davor zu warnen, mit einer einseitigen Gewichtung von Datenschutzinteressen letztlich in andere Grundrechte, und zwar sowohl der Nutzer von sozialen Netzwerken als auch der Plattformbetreiber selbst, ohne Interessensabwägung einzugreifen.[1003]

3. Achtung gegenseitiger Interessen bei bilateralen Vereinbarungen

Bei den Regelungen zum Drittlandtransfer und insbesondere beim EU-U.S.-Privacy Shield sollte nicht außer Acht gelassen werden, dass es sich hierbei um eine bilaterale Vereinbarung handelt, die die Interessen beider

---

1001 *ULD*, Positionspapier des ULD zum Urteil des EuGH vom 6.10.2015, C-362/14, abrufbar unter https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf (abgerufen am 13.10.2017), S. 4; kritisch *Kühling/Heberlein*, NVwZ 2016, 7, 10 f.; *Heckmann/Starnecker*, jM 2016, 58, 61.

1002 Vgl. etwa *Jansen*, Geheimdienstüberwachung. So können Sie nachprüfen, ob Sie ausgespäht wurden, in: Frankfurter Allgemeine Zeitung v. 19.12.2015, abrufbar unter http://www.faz.net/aktuell/feuilleton/debatten/privacy-international-zeigt-ueberwachung-durch-gchq-13437376.html (abgerufen am 13.10.2017) bezüglich Überwachungen durch den britischen Geheimdienst Government Communications Headquarters.

1003 Bereits zur *Schrems*-Entscheidung kritisch *Kühling/Heberlein*, NVwZ 2016, 7, 12.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Seiten berücksichtigen muss. Bereits als die Safe Harbor-Grundsätze erarbeitet wurden, riefen diese Kritik in den USA hervor. Ein Kritikpunkt war, dass die EU durch den Erlass der DSRL die USA zur Zustimmung zu den Safe Harbor-Grundsätzen gezwungen hätte, weil der Druck durch Art. 25 DSRL und der damit drohenden Gefahr der Beeinträchtigung des Datenflusses zwischen der EU und den USA sehr hoch gewesen sei.[1004] Dies stelle die Souveränität der USA in Frage[1005] und hätte protektionistische Hintergründe.[1006] Auch von der Einnahme einer aggressiven Führungsposition durch die EU war die Rede.[1007] Besonders scharfe Kritiker zeichneten ein düsteres Bild, nachdem EU-Unternehmen durch die Safe Harbor-Entscheidung einen wettbewerblichen Vorteil hätten, wenn US-Unternehmen sich an die hohen Standards von Safe Harbor halten müssten. Dies würde darin resultieren, dass etwa Firmen wie *Ebay* auf dem EU-Markt keine Chance hätten.[1008] Freilich hat sich letzteres nicht bewahrheitet. Gleichwohl zeigen diese Stimmen, dass die Debatte um datenschutzkonforme Datentransfers nicht nur aus europäischer Perspektive betrachtet werden sollte.

D. Fazit

Die Datenschutzsysteme in den USA und in der EU unterscheiden sich in grundlegenden Punkten. Bereits auf grundrechtlicher Ebene fällt auf, dass das Recht auf den Schutz personenbezogener Daten im europäischem Sinne in den USA kein Äquivalent mit Verfassungsrang hat. Auf einfachgesetzlicher Ebene besteht das Datenschutzrecht der USA aus punktuellen Verboten, während in der EU jegliche Verarbeitung personenbezogener Daten auf einen Zulässigkeitstatbestand gestützt werden muss. Zudem werden die einfachgesetzlichen Normen in den USA durch die Gerichte bislang überwiegend so interpretiert, dass die Einwilligung des Datenverarbeiters ausreicht, um den eigentlich verbotenen Datenumgang zu erlauben.

Gleichzeitig zeichnet sich in den USA jedoch ein Bild eines strengen Vollzugs verbraucherschützender, datenschutzrechtlicher Regelungen durch die FTC, insbesondere gegen große Unternehmen, ab. Dabei werden die Unternehmen teilweise zu Zahlungen in einer Höhe verpflichtet, die im

1004 *Vitale*, 35 Vand. J. Transnat'l L. 321, 323.
1005 *Shaffer*, 25 Yale J. Int'l L. 1, 17.
1006 *Shaffer*, 25 Yale J. Int'l L. 1, 47.
1007 *Salbu*, 35 Vand. J. Transnat'l L. 655, 695.
1008 *Vitale*, 35 Vand. J. Transnat'l L. 321, 347 f.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

BDSG im Grundsatz nicht einmal theoretisch vorgesehen ist. Dies könnte sich jedoch bald durch die DSGVO, die scharfe Sanktionen erlaubt, ändern. Gleichwohl zeigt sich an dem Beispiel der FTC, dass die europäischen Regelungen zwar strenger ausgestaltet sind, jedoch nicht zwingend strenger durchgesetzt werden.

Diese Feststellung sollte bei der Bewertung des Datentransfers von der EU in die USA im Blick behalten werden. Der *EuGH* hat in seiner *Schrems*-Entscheidung strenge Maßstäbe für den Datentransfer von der EU in die USA geschaffen. Ob das neu geschaffene EU-U.S.-Privacy Shield diesen Maßstäben gerecht werden kann, mag bezweifelt werden. Nimmt man die Anforderungen der Entscheidung des *Gerichtshofs* an Datentransfers in die USA genau, sind jegliche Instrumente, die den Datentransfer in die USA bislang ermöglichen, aufgrund der Möglichkeit behördlicher Zugriffe unzulässig. In der Konsequenz müsste der Datenfluss in die USA eingestellt werden. Die grundrechtlichen Implikationen dieser Konsequenz sollten aber nicht vorschnell außer Acht gelassen werden. Nicht nur bedeutet dieses „Exportverbot“[1009] einen schwerwiegenden Eingriff in die unternehmerische Freiheit der Diensteanbieter, sondern auch in die Meinungsfreiheit der Nutzer und deren Recht auf informationelle Selbstbestimmung dahingehend, den Schutz ihrer Daten zugunsten kostengünstiger Dienste einzuschränken. Eine einseitige Favorisierung des Schutzes personenbezogener Daten ohne eine hinreichende Interessenabwägung dürfte damit auch nicht im Sinne der Nutzer sein, deren Schutz bezweckt wird.

1009 *Heckmann/Starnecker*, jM 2016, 58, 61.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Schlussbetrachtungen

Der „Tod des Datenschutzes“[1010] in sozialen Netzwerken ist nicht zu befürchten. Insbesondere mit der DSGVO, die ab Mai 2018 gilt, ist auf ein vollzugsstarkes Datenschutzrecht zu hoffen, das die Aufsichtsbehörden mit scharfen Sanktionierungsmöglichkeiten ausstattet.

Im Folgenden seien die Ergebnisse der Untersuchung zusammengefasst:

A. Entterritorialisierte Sachverhalte als Herausforderung des Datenschutzrechts

I. Einführung des Marktortprinzips in der DSGVO

Die grenzüberschreitende Natur des Datenflusses ist eine der größten Herausforderungen des Datenschutzrechts in sozialen Netzwerken. Bereits die Identifikation des territorial anwendbaren Rechts, auf dessen Grundlage die Zulässigkeit konkreter Datenverarbeitungen bewertet wird, bereitet Probleme. Das Regelungsregime der DSRL knüpft im Grundsatz an das Vorhandensein einer Niederlassung in einem Mitgliedstaat in der EU bzw. dem EWR an, jedoch ohne den Niederlassungsbegriff hinreichend genau zu definieren.

Mit der DSGVO werden diese Probleme zumindest teilweise beseitigt. Zwar knüpft die DSGVO im Grundsatz ebenfalls an den Niederlassungsbegriff an. Die Bedeutung der Interpretation dieses Begriffs wird gleichwohl schwinden. Denn Art. 3 Abs. 2 DSGVO sieht vor, dass die Verordnung dann anwendbar sein soll, wenn Diensteanbieter ihre Dienstleistungen Personen in der Union anbieten oder das Verhalten von Personen in der Union beobachten. Damit werden sich die großen Betreiber sozialer Netzwerke nunmehr zweifellos dem Regime der DSGVO unterwerfen müssen, ohne dass es darauf ankommt, ob sie eine Niederlassung auf dem Unionsgebiet unterhalten.

Auch die Abgrenzung mitgliedstaatlicher Regelungsregimes wird bei einer unmittelbar anwendbaren Verordnung weniger – aber nicht gar keine –

1010 Vgl. *Andrews,* I know who you are and I saw what you did.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Probleme bereiten. Denn mit den durch die DSGVO markierten Regelungsspielräumen wird es weiterhin Unterschiede in mitgliedstaatlichen Datenschutzgesetzen geben. Für die Abgrenzung dieser mitgliedstaatlichen Regelungen enthält die DSGVO, die nur ihren eigenen räumlichen Anwendungsbereich regelt, keine Kollisionsnorm. Das bedeutet, dass es für diese Fälle ab Mai 2018, mit der Ablösung der DSRL durch die DSGVO, keine spezielle datenschutzrechtliche Kollisionsnorm mehr gibt. Hier lässt sich ein Minus der Reichweite der DSGVO gegenüber der DSRL erkennen, die auch die Abgrenzung nationaler Datenschutzregelungen im Blick hatte. Damit ist für die Abgrenzung der mitgliedstaatlichen Regelungen, die im Rahmen der durch die Öffnungsklauseln markierten Regelungsspielräume erlassen werden, auf die allgemeinen Kollisionsnormen zurückzugreifen. Da dies aber zu uneinheitlichen Ergebnissen je nach Sachverhalt führen kann – so unterlägen gewerbliche Nutzer eines sozialen Netzwerks etwa anderen Regelungen als Verbraucher, Art. 6 Rom-I-VO – wäre eine rasche Schließung dieser Lücke mit spezifischem Kollisionsrecht vorzugswürdig.

II. Datenfluss in die USA als Folge der Datenverarbeitung in sozialen Netzwerken

Nicht nur die Identifikation des räumlich anwendbaren Rechts bereitet Probleme, sondern auch der Datenfluss zwischen der EU und Drittländern. Besondere Bedeutung hat dabei der Datentransfer von personenbezogenen Daten in die USA, die Heimat der sozialen Netzwerke mit den höchsten europäischen Nutzerzahlen sind, die personenbezogene Daten europäischer Nutzer in Datenzentren in den USA übermitteln.

Dabei stellen ein grundlegend unterschiedliches datenschutzrechtliches Verständnis zwischen der EU und den USA sowie der europäische Ansatz, der einen Datenfluss nur in Drittländer mit einem „angemessenen" Schutzniveau zulässt, die praktische Umsetzbarkeit des Datentransfers vor zusätzliche Herausforderungen.

Das US-amerikanische Recht kennt kein Verbot mit Erlaubnisvorbehalt; stattdessen sind im Grundsatz alle Datenverarbeitungen zulässig, solange sie nicht explizit gesetzlich eingeschränkt sind. Die möglicherweise einschlägigen US-amerikanischen Bundesgesetze sind entweder schon vom Tatbestand her nicht anwendbar, oder aber ihre Anwendbarkeit wird durch die sog. one consent-rule, nach der ein Teilnehmer einer Kommunikation dem Abfangen der dort übermittelten Informationen zustimmen kann, blockiert. Die gewohnheitsrechtlich anerkannten privacy torts helfen ebenso

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

nur bedingt weiter, da ihre Anwendung durch die Rechtsprechung auf besonders schwerwiegende Fälle reduziert wird.

Durch diese materiell-rechtlichen Unterschiede gestaltet sich die Zulässigkeit des Datenflusses in die USA schwierig. Denn nach europäischem Ansatz können personenbezogene Daten den unionalen datenschutzrechtlichen Binnenraum nur verlassen, soweit das Drittland, in das die Daten transferiert werden sollen, ein angemessenes Schutzniveau aufweist, d. h. ein Schutzniveau, dass nach Rechtsprechung des *EuGH* gleichwertig mit dem europäischen Schutzniveau sein soll.[1011]

Diese Differenzen suchten die Safe Harbor-Entscheidung der Kommission aus dem Jahr 2000 sowie ihr Nachfolger, das EU-U.S.-Privacy Shield aus dem Jahr 2016, auszugleichen. So legen beide Konzepte gewisse im US-amerikanischen Datenschutzrecht nicht vorgesehene materiell-rechtliche Grundsätze fest, wie etwa ein Einwilligungserfordernis für die Datenverarbeitung. Allerdings leidet das EU-U.S.-Privacy Shield, wie schon sein Vorgänger, an umfassenden Begrenzungsmöglichkeiten der Grundsätze sowie an einer defizitären Ausprägung der bereitgestellten Rechtsansprüche. So verwundert es nicht, dass gegen das EU-U.S.-Privacy Shield bereits eine Nichtigkeitsklage vor dem *EuG* anhängig ist.[1012]

Bei aller Freude über einen starken Datenschutz in Europa ist indes vor einer „recht unmöglichen Anspruchshaltung der europäischen Datenschutzordnung“[1013] zu warnen. Denn erstens verfügen die USA zwar nicht über den europäischen Datenschutzgesetzen ähnliche strenge Regelungen. Dafür ist jedoch die FTC Vorreiter im Vollzug der bestehenden datenschutzrechtlichen Regelungen und zeigt sich teilweise deutlich strenger als ihre europäischen Kollegen. Zweitens ist die drohende Konsequenz zu strenger Maßstäbe für den Datentransfer die Blockade des Datentransfers in die USA. Selbst die Möglichkeit zur Einwilligung in den Datentransfer wird den Betroffenen angesichts eines nach europäischer Vorstellung defizitären Datenschutzes in den USA teilweise abgesprochen.

1011 *EuGH,* Urt. v. 06.10.2015, Rs. C-362/14, ECLI:EU:C:2015:650, Rn. 73 – Schrems.

1012 *EuG,* Nichtigkeitsklage, eingereicht am 16.09.2016, Rs. T-670/16, Abl.EU 2016 C 410, 26.

1013 *Heckmann/Starnecker*, jM 2016, 58, 60.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

B. Der Nutzer als Verantwortlicher (nur) für die eigene Datenverarbeitung

Die Privilegierung für ausschließlich familiäre oder persönliche Tätigkeiten greift nicht bei der Datenverarbeitung durch Nutzer in sozialen Netzwerken, das bedeutet, dass datenschutzrechtliche Bestimmungen sowohl des BDSG als auch der DSGVO auf die Datenverarbeitung durch Nutzer anwendbar sind. Sie unterfällt nur dann der Privilegierung für ausschließlich persönliche oder familiäre Tätigkeiten, sofern es sich um eine Datenverarbeitung mittels Nachrichtenfunktionen handelt. Für alle weiteren Datenverarbeitungen ergibt sich jedoch, dass ein gewisser Außenbezug der Datenverarbeitung dazu führt, dass es sich nicht mehr um eine *ausschließlich* familiäre oder persönliche Tätigkeit handelt. Demnach wäre es nicht gerechtfertigt, jegliche Verarbeitung personenbezogener Daten in sozialen Netzwerken durch die Nutzer aus dem datenschutzrechtlichen Anwendungsbereich auszunehmen.

Der Nutzer ist zudem Verantwortlicher im datenschutzrechtlichen Sinne, solange er das „Warum" und „Wie" der Verarbeitung steuert. Daraus folgt, dass der Nutzer für von ihm hochgeladene oder verbreitete Informationen Verantwortlicher ist, nicht aber für die eigenständige Verarbeitung dieser personenbezogenen Daten durch den Betreiber des sozialen Netzwerks. Dieser Grundsatz lässt sich auch auf Nutzer übertragen, die öffentliche Profile betreiben: Sie steuern nicht das „Warum" und „Wie" der Verarbeitung personenbezogener Daten von Besuchern ihres öffentlichen Profils durch den Betreiber des sozialen Netzwerks. Ebenso wenig kommt ihnen eine Auswahlverantwortung für die sorgfältige Auswahl des Betreibers des sozialen Netzwerks, das sie für ihr öffentliches Profil wählen, zu. Nicht nur würde diese Auswahlverantwortlichkeit an der Grenze der Zumutbarkeit dahingehend scheitern, dass ein datenschutzrechtlicher Verstoß durch den Betreiber des sozialen Netzwerks für den Betreiber des öffentlichen Profils offensichtlich sein müsste. Die hoheitliche Unterbindung des Austausches auf öffentlichen Profilen wäre zudem aus grundrechtlichen Gesichtspunkten bedenklich. Betreiber öffentlicher Profile sind daher nicht für die Verarbeitung personenbezogener Daten ihrer Profilbesucher durch den Betreiber des sozialen Netzwerks verantwortlich.

Anders verhält es sich jedoch bei Websitebetreibern, die ein Social Plug-In eines sozialen Netzwerks auf ihre Website einbinden. Sie steuern mit der Einbindung das „Ob" der Verarbeitung vollumfänglich und das „Warum"

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

der Datenverarbeitung in ausreichendem Maße. Es kann ihnen daher auferlegt werden, das Social Plug-In erst nach hinreichender Information der Nutzer und deren Einwilligung zu aktivieren.

C. *Die DSGVO als Pfadbereiter für ein vollzugstarkes Datenschutzrecht*

I. Von der DSRL zur DSGVO: Altbekannte Prinzipien mit neuen Vollzugsmöglichkeiten

In materiell-rechtlicher Sicht bietet die DSGVO kaum Neuerungen zur DSRL. Die beiden Regelwerke gleichen sich in einigen wesentlichen Punkten, wie etwa den Zulässigkeitstatbeständen. So wurde der Zulässigkeitstatbestand des Art. 6 Abs. 1 S. 1 lit. f DSGVO, der neben der in Art. 6 Abs. 1 S. 1 lit. a DSGVO geregelten Einwilligung den im privaten Bereich wichtigsten Zulässigkeitstatbestand für die Verarbeitung personenbezogener Daten darstellt, beinahe wortlautgleich von seiner Vorgängernorm des Art. 7 lit. f DSRL übernommen. Auch hinsichtlich der Betroffenenrechte, wie etwa des Rechts auf Löschung, das als „Recht auf Vergessenwerden" starke Aufmerksamkeit erregt hatte, bietet die DSGVO keine relevanten Neuerungen. Ein tatsächliches materiell-rechtliches Novum stellt demgegenüber die Regelung des Art. 8 DSGVO dar, die erstmals eine feste Altersgrenze für die Einwilligungsfähigkeit von Minderjährigen festlegt.

Den altbekannten Prinzipien aus der DSRL verhilft die DSGVO mit neuen Möglichkeiten zur Durchsetzung: Mit Sanktionen von Geldbußen in Höhe von bis zu 4 % des weltweiten Jahresumsatzes stellt die DSGVO den Aufsichtsbehörden ein scharfes Schwert zur Verfügung, Datenschutzverstöße zu ahnden. Die Möglichkeit dieser Sanktionen kann dazu beitragen, das Datenschutzrecht effektiv durchzusetzen, falls von ihr Gebrauch gemacht wird. Es liegt damit in der Hand der Aufsichtsbehörden, die neuen Mittel zur Durchsetzung des Datenschutzrechts effektiv zu nutzen.

Auch für den Betroffenen selbst wird die Rechtsdurchsetzung durch den Schadensersatzanspruch gem. Art. 82 Abs. 1 DSGVO, nach dem auch immaterielle Schäden ersatzfähig sind, erleichtert. Im Gegensatz zu dem Anspruch aus § 823 Abs. 1, 2 i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG regelt Art. 82 Abs. 3 DSGVO eine Beweislastumkehr für das Verschulden des Datenverarbeiters für den Eintritt des Schadens zu Lasten des Datenverarbeiters.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Zudem sieht die DSGVO ein ausdifferenziertes System der Zusammenarbeit der Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten vor. Während unter dem DSRL-Regime bei Internetsachverhalten, die mehrere Mitgliedstaaten berühren – etwa wenn ein Nutzer eines Mitgliedstaates die Website eines in einem anderen Mitgliedstaat ansässigen Betreibers aufruft – die Zuständigkeit und Befugnisse der Aufsichtsbehörden der unterschiedlichen Mitgliedstaaten Schwierigkeiten bereiten[1014], legt die DSGVO nun die Aufsichtsbehörde der Hauptniederlassung des Datenverarbeiters als federführende Behörde fest, Art. 56 Abs. 1 DSGVO, die zur Zusammenarbeit mit der betroffenen Behörde i. S. d. Art. 56 Abs. 2 DSGVO verpflichtet wird, Art. 60 Abs. 1 DSGVO. Sollten die Aufsichtsbehörden dabei keine Einigung erzielen, sieht die DSGVO zudem das Kohärenzverfahren gem. Art. 63 ff. DSGVO vor.

Mit scharfen Sanktionsmöglichkeiten und Regelungen zur Zusammenarbeit der Aufsichtsbehörden sowie den Anpassungen zivilrechtlicher Ansprüche gegen Datenschutzverstöße legt die DSGVO den Grundstein für einen effektiven Vollzug des Datenschutzrechts. Die innovativen Elemente der DSGVO im Vergleich zur DSRL liegen damit in den verschärften Instrumenten zu einer effektiven Rechtsdurchsetzung und der Rechtsform einer Verordnung.

II. Vom deutschen Datenschutzrecht zur DSGVO

1. Ende der bereichsspezifischen Zersplitterung bei Datenverarbeitungen durch Private

Durch die unmittelbare Geltung der DSGVO werden die Regelungen des BDSG und des TMG in der DSGVO aufgehen. Das wird in Deutschland zu einigen tatsächlichen Änderungen in der Rechtslage führen: Zunächst werden schwierige Abgrenzungsfragen hinsichtlich des sachlich anwendbaren Rechts im deutschen Datenschutzrecht, das durch zahlreiche bereichsspezifische Regelungen mit einem nur subsidiär anwendbaren BDSG geprägt ist, mit der DSGVO beseitigt sein. Damit ist auch die durch die Subsidiaritätsregelung im BDSG hervorgerufene Problematik unterschiedlicher Schutzstandards für unterschiedliche Informationen – so unterliegen beispielsweise Partyfotos einem weniger strengen Schutz als eine E-Mail-Adresse –

1014 Vgl. etwa *EuGH,* Urt. v. 01.10.2015, Rs. C-230/14, ECLI:EU:C:2015:639 – Weltimmo.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

gelöst. Nicht zuletzt wird die DSGVO auch unionswidrige Normen, wie etwa § 15 Abs. 1 TMG, ablösen.

2. Art. 6 Abs. 1 S. 1 lit. f DSGVO als allumfassender Legitimationstatbestand

In materiell-rechtlicher Hinsicht ist die Umstellung von sehr detailreichen Zulässigkeitstatbeständen in §§ 28 ff. BDSG zu der deutlich knapperen, dafür aber sehr weitreichenden Norm des Art. 6 Abs. 1 DSGVO augenfällig.

Die umfangreichen Regelungen der §§ 28 ff. BDSG können teilweise nur mit Mühe auf Sachverhalte in sozialen Netzwerken angelegt werden. So sind die Regelungen hauptsächlich auf kommerzielle Datenverarbeiter ausgelegt und können teilweise nur im Rahmen einer teleologischen Extension auf nicht-kommerzielle Datenverarbeiter – den privaten Nutzern sozialer Netzwerke ohne gewerbliche Interessen – angewendet werden. Dies führt dazu, dass kommerzielle Datenverarbeiter sich in einer gegenüber nichtkommerziellen Datenverarbeitern privilegierten Stellung befinden. Überdies sieht § 29 Abs. 2 BDSG vor, dass bei einer Übermittlung zulässigerweise akquirierter personenbezogener Daten der Empfänger dieser Daten noch vor der Übermittlung sein Interesse an den Daten darlegen muss. Diese Bedingung gilt nach der Norm auch dann, wenn es sich um eine Übermittlung personenbezogener Daten von Personen der Zeitgeschichte, etwa namenhaften Politikern, handelt. Übermittlungen im Internet an eine Vielzahl potentieller Empfänger sind damit faktisch unzulässig, was starke Bedenken hinsichtlich der Verfassungsmäßigkeit[1015] sowie Unionsrechtskonformität der Norm aufwirft.

Demgegenüber knüpft Art. 6 Abs. 1 S. 1 lit. f DSGVO, der im Verhältnis zwischen Privaten die entscheidende Zulässigkeitsnorm darstellt, die Zulässigkeit der Datenverarbeitung allein an eine Interessenabwägung zwischen den Betroffenen-, Dritt- und Verarbeiterinteressen. Die Norm erweist sich damit als deutlich flexibler als die Normen des BDSG und lässt sich durch ihre offene Formulierung auf eine Vielzahl von Sachverhalten anwenden. Allerdings ist die in Art. 6 Abs. 1 S. 1 lit. f DSGVO vorgesehene Interessenabwägung durch den Verarbeiter selbst vorzunehmen, wodurch die Gefahr besteht, dass eine allzu großzügige Interpretation der Norm durch die

1015 Vgl. *BGH,* Urt. v. 23.06.2009, Az. VI ZR 196/08, BGHZ 181, 328 – spickmich.de; *BGH,* Urt. v. 23.09.2014, Az. VI ZR 358/13, BGHZ 202, 242 – Ärztebewertung II.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Verantwortlichen selbst zu einer Umgehung des Verbots mit Einwilligungsvorbehalt führt. Aus Perspektive der Verantwortlichen ist damit ein Zustand der Rechtsunsicherheit geschaffen, da bislang kaum Anhaltspunkte für die Interpretation der Norm vorliegen. Nach ursprünglicher Konzeption sollte die Norm durch delegierte Rechtsakte der Kommission eine Konkretisierung erfahren, jedoch wurde diese Bestimmung nicht in die endgültige Fassung der DSGVO aufgenommen. Damit ist ein Appell an die Rechtsprechung und die Aufsichtsbehörden zu richten, die Voraussetzungen der Norm rasch zu konkretisieren. Ebenso ist auf eine rasche Veröffentlichung von Leitlinien zur Anwendung von Art. 6 Abs. 1 S. 1 lit. f DSGVO durch den europäischen Datenschutzausschuss i. S. d. Art. 70 Abs. 1 S. 2 lit. e DSGVO zu hoffen.

3. Gleichbleibende Bedeutung der Einwilligung

Schließlich bleibt die Einwilligung, ebenso wie unter dem BDSG, auch unter der DSGVO das wichtigste Legitimationsmittel für Datenverarbeitungen.

In formeller Hinsicht kennt die DSGVO – wie schon die DSRL – kein Schriftformerfordernis der Einwilligung und löst entsprechende bislang bestehende Rechtsunsicherheiten im Nutzer-Nutzer-Verhältnis auf. Denn die entsprechende Vorschrift im BDSG, § 4a Abs. 1 S. 3, führt bei strengem Verständnis der Norm dazu, dass Nutzer für das Hochladen von Informationen über andere Nutzer in einem sozialen Netzwerk eine schriftliche Einwilligung benötigen, während eine Einwilligung etwa per E-Mail nicht ausreicht.

Für die Einwilligungsfähigkeit Minderjähriger setzt Art. 8 Abs. 1 DSGVO erstmals eine Altersgrenze von 16 Jahren fest, die von den Mitgliedstaaten im Rahmen der Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DSGVO bis zum Alter von 13 Jahren abgesenkt werden darf. Anbietern von Diensten der Informationsgesellschaft wird dabei i. S. d. Art. 8 Abs. 2 DSGVO auferlegt zu überprüfen, ob die Einwilligung tatsächlich durch die Eltern bzw. den Vormund des Minderjährigen erteilt wurde. Hierbei bietet sich eine Einwilligungsbestätigung des Vormundes über eine E-Mail an. Eine weitergehende Überprüfung der Identität, etwa durch den Versand einer Kopie eines Ausweisdokuments, wäre zwar weniger missbrauchsanfällig, würde jedoch auch einen deutlich gesteigerten Zugriff der Diensteanbieter auf personenbezogene Daten aller Nutzer bedeuten. Der damit einhergehende Schutz von Minderjährigen vermag die mit dem Zugriff auf

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

sensiblere Informationen aller Nutzer, wie etwa Ausweisdokumente, einhergehenden Gefahren nicht zu überwiegen.

Die inhaltlichen Voraussetzungen an eine wirksame Einwilligung bleiben demgegenüber grundsätzlich erhalten, wobei sich allerdings Änderungen hinsichtlich der Freiwilligkeit der Einwilligung ergeben: Das BDSG sieht in § 28 Abs. 3b ein Koppelungsverbot zu Zwecken des Adresshandels und der Werbung vor, während die DSGVO in Art. 7 Abs. 4 eine an ein allgemeines Koppelungsverbot angelehnte Auslegungsregel hinsichtlich der Freiwilligkeit der Einwilligung enthält. Gem. Art. 7 Abs. 4 DSGVO ist darauf abzustellen, ob die Erfüllung eines Vertrags von der Einwilligung in die Verarbeitung personenbezogener Daten abhängig gemacht wird, die für die Erfüllung des Vertrags nicht erforderlich ist. Zudem soll in Fällen eines klaren Ungleichgewichts zwischen den Parteien die Einwilligung nicht als Legitimationsgrundlage dienen, EG 43 S. 1 DSGVO. Allerdings sind die Anforderungen an das Vorliegen eines Ungleichgewichts mit Blick auf das in EG 43 genannte Beispiel des Verhältnisses von Behörde und Bürger als hoch einzustufen. Dies ergibt sich auch daraus, dass das Beispiel des Arbeitgeber-Arbeitnehmer-Verhältnisses für ein solches Ungleichgewicht, das noch im Kommissionsentwurf der DSGVO enthalten war, nicht in die endgültige Fassung aufgenommen wurde. Auch verdeutlicht der Wortlaut des Art. 7 Abs. 4 DSGVO, dass es sich bei der Regelung lediglich um eine Auslegungshilfe handelt und selbst bei Vorliegen eines Abhängigmachens die Einwilligung nicht automatisch unwirksam ist.

Aus dem Aufstreben einer Vielzahl von Angeboten sozialer Netzwerke mit hohen Mitgliedszahlen lässt sich die Bereitschaft der Nutzer erkennen, sich in mehreren sozialen Netzwerken gleichzeitig anzumelden. Daraus ist zu schließen, dass der Markt sozialer Netzwerke nicht von einem einzigen Anbieter beherrscht wird, sondern den Nutzern verschiedene Angebote zur Verfügung stehen. Volljährigen Nutzern ist es im Rahmen ihres Rechts auf informationelle Selbstbestimmung daher durchaus zuzutrauen, gewisse Angebote, deren Datenschutz sie nicht für ausreichend erachten, nicht in Anspruch zu nehmen, da ihnen ausreichend Alternativen zur Verfügung stehen. Bei Minderjährigen ist indes ein modifizierter Maßstab anzulegen, nach dem das Koppelungsverbot streng verstanden werden muss.

III. Modifikationen der DSGVO-Regelungen durch das BDSG-neu

Die unmittelbare Geltung der DSGVO wird durch zahlreiche Öffnungsklauseln durchbrochen, die den nationalen Gesetzgebern die Möglichkeit

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

geben, die entsprechenden Regelungen der Verordnung durch nationales Recht zu modifizieren.[1016] Der Bundesgesetzgeber hat davon in einem „BDSG-neu" Gebrauch gemacht,[1017] das unter anderem als Ergänzung zu den Regelungen der DSGVO fungieren wird. Im Rahmen der Zulässigkeitstatbestände finden sich Öffnungsklauseln in Art. 6 Abs. 1 S. 1 lit. c, e DSGVO i. V. m. Abs. 2, 3 DSGVO. Für die Untersuchung der Verarbeitung in sozialen Netzwerken sind diese Öffnungsklauseln jedoch kaum relevant, da sie die Zulässigkeit aufgrund der Erfüllung einer rechtlichen Verpflichtung (lit. c) bzw. die Wahrnehmung einer Aufgabe im öffentlichen Interesse (lit. e) betreffen. Für die Normen der Art. 6 Abs. 1 S. 1 lit. a, f DSGVO, die für die Zulässigkeit der Datenverarbeitung in sozialen Netzwerken eine signifikante Rolle spielen, hält die DSGVO keine Öffnungsklauseln bereit. Art. 23 Abs. 1 DSGVO gibt den Mitgliedstaaten jedoch die Möglichkeit, die in Art. 12 bis 22 DSGVO geregelten Betroffenenrechte einzuschränken. Von dieser Möglichkeit wird in den §§ 32 ff. BDSG-neu Gebrauch gemacht. Während allerdings der Entwurf der Bundesregierung noch weitreichende Beschränkungsmöglichkeiten vorsah, bei denen gewisse Zweifel bestanden, ob sie überhaupt von der Öffnungsklausel des Art. 23 Abs. 1 DSGVO gedeckt wären, wurden diese Beschränkungsmöglichkeiten in der endgültigen Fassung des BDSG-neu an konkretisierte Voraussetzungen geknüpft und somit begrenzt.

Im Bereich der Betroffenenrechte sind auch ab Mai 2018 demnach, ergänzend zur DSGVO, nationale Regelungen zu beachten.

IV. Ablösung der ePrivacy-RL durch eine ePrivacy-VO

Die ePrivacy-RL, die im Rahmen von sozialen Netzwerken hinsichtlich der Nutzung von Tracking Tools wie Cookies Vorrang vor den Vorgaben der DSRL hat, Art. 1 Abs. 2 ePrivacy-RL, soll von einer ePrivacy-VO abgelöst werden. Zu diesem Zweck hat die Kommission im Januar 2017 einen Entwurf einer ePrivacy-VO vorgelegt, die gem. Art. 29 Abs. 2 ePrivacy-VO-E ebenso wie die DSGVO ab Mai 2018 anwendbar sein soll.

Ebenso wie Art. 5 Abs. 3 ePrivacy-RL sieht der ePrivacy-VO-E vor, dass der Nutzer in die Verwendung von Tracking Tools einwilligen muss, Art. 8

1016 Vgl. zur Typologie der Öffnungsklauseln *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die DSGVO und das nat. Recht, S. 10 ff.

1017 BR-Drucks. 332/17 (Beschluss); vgl. Art. 1 DSAnpUG-EU, BGBl. 2017 I, 2097.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Abs. 1 ePrivacy-VO-E. Bislang wurde diese Vorgabe der ePrivacy-RL im TMG nur unzureichend umgesetzt. Die entsprechende Norm verlangt nämlich keine ausdrückliche Einwilligung, sondern spricht den Nutzern lediglich ein Widerspruchsrecht zu, § 15 Abs. 3 TMG. Diese Problematik wird mit der ePrivacy-VO beendet.

In formeller Hinsicht soll der ePrivacy-VO-E der bislang üblichen Praxis entgegenwirken, die Einwilligung mittels Erscheinens von Bannern, die über die Nutzung von Cookies informieren, einzuholen, EG 22 ePrivacy-VO-E. Stattdessen sollen Nutzer gem. Art. 9 ePrivacy-VO-E über ihre Browser-Einstellungen einwilligen können.

V. Ausblick: Notwendigkeit einer raschen Konturierung der Zulässigkeitstatbestände

Durch den Wechsel von einer Richtlinie zu einer Verordnung werden nicht nur die nationalen Umsetzungsgesetze der DSRL abgelöst und – abgesehen von den durch die in der DSGVO enthaltenen Öffnungsklauseln entstehenden Regelungsspielräumen – weitgehend eine Vollharmonisierung des europäischen Datenschutzrechts herbeigeführt. Damit einher geht auch die Bildung eines umfangreichen, unionsweiten Schatzes an Auslegung des Regelungssystems durch die Literatur sowie durch die Rechtsprechung, der durch eine scharfe Konturierung der Regelungen zu einer größeren Rechtssicherheit führen kann.

Bis die Rechtsprechung jedoch auf die DSGVO reagieren kann, wird einige Zeit vergehen. In der Zwischenzeit rufen die nur kursorisch ausgeprägten Zulässigkeitstatbestände einen Zustand der Rechtsunsicherheit hervor. Dies betrifft insbesondere Art. 6 Abs. 1 S. 1 lit. f DSGVO, dessen Anwendbarkeit allein von einer Interessenabwägung durch den Verantwortlichen abhängt. Dem kann der europäische Datenschutzausschuss entgegentreten, indem er Leitlinien mit entsprechenden Abwägungskriterien bereitstellt und den Verantwortlichen damit eine Auslegungshilfe an die Hand gibt.

Insgesamt wird durch die DSGVO ein funktionsfähiger Rahmen geschaffen, der einerseits flexibel genug ist, um auch auf künftige technische Entwicklungen reagieren zu können, und durch den andererseits mit der nötigen Schärfe gegen Datenschutzverstöße vorgegangen werden kann.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

D. Datenschutzrecht zwischen Privaten als multipolares Grundrechtsgefüge

Nicht zuletzt muss darauf hingewiesen werden, dass dem Datenschutzrecht zwischen Privaten die Interessenabwägung inhärent ist. Zu diesem Zweck müssen Betroffeneninteressen mit den Interessen der Plattformbetreiber und Dritter in Einklang gebracht werden. Insbesondere ist dabei zu beachten, dass Nutzer sozialer Netzwerke nicht nur ein datenschutzrechtliches Interesse, sondern auch ein Interesse an der Nutzung der Dienste und dem Kommunikationsaustausch darin haben. Indes ist eindringlich davor zu warnen, dem Datenschutz eine pauschale Vorrangstellung einzuräumen.

Denn das Beispiel eines allzu strengen Maßstabs für den Datentransfer in Drittländer verdeutlicht die möglicherweise drohende Konsequenz defizitärer Interessenabwägungen: Dann droht, möchte man es in ähnlich exklamatorischer Weise ausdrücken, möglicherweise „der Tod der sozialen Netzwerke“. Das entspricht sicherlich nicht dem Wunsch der Nutzer.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Literaturverzeichnis

Acar, Gunes/Eubank, Christian/Englehardt, Steven/Juarez, Marc/Narayanan, Arvind/Diaz, Claudia, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, in: Association for Computing Machinery (Hrsg.), CCS'14. 21st ACM Conference on Computer and Communications Security 2014, New York 2014, S. 263–274.

Acar, Güneş/van Alsenoy, Brendan/Piessens, Frank/Diaz, Claudia/Preneel, Bart, Facebook Tracking Through Social Plug-ins. Technical Report prepared for the Belgian Privacy Commission, Version 1.1 (24.06.2015), abrufbar unter https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf (abgerufen am 13.10.2017).

Achtruth, Björn, Der rechtliche Schutz bei der Nutzung von Social Networks, Münster 2014.

Ahlberg, Hartwig/Götting, Horst-Peter (Hrsg.), Beck'scher Online-Kommentar Urheberrecht, 15. Edition, München 2017 (zitiert: *Bearbeiter(in)*, in: BeckOK UrhR).

Albrecht, Jan Phillip/Jotzo, Florian, Das neue Datenschutzrecht der EU. Grundlagen. Gesetzgebungsverfahren. Synopse, Baden-Baden 2017.

Albrecht, Jan Phillip, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, CR 2016, 88–98.

Allen, Ronald J./Mace, M. Kristin, The Self-incrimination Clause Explained and its Future Predicted, 94 J. Crim. L. & Criminology 243–293.

Joecks, Wolfgang/Miebach, Klaus (Hrsg.), Münchener Kommentar zum Strafgesetzbuch. Band 1, 3. Auflage, München 2017 (zitiert: *Bearbeiter(in)*, in: MüKo-StGB).

Andrews, Lori B., I know who you are and I saw what you did. Social networks and the death of privacy, New York 2012.

Arbeitsgruppe des AK I „Staatsrecht und Verwaltung", Ergebnisbericht der Arbeitsgruppe AK I „Staatsrecht und Verwaltung" zum Datenschutz in Sozialen Netzwerken vom 4. April 2012, abrufbar unter https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf (abgerufen am 13.10.2017).

Arnold, René/Hillebrand, Annette/Waldburger, Martin, Informed Consent in Theorie und Praxis. Warum Lesen, Verstehen und Handeln auseinanderfallen, DuD 2015, 730–734.

Art. 29-Datenschutzgruppe, Opinion 01/2016 on the EU - U.S. Privacy Shield draft adequacy decision. WP 238 (13.04.2016), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (abgerufen am 13.10.2017).

Art. 29-Datenschutzgruppe, Update of Opinion 8/2010 on applicable law in light of CJEU judgement in Google Spain. WP 179 update (16.12.2015), abrufbar unter

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf (abgerufen am 13.10.2017).

Art. 29-Datenschutzgruppe, Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies. WP 208 (02.10.2013), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_de.pdf (abgerufen am 13.10.2017).

Art. 29-Datenschutzgruppe, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht. WP 194 (07.06.2012), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_de.pdf (abgerufen am 13.10.2017).

Art. 29-Datenschutzgruppe, Stellungnahme 08/2010 zum anwendbaren Recht. WP 179 (16.12.2010), abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf (abgerufen am 13.10.2017).

Art. 29-Datenschutzgruppe, Stellungnahme 2/2010 zur Werbung auf Basis von Behavorial Targeting. WP 171 (22.06.2010), abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_de.pdf (abgerufen am 13.10.2017).

Art. 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsdatenverarbeiter". WP 169 (16.02.2010), abrufbar unter http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf (abgerufen am 13.10.2017).

Art. 29-Datenschutzgruppe, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU. WP 56 (30.05.2002), abrufbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_de.pdf (abgerufen am 13.10.2017).

Ashkar, Daniel, Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutz-Grundverordnung, DuD 2015, 796–800.

Autenrieth, Ulla P./Bänziger, Andreas/Rohde, Wiebke/Schmidt, Jan, Gebrauch und Bedeutung von Social Network Sites im Alltag junger Menschen: Ein Ländervergleich zwischen Deutschland und der Schweiz, in: Neumann-Braun/Autenrieth (Hrsg.), Freundschaft und Gemeinschaft im Social Web. Baden-Baden 2011, S. 31–54.

Autenrieth, Ulla P., MySelf. MyFriends. MyLife. MyWorld: Fotoalben auf Social Network Sites und ihre kommunikativen Funktionen für Jugendliche und junge Erwachsene, in: Neumann-Braun/Autenrieth (Hrsg.), Freundschaft und Gemeinschaft im Social Web. Baden-Baden 2011, S. 123–162.

Ayenson, Mika D./Wambach, Dietrich J./Soltani, Ashkan/Good, Nathaniel/Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, abrufbar unter https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390 (abgerufen am 13.10.2017).

Bamberger, Heinz Georg/Roth, Herbert (Hrsg.), Beck'scher Online-Kommentar BGB, 42. Edition, München 2017 (zitiert: *Bearbeiter(in)*, in: BeckOK BGB).

Barocas, Solon/Nissenbaum, Helen, On Notice: The Trouble with Notice and Consent, Proceedings of the Engaging Data Forum: The First International Forum on the Ap-

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

plication and Management of Personal Electronic Information (October 2009), abrufbar unter http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf (abgerufen am 13.10.2017).

Bauer, Stephan, Personalisierte Werbung auf Social Community Websites. Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen, MMR 2008, 435–438.

Bergmann, Lutz/Möhrle, Roland/Herb, Armin, Datenschutzrecht. Kommentar Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, bereichsspezifischer Datenschutz, 51. Ergänzungslieferung, Stuttgart, München u. a. 2016 (zitiert: *Bergmann/Möhrle/Herb*, BDSG).

Bergt, Matthias, Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, 555–561.

Beyvers, Eva, Datenschutzrecht: Anwendbarkeit nationalen Rechts auf ausländische Gesellschaft. EuGH (Dritte Kammer), Urt. v. 1.10.2015 – C-230/14 (Weltimmo/Nemzeti Adatvédelmi és Információszabadság Hatóság). Anmerkung, EuZW 2015, 912–917.

Bodoni, Stephanie, If Trump Spoils Privacy Pact, We'll Pull It, EU Official Warns, abrufbar unter https://www.bloomberg.com/news/articles/2017-03-02/if-trump-spoils-privacy-pact-we-ll-pull-it-eu-official-warns (abgerufen am 13.10.2017).

Borges, Georg, Datentransfer in die USA nach Safe Harbor, NJW 2015, 3617–3621.

Bräutigam, Peter/Schmidt-Wudy, Florian, Das geplante Auskunfts- und Herausgaberecht des Betroffenen nach Art. 15 der EU-Datenschutzgrundverordnung. Ein Diskussionsbeitrag zum anstehenden Trilog der EU-Gesetzgebungsorgane, CR 2015, 56–63.

Breyer, Patrick, Personenbezug von IP-Adressen, ZD 2014, 400–405.

Buchner, Benedikt, Message to Facebook, DuD 2015, 402–405.

Buchner, Benedikt, Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsinstrument zum Kommerzialisierungsinstrument, DuD 2010, 39–43.

Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.

Bußmann, Hadumod (Hrsg.), Lexikon der Sprachwissenschaft, 4. Auflage, Stuttgart 2008.

Calliess, Christian/Ruffert, Matthias, (Hrsg.), EUV/AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta. Kommentar, 5. Auflage, München 2016 (zitiert: *Bearbeiter(in)*, in: Calliess/Ruffert, EUV/AEUV).

Chaabane, Abdelberi/Kaafar, Mohamed Ali/Boreli, Roksana/Davis, Donna M., Big Friend is Watching You: Analyzing Online Social Networks Tracking Capabilities, in: Association for Computing Machinery (Hrsg.), WOSN'12. Proceedings of the ACM Workshop on Online Social Networks, New York 2012, S. 7–12.

Chemerinsky, Erwin, Constitutional Law, 4th edition, New York 2013.

Clinton, William J./Gore, Albert Jr., Framework for Global Electronic Commerce, abrufbar unter https://clinton4.nara.gov/WH/New/Commerce/read.html (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo (Hrsg.), Bundesdatenschutzgesetz. Kompaktkommentar zum BDSG, 4. Auflage, Frankfurt a. M. 2014 (zitiert: *Bearbeiter(in)*, in: DKWW, BDSG).

Department of Commerce, Privacy Shield Program. How to Join Privacy Shield (part 1), abrufbar unter https://www.privacyshield.gov/article?id=How-to-Join-Privacy-Shield-part-1 (abgerufen am 13.10.2017).

Denti, Leif/Barbopoulos, Isak/Nilsson, Ida/Holmberg, Linda/Thulin, Magdalena/Wendeblad, Malin/Andén, Lisa/Davidsson, Emelie, Sweden´s largest Facebook study, GRI-rapport 2012:3, 1–38, abrufbar unter https://gupea.ub.gu.se/bitstream/2077/28893/1/gupea_2077_28893_1.pdf (abgerufen am 13.10.2017).

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Anordnung gegen Massendatenabgleich zwischen WhatsApp und Facebook, abrufbar unter https://www.datenschutz-hamburg.de/news/detail/article/anordnung-gegen-massendatenabgleich-zwischen-whatsapp-und-facebook.html (abgerufen am 13.10.2017).

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts. Positionen der Bundesbeauftragten für den Datenschutz, abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/DSAnpaUG_Positionspapier.html?cms_templateQueryString=dsanpug&cms_sortOrder=score+desc (abgerufen am 13.10.2017).

Dietrich, Thomas, Rechtsdurchsetzungsmöglichkeiten der DS-GVO. Einheitlicher Rechtsrahmen führt nicht zwangsläufig zu einheitlicher Rechtsanwendung, ZD 2016, 260–266.

Dietrich, Thomas, Canvas Fingerprinting. Rechtliche Anforderungen an neue Methoden der Nutzerprofilerstellung, ZD 2015, 199–204.

Dreier, Thomas/Schulze, Gernot/Specht, Louisa (Hrsg.), Urheberrechtsgesetz. Urheberrechtswahrnehmungsgesetz. Kunsturhebergesetz, 5. Auflage, München 2015 (zitiert: *Bearbeiter(in)*, in: Dreier/Schulze/Specht, UrhR).

Dudenredaktion (Hrsg.), Duden. Deutsches Universalwörterbuch; das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache, 8. Auflage, Berlin 2015.

Düsseldorfer Kreis, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 24./25. November 2010), abrufbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-UmsetzungDatenschutzrichtlinie.html?nn=5217228 (abgerufen am 13.10.2017).

Düsseldorfer Kreis, Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen, abrufbar unter https://www.datenschutz-mv.de/datenschutz/publikationen/informat/formular/OH_Formular.pdf (abgerufen am 13.10.2017).

Eckersley, Peter, How Unique Is Your Browser?, in: Attalah/Hopper (Hrsg.), Privacy Enhancing Technologies. 10th International Symposium, PETS 2010. Berlin, Germany, July 21-23, 2010. Proceedings, Berlin, Heidelberg 2010, S. 1–18.

Eckhardt, Jens, IP-Adresse als personenbezogenes Datum – neues Öl ins Feuer, CR 2011, 339–344.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DS-GVO. Datenschutz-Grundverordnung, Kommentar, München 2017 (zitiert: *Bearbeiter(in)*, in: Ehmann/Selmayr, DSGVO).

Eko, Lyombe, Many Spiders, One Worldwide Web: Towards a Typology of Internet Regulation, 6 Comm. L. & Pol'y 445–484.

Epping, Volker/Hillgruber, Christian (Hrsg.), Beck'scher Online-Kommentar Grundgesetz, 32. Edition, München 2017 (zitiert: *Bearbeiter(in)*, in: BeckOK GG).

Ernst, Stefan, Die Einwilligung nach der Datenschutzgrundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 DSGVO, ZD 2017, 110–114.

Ernst, Stefan, Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, 1917–1919.

Eßer, Martin/Kramer, Philipp/Lewinski, Kai von (Hrsg.), BDSG. Kommentar zum Bundesdatenschutzgesetz; Nebengesetze, 4. Auflage, Köln 2014 (*Bearbeiter(in)*, in: Auernhammer).

Facebook Inc., Annual Report 2016, abrufbar unter https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2016_FINAL.pdf (abgerufen am 13.10.2017).

Faust, Sebastian/Spittka, Jan/Wybitul, Tim, Milliardenbußgelder nach der DS-GVO? Ein Überblick über die neuen Sanktionen bei Verstößen gegen Datenschutz, ZD 2016, 120–125.

Ferretti, Frederico, Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the Winter of Rights?, CMLR 2014, 843–868.

Föhlisch, Carsten/Pilous, Madeleine, Der Facebook Like-Button – datenschutzkonform nutzbar? Analyse und Risikoeinschätzung des „Gefällt mir"-Buttons auf Webseiten, MMR 2015, 631–636.

FTC, Privacy Online: Fair Information Practices. A Report to Congress (May 2000), abrufbar unter https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (abgerufen am 13.10.2017).

FTC, Complying with COPPA: Frequently Asked Questions, abrufbar unter https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Audience (abgerufen am 13.10.2017).

FTC, Enforcing Privacy Promises, abrufbar unter https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises (abgerufen am 13.10.2017).

FTC, Facebook, Inc., abrufbar unter https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc (abgerufen am 13.10.2017).

FTC, GeoCities, abrufbar unter https://www.ftc.gov/enforcement/cases-proceedings/982-3015/geocities (abgerufen am 13.10.2017).

FTC, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser. Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order, abrufbar unter https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (abgerufen am 13.10.2017).

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

FTC, Myspace LLC, In the Matter of, abrufbar unter https://www.ftc.gov/enforcement/cases-proceedings/102-3058/myspace-llc-matter (abgerufen am 13.10.2017).

FTC, U.S.-EU Safe Harbor compliance: Don't run aground, abrufbar unter https://www.ftc.gov/news-events/blogs/business-blog/2015/08/us-eu-safe-harbor-compliance-dont-run-aground (abgerufen am 13.10.2017).

FTC, Wyndham Settles FTC Charges It Unfairly Placed. Consumers' Payment Card Information At Risk, abrufbar unter https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment (abgerufen am 13.10.2017).

Galexia, EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance, abrufbar unter http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf (abgerufen am 13.10.2017).

Gennen, Klaus/Kremer, Sascha, Social Networks und der Datenschutz. Datenschutzrelevante Funktionalitäten und deren Vereinbarkeit mit dem deutschen Recht, ITRB 2011, 59–63.

Gerlach, Carsten, Personenbezug von IP-Adressen, CR 2013, 478–484.

Gersdorf, Hubertus/Paal, Boris P (Hrsg.), Beck'scher Online-Kommentar Informations- und Medienrecht, 15. Edition, München 2017 (zitiert: *Bearbeiter(in)*, in: BeckOK InfoMedienR).

Gola, Peter (Hrsg.), DS-GVO. Datenschutz-Grundverordnung. VO (EU) 2016/679. Kommentar, München 2017 (zitiert: *Bearbeiter(in)*, in: Gola, DSGVO).

Gola, Peter/Lepperhoff, Niels, Reichweite des Haushalts- und Familienprivilegs in der Datenverarbeitung. Aufnahme und Umfang der Ausnahmeregelung der in der DS-GVO, ZD 2016, 9–12.

Gola, Peter/Klug, Christoph/Körffer, Barbara/Schomerus, Rudolf (Hrsg.), Bundesdatenschutzgesetz. Kommentar, 12. Auflage, München 2015 (zitiert: *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG).

Gola, Peter/Schulz, Sebastian, Der Entwurf für eine EU-Datenschutz-Grundverordnung – eine Zwischenbilanz, RDV 2013, 1–7.

Gola, Peter/Schulz, Sebastian, DS-GVO – Neue Vorgaben für den Datenschutz bei Kindern? Überlegungen zur einwilligungsbasierten Verarbeitung von personenbezogenen Daten Minderjähriger, ZD 2013, 475–481.

Golla, Sebastian J., Säbelrasseln in der DS-GVO: Drohende Sanktionen bei Verstößen gegen die Vorgaben zum Werbedatenschutz, RDV 2017, 123–128.

Grabenwarter, Christoph (Hrsg.), Europäischer Grundrechteschutz, Baden-Baden 2014.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.), Das Recht der Europäischen Union. Band IV. Sekundärrecht, 40. Ergänzungslieferung, München 2009 (zitiert: *Bearbeiter(in)*, in: Grabitz/Hilf/Nettesheim).

Grant, Jon E./Chamblerlain, Samuel R., Expanding the Definition of Addiction: DSM-5 vs. ICD-11, CNS Spectrums 2016, 300–303.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Grau, Timon/Granetzny, Thomas, EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?, NZA 2016, 405–410.

Groeben, Hans von der/Schwarze, Jürgen/Hatje, Armin (Hrsg.), Europäisches Unionsrecht. Vertrag über die Europäische Union – Vertrag über die Arbeitsweise der Europäischen Union – Charta der Grundrechte der Europäischen Union, 7. Auflage, Baden-Baden 2015 (*Bearbeiter(in)*, in: Groeben/Schwarze/Hatje, Europäisches Unionsrecht).

Grote, Paul A., Purging Contempt: Eliminating the Distinction between Civil and Criminal Contempt, 88 Wash. U. L. Rev. 1247–1280.

Guedes, Eduardo/Sancassiani, Frederica/Carta, Mauro Giovani/Campos, Carlos/Machado, Sergio/Spear King, Anna Lucia/Nardi, Antonio Egidio, Internet Addiction and Excessive Social Networks Use: What About Facebook?, Clin Pract Epidemiol Ment Health 2016, 43–48.

Heberlein, Annemarie/Bleich, Stefan, Neurobiologische Grundlagen des Wahlverhaltens bei Abhängigkeitserkrankungen, Die Psychiatrie 2013, 239–242.

Heckmann, Dirk/Starnecker, Tobias, Kein Land in Sicht – das Dilemma des Safe-Harbor-Urteils, jM 2016, 58–61.

Heckmann, Dirk (Hrsg.), Juris PraxisKommentar Internetrecht. Telemediengesetz. E-Commerce. E-Government, 5. Auflage, Saarbrücken 2017 (zitiert: *Bearbeiter(in)*, in: Heckmann, jurisPK-Internetrecht).

Heise Medien GmBH & Co. KG, 2 Klicks für mehr Datenschutz, abrufbar unter https://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html (abgerufen am 13.10.2017).

Herbrich, Tilman Walter/Beyvers, Eva Miriam Alexandra, Anwendbares Recht bei Bezugnahme auf materielles Datenschutzrecht. Eine kritische Würdigung der Rechtslage, RDV 2016, 3–10.

Herbrich, Tilman Walter, VG Hamburg: Keine Anwendbarkeit deutschen Datenschutzrechts auf Facebook. Anmerkung, ZD 2016, 243–250.

Hoeren, Thomas, Und der Amerikaner wundert sich …– Das Google-Urteil des EuGH, ZD 2014, 325–326.

Hoffmann, Bernd von/Thorn, Karsten/Firsching, Karl, Internationales Privatrecht. Einschließlich der Grundzüge des internationalen Zivilverfahrensrechts, 9. Auflage, München 2007.

Hoffmann, Christian/Schulz, Sönke E./Brackmann, Franziska, Die öffentliche Verwaltung in den sozialen Medien? Zulässigkeit behördlicher Facebook-Fanseiten, ZD 2013, 122–126.

Hondius, Frits W., A Decade of International Data Protection, NILR 1983, 103–128.

Hornung, Gerrit/Müller-Terpitz, Ralf, Rechtshandbuch Social Media, Heidelberg 2015.

Hornung, Gerrit, Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012, ZD 2012, 99–106.

Hullen, Nils, LG Berlin, Beschluss vom 14.3.2011 - 91 O 25/11. Anmerkung, MMR 2011, 387–389.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Imhof, Ralf, One-to-One-Marketing im Internet – Das TDDSG als Marketinghindernis, CR 2000, 110–117.

Iraschko-Luscher, Stephanie/Kiekenbeck, Pia, Internetbewertungen von Dienstleistern – praktisch oder kritisch? Meinungsäußerungen zu Lehrer, Arzt & Co. vor dem Hintergrund des § 30a BDSG, ZD 2012, 261–265.

Jandt, Silke/Roßnagel, Alexander, Datenschutz in Social Networks. Kollektive Verantwortlichkeit für die Datenverarbeitung, ZD 2011, 160–166.

Jandt, Silke/Roßnagel, Alexander, Social Networks für Kinder und Jugendliche. Besteht ein ausreichender Datenschutz?, MMR 2011, 637–642.

Jansen, Jonas, Geheimdienstüberwachung. So können Sie nachprüfen, ob Sie ausgespäht wurden, in: Frankfurter Allgemeine Zeitung v. 19.12.2015, abrufbar unter http://www.faz.net/aktuell/feuilleton/debatten/privacy-international-zeigt-ueberwachung-durch-gchq-13437376.html (abgerufen am 13.10.2017).

Jarass, Hans D., Charta der Grundrechte der Europäischen Union. Unter Einbeziehung der vom EuGH entwickelten Grundrechte, der Grundrechtsregelungen der Verträge und der EMRK. Kommentar, 3. Auflage, München 2016 (zitiert: *Jarass*, GrCh).

Jaspers, Andreas, Die EU-Datenschutz-Grundverordnung. Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens, DuD 2012, 571–575.

Jülicher, Tim/Röttgen, Charlotte/Schönfeld, Max von, Das Recht auf Datenübertragbarkeit. Ein datenschutzrechtliches Novum, ZD 2016, 358–362.

Kampert, David, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, Hamburg 2016.

Kamp, Meike/Rost, Martin, Kritik an der Einwilligung. Ein Zwischenruf zu einer fiktiven Rechtsgrundlage in asymmetrischen Machtverhältnissen, DuD 2013, 80–84.

Karg, Moritz, EuGH: Anwendbares nationales Datenschutzrecht und Zuständigkeit der Aufsichtsbehörden – Weltimmo. Anmerkung, ZD 2015, 580–585.

Karg, Moritz, IP-Adressen sind personenbezogene Verkehrsdaten, MMR-Aktuell 2011, 315811.

Kartheuser, Ingemar/Schmitt, Florian, Der Niederlassungsbegriff und seine praktischen Auswirkungen. Anwendbarkeit des Datenschutzrechts eines Mitgliedstaats auf ausländische EU-Gesellschaften, ZD 2016, 155–159.

Kaufhold, Sylvia, Internationale Webshops – anwendbares Vertrags- und AGB-Recht im Verbraucherverkehr, EuZW 2016, 247–252.

Keppeler, Lutz Martin, Was bleibt vom TMG-Datenschutz nach der DS-GVO? Lösung und Schaffung von Abgrenzungsproblemen im Multimedia-Datenschutz, MMR 2015, 779-783.

Kipker, Dennis-Kenji/Voskamp, Friederike, Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung, DuD 2012, 737–742.

Kirchberg-Lennartz, Barbara/Weber, Jürgen, Ist die IP-Adresse ein personenbezogenes Datum?, DuD 2010, 479–481.

Klar, Manuel, Die extraterritoriale Wirkung des neuen europäischen Datenschutzrechts, DuD 2017, 533–537.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Klar, Manuel/Kühling, Jürgen, Privatheit und Datenschutz in der EU und den USA – Kollission zweier Welten?, AöR 2016, 165–224.

Klar, Manuel, Private Videoüberwachung unter Miterfassung des öffentlichen Raums. EuGH (4. Kammer), Urteil vom 11.12.2014 – C-212/13 (Ryneš/Úřad pro ochranu osobních údajů). Anmerkung, NJW 2015, 463– 465.

Klar, Manuel, Räumliche Anwendbarkeit des (europäischen) Datenschutzrechts. Ein Vergleich am Beispiel von Satelliten-, Luft- und Panoramastraßenaufnahmen, ZD 2013, 109–115.

Klar, Manuel, Datenschutzrecht und die Visualisierung des öffentlichen Raums, Berlin 2012.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015 zur Verfolgung des Nutzerverhaltens im Internet, abrufbar unter https://www.datenschutz-bayern.de/dsbk-ent/DSK_88p-Cookies.html (abgerufen am 13.10.2017).

Korff, Douwe, Der EG-Richtlinienentwurf über Datenschutz und „anwendbares Recht". Übersetzung vom Englischen ins Deutsche von M.A. Desirée Zolotas, RDV 1994, 209–217.

Kranig Thomas, Deutsch-amerikanischer Datenschutztag. Tagungsbericht zur Veranstaltung am 10.5.2012 in München, ZD-Aktuell 2012, 02910.

Kremer, Sascha, Datenschutzerklärungen von Social Media Diensten: Anwendbares Recht und AGB-Kontrolle, RDV 2014, 73–83.

Kreutzer, Ralf T./Rumler, Andrea/Wille-Baumkauff, Benjamin, B2B-Online-Marketing und Social Media. Ein Praxisleitfaden, Wiesbaden 2015.

Krohm, Niclas, Abschied vom Schriftformgebot der Einwilligung. Lösungsvorschläge und künftige Anforderungen, ZD 2016, 368–373.

Krönke, Christoph, Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 2016, 319–351.

Krügel, Tina/Pfeiffenbring, Julia/Pieper, Fritz-Ulli, „Social Sharing" via Twitter und Datennutzung durch Dritte: Drum prüfe, wer sich ewig bindet?, K&R 2014, 699–703.

Kühling, Jürgen, Neues Bundesdatenschutzgesetz – Anpassungsbedarf bei Unternehmen, NJW 2017, 1985–1990.

Kühling, Jürgen/Buchner, Benedikt, Die Einwilligung in der Datenschutzordnung 2018, DuD 2017, 544–548.

Kühling, Jürgen/Buchner, Benedikt (Hrsg.), Datenschutz-Grundverordnung. Kommentar, München 2017 (zitiert: *Bearbeiter(in)*, in: Kühling/Buchner, DSGVO).

Kühling, Jürgen/Klar, Manuel, EuGH, Urt. v. 19.10.2016, Rs. C-582/14 – Breyer. Anmerkung, ZD 2017, 27–29.

Kühling, Jürgen/Martini, Mario/Heberlein, Johanna/Kühl, Benjamin/Nink, David/Weinzierl, Quirin/Wenzel, Michael, Die Datenschutz-Grundverordnung und das

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf, Münster 2016.

Kühling, Jürgen/Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 488–454.

Kühling, Jürgen/Heberlein, Johanna, EuGH „reloaded": „unsafe harbor" USA vs. „Datenfestung" EU, NVwZ 2016, 7–12.

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios, Datenschutzrecht, 3. Auflage, Heidelberg 2015.

Kühling, Jürgen/Schall, Tobias, WhatsApp, Skype & Co. – OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts. "Level playing field" de lege lata oder de lege ferenda?, CR 2015, 641–655.

Kühling, Jürgen, Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz, EuZW 2014, 527–532.

Kühling, Jürgen, Die Nicht-Vorlage als Bärendienst – Plädoyer für eine höhere Kommunikationsfreude im Mehrebenensystem, EuZW 2013, 641–642.

Kühling, Jürgen/Klar, Manuel, Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, 3611–3617.

Kühling, Jürgen, Auf dem Weg zum vollharmonisierten Datenschutz!?, EuZW 2012, 281–282.

Kühnl, Christina, Persönlichkeitsschutz 2.0. Profilbildung und -nutzung durch Soziale Netzwerke am Beispiel von Facebook im Rechtsvergleich zwischen Deutschland und den USA, Berlin 2016.

Kurz, Constanze/Rieger, Frank, Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen, Frankfurt a. M. 2012.

Kuss, Daria J./Griffiths, Mark D., Online Social Networking and Addiction – A Review of the Psychological Literature, Int J Environ Res Public Health. 2011, 3528–3552.

Lammenett, Erwin, Praxiswissen Online-Marketing. Affiliate- und E-Mail-Marketing, Suchmaschinenmarketing, Online-Werbung, Social Media, Facebook-Werbung, 6. Auflage, Wiesbaden 2017.

Laue, Philip/Nink, Judith/Kremer, Sascha, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016.

Laue, Philip, Öffnungsklauseln in der DS-GVO – Öffnung wohin?, ZD 2016, 463–467.

Lee, Edward, The Right to Be Forgotten v. Free Speech, 12 J. L. Pol'y for Info. Soc'y 85.

Lewinski, Kai von/Herrmann, Christoph, Cloud vs. Cloud – Datenschutz im Binnenmarkt. Verantwortlichkeit und Zuständigkeit bei grenzüberschreitender Datenverarbeitung, ZD 2016, 467–474.

Lewinski, Kai von, Privacy Shield – Notdeich nach dem Pearl Harbor für die transatlantischen Datentransfers, EuR 2016, 405–421.

Lorenz, Bernd, Das Schriftformerfordernis für das Veröffentlichen von Bildnissen. Verhältnis der Datenschutzgesetze zum KUG, ZD 2012, 367–371.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Lundevall Unger, Patrick/Tranvik, Tommy, Was sind personenbezogene Daten? Die Kontroverse um IP-Adressen, ZD-Aktuell 2012, 03004.

Maisch, Michael Marc, Informationelle Selbstbestimmung in Netzwerken. Rechtsrahmen, Gefährdungslagen und Schutzkonzepte am Beispiel von Cloud Computing und Facebook, Berlin 2015.

Mantz, Reto/Spittka, Jan, Speicherung von IP-Adressen beim Besuch einer Website. EuGH (2. Kammer), Urteil vom 19.10.2016 – C-582/14 (Breyer/Deutschland). Anmerkung, NJW 2016, 3579–3583.

Martini, Mario/Fritzsche, Saskia, Mitverantwortung in sozialen Netzwerken. Facebook-Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, NVwZ-Extra 2015, 1–16.

Maunz, Theodor/Dürig, Günter (Hrsg.), Grundgesetz. Kommentar, 78. Ergänzungslieferung, München 2016.

McDonald, Aleecia M./Cranor, Lorrie Faith, A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookies, 2011 I/S: J.L. & Pol'y for Info. Soc'y 639–687.

Meyerdierks, Per, Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8–13.

Michl, Walther, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 2017, 349–353.

Mohan, Vivek/Villasenor, John, Mohan/Villasenor, Decrypting the fifth Amendment: The limits of self-incrimination in the digi-tal era, 15 U. Pa. J. Const. L. Height. Scrutiny 11–28.

Möhrke-Sobolewski, Christine/Klas, Benedikt, Zur Gestaltung des Minderjährigendatenschutzes in digitalen Informationsdiensten, K&R 2016, 373–378.

Monreal, Manfred, „Der für die Verarbeitung Verantwortliche" – das unbekannte Wesen des deutschen Datenschutzrechts. Mögliche Konsequenzen aus einem deutschen Missverständnis, ZD 2014, 611–615.

Moos, Flemming/Rothkegel, Tobias, Speicherung von IP-Adressen beim Besuch einer Internetseite. EuGH, Urteil vom 19.10.2016 – C-582/14 – Breyer. Anmerkung, MMR 2016, 842–847.

Moos, Flemming/Schefzig, Jens, „Safe Harbor" hat Schiffbruch erlitten. Auswirkungen des EuGH-Urteils C-362/14 in Sachen Schrems ./. Data Protection Commissioner, CR 2015, 625–633.

Nägele, Thomas/Jacobs, Sven, Rechtsfragen des Cloud Computing, ZUM 2010, 281–292.

National Archives, Federal Register Tutorial, abrufbar unter https://www.archives.gov/federal-register/tutorial/online-html.html (abgerufen am 13.10.2017).

Nebel, Maxi, Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht, ZD 2015, 517–522.

Nguyen, Alexander M., Die zukünftige Datenschutzaufsicht in Europa. Anregungen für den Trilog zu Kap. VI bis VII der DS-GVO, ZD 2015, 265–270.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Nink, Judith/Pohle, Jan, Die Bestimmbarkeit des Personenbezugs. Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze, MMR 2015, 563–567.

OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. OECD-Dok, C(80)58/FINAL (23.09.1980), abrufbar unter http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=114&Lang=en&Book=False (abgerufen am 13.10.2017).

OECD, 2013 OECD Privacy Guidelines, abrufbar unter http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (abgerufen am 13.10.2017).

Olejnik, Lukasz/Tran, Minh-Dung/Castelluccia, Claude, Selling Off Privacy at Auction, Network and Distributed System Security Symposium 2014, abrufbar unter https://www.researchgate.net/publication/269197027_Selling_Off_Privacy_at_Auction (abgerufen am 13.10.2017).

O'Reilly, Dave, Facebook Technical Analysis Report. Prepared for the Data Protection Commissioner (16th December 2011), abrufbar unter https://dataprotection.ie/documents/facebook%20report/final%20report/Appendices.pdf (abgerufen am 13.10.2017).

Paal, Boris P./Pauly, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, München 2017 (zitiert: *Bearbeiter(in)*, in: Paal/Pauly, DSGVO).

Pauly, Daniel A./Ritzer, Christoph/Geppert, Nadine, Gilt europäisches Datenschutzrecht auch für Niederlassungen ohne Datenverarbeitung? Weitreichende Folgen für internationale Konzerne, ZD 2013, 423–426.

Pauly, Daniel A./Ritzer, Christoph, Datenschutz-Novellen: Herausforderungen für die Finanzbranche, WM 2010, 8–17.

Petri, Thomas, Die Safe-Harbor-Entscheidung. Erste Anmerkungen, DuD 2015, 801–805.

Pfeffer, Jürgen/Neumann-Braun, Klaus/Wirz, Dominic, Nestwärme in Bild-vermittelten Netzwerken – am Beispiel von Festzeit.ch, in: Fuhse/Stegbauer (Hrsg.), Kultur und mediale Kommunikation in sozialen Netzwerken. Wiesbaden 2011, S. 125–148.

Piltz, Carlo, Datentransfers nach Safe Harbor: Analyse der Stellungnahmen und mögliche Lösungsansätze, K&R 2016, 1–7.

Piltz, Carlo, Anwendbares Datenschutzrecht: Europäischer Gerichtshof schafft ein wenig mehr Klarheit, abrufbar unter https://www.delegedata.de/2016/07/anwendbares-datenschutzrecht-europaeischer-gerichtshof-schafft-ein-wenig-mehr-klarheit/ (abgerufen am 13.10.2017).

Piltz, Carlo, Störerhaftung im Datenschutzrecht?, K&R 2014, 80–85.

Piltz, Carlo, Der räumliche Anwendungsbereich europäischen Datenschutzrechts. Nach geltendem und zukünftigem Recht, K&R 2013, 292–297.

Piltz, Carlo, Soziale Netzwerke im Internet – Eine Gefahr für das Persönlichkeitsrecht?, Frankfurt a. M. 2013.

Piltz, Carlo, Rechtswahlfreiheit im Datenschutzrecht?, „Diese Erklärung unterliegt deutschem Recht", K&R 2012, 640–645.

Piltz, Carlo, Der Like-Button von Facebook. Aus datenschutzrechtlicher Sicht: „gefällt mir nicht", CR 2011, 657–664.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Polenz, Sven, Die Datenverarbeitung durch und via Facebook auf dem Prüfstand, VuR 2012, 207–213.

Pollmann, Maren/Kipker, Dennis-Kenji, Informierte Einwilligung in der Online-Welt, DuD 2016, 378–381.

Raab, Johannes, Die Harmonisierung des einfachgesetzlichen Datenschutzes, Berlin 2015.

Radlanski, Philip, Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, Tübingen 2016.

Rauer, Nils/Ettig, Diana, Nutzung von Cookies. Rechtliche Anforderungen in Europa und deren Umsetzungsmöglichkeiten, ZD 2014, 27–32.

Reidenberg, Joel R., E-Commerce and Privacy Institute for Intellectual Property & Information Law Symposium: E-Commerce and Trans-Atlantic Privacy, 38 Hous. L. Rev. 717–749.

Renner, Cornelius, Schriftform der Einwilligung nach § 22 KUG? Anmerkung zu BAG, Urteil vom 11. Dezember 2014 – 8 AZR 1010/13, ZUM 2015, 608–610.

Richter, Heiko, Datenschutzrecht: Speicherung von IP-Adressen beim Besuch einer Website. EuGH (Zweite Kammer), Urt. v. 19.10.2016 – C-582/14 (Breyer/Deutschland). Anmerkung, EuZW 2016, 909–914.

Rigaux, François, La loi applicable à la protection des individuals à l'égard du traitement automatisé des données à caratère personnel, 60 Rev. crit. 1980, 443–478.

Roesner, Franziska/Kohno, Tadayoshi/Wetherall, David, Detecting and Defending Against Third-Party Tracking on the Web, 9th USENIX Symposium on Networked Systems Design and Implementation 2012, abrufbar unter https://www.usenix.org/system/files/conference/nsdi12/nsdi12-final17.pdf (abgerufen am 13.10.2017).

Roßnagel, Alexander, Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts, Baden-Baden 2017.

Roßnagel, Alexander/Richter, Philipp/Nebel, Maxi, Besserer Internetdatenschutz für Europa. Vorschläge zur Spezifizierung der DS-GVO, ZD 2013, 103–108.

Rost, Martin, Zur Soziologie des Datenschutzes, DuD 2013, 85–90.

Salbu, Steven R., Corporate Governance, Stakeholder, Accountability, and sustainable peace: The European Union Data Privacy Directive and International Relations, 35 Vand. J. Transnat'l L. 655–695.

Schaffland, Hans-Jürgen/Wiltfang, Noeme, Datenschutz-Grundverordnung (DS-GVO). Kommentar, Ergänzungslieferung 2/2017, Berlin 2017 (zitiert: *Schaffland/Wiltfang*, DSGVO).

Schaffland, Hans-Jürgen/Wiltfang, Noeme (Hrsg.), Bundesdatenschutzgesetz (BDSG). Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Ergänzungslieferung 5/2016, Berlin 2016 (zitiert: *Bearbeiter(in)*, in: Schaffland/Wiltfang, BDSG).

Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechung im Datenschutzrecht, NJW 2016, 1841–1846.

Schild, Hans-Hermann/Tinnefeld, Marie-Theres, Datenschutz in der Union – Gelungene oder missglückte Gesetzesentwürfe?, DuD 2012, 312–317.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Schleipfer, Stefan, Facebook-Like-Buttons. Technik, Risiken und Datenschutzfragen, DuD 2014, 318–324.

Schmidt, Bernd/Babilon, Tobias, Anforderungen an den Einsatz von Cookies, Browser-Fingerprinting und ähnlichen Techniken im deutschen Recht, K&R 2016, 86–91.

Schnabel, Christoph, Die richterrechtliche Dogmatik zur Einwilligung vor dem Hintergrund europarechtlicher Einflüsse des Datenschutzes, ZUM 2008, 657–662.

Schneider, Jochen, Datenschutz nach der EU-Datenschutz-Grundverordnung, München 2017.

Schneider, Mathias, WhatsApp & Co. – Dilemma um anwendbare Datenschutzregeln. Problemstellung und Regelungsbedarf bei Smartphone-Messengern, ZD 2014, 231–237.

Schreiber, Kristina/Kohm, Simon, Rechtssicherer Datentransfer unter dem EU-US-Privacy-Shield? Der transatlantische Datentransfer in der Unternehmenspraxis, ZD 2016, 255–260.

Schrems, Max, Kämpf um deine Daten, Wien 2014.

Schulz, Sebastian, Datenschutz als überindividuelles Interesse? Anmerkungen zur geplanten Reform des UKlaG, ZD 2014, 510–514.

Schwartz, Paul M./Solove, Daniel, Notice and Choice: Implications for Digital Marketing to Youth, Berkeley Media Studies Group. NPLAN/BMSG Meeting Memo, abrufbar unter http://www.changelabsolutions.org/sites/default/files/documents/Notice_and_choice.pdf (abgerufen am 13.10.2017).

Schwartz, Paul M., Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1607–1702.

Schwarze, Jürgen/Becker, Ulrich/Bär-Bouyssière, Bertold (Hrsg.), EU-Kommentar, 3. Auflage, Baden-Baden 2012 (zitiert: *Bearbeiter(in)*, in: Schwarze, EU-Kommentar).

Shaffer, Gregory, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, 25 Yale J. Int'l L. 1–88.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden 2014 (zitiert: *Bearbeiter(in)*, in: Simitis, BDSG).

Sloan, Robert H./Warner, Richard, Beyond Notice and Choice: Privacy, Norms, and Consent. Scholarly Commons @ IIT Chicago-Kent College of Law. Research Paper No. 1-1-2013, abrufbar unter http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1567&context=fac_schol (abgerufen am 13.10.2017).

Solmecke, Christian/Dam, Annika, Wirksamkeit der Nutzungsbedingungen sozialer Netzwerke. Rechtskonforme Lösung nach dem AGB- und dem Urheberrecht, MMR 2012, 71–74.

Soltani, Ashkan/Canty, Shannon/Mayo, Quentin/Thomas, Lauren/Hoofnagle, Chris Jay, Flash Cookies and Privacy, 2010 AAAI Spring Symposium Series, abrufbar unter http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1070/1505 (abgerufen am 13.10.2017).

Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien, 3. Auflage, München 2015.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Statista GmbH, Aktuelle Statistiken zum Thema Soziale Netzwerke, abrufbar unter https://de.statista.com/themen/1842/soziale-netzwerke/ (abgerufen am 13.10.2017).

Statista GmbH, Anzahl der monatlich aktiven Nutzer von WhatsApp weltweit in ausgewählten Monaten von April 2013 bis Juli 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/ (abgerufen am 13.10.2017).

Statista GmbH, Anzahl der monatlich aktiven Instagram Nutzer weltweit in ausgewählten Monaten von Januar 2013 bis April 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/300347/umfrage/monatlich-aktive-nutzer-mau-von-instagram-weltweit/ (abgerufen am 13.10.2017).

Statista GmbH, Ranking der größten sozialen Netzwerke und Messenger nach der Anzahl der monatlich aktiven Nutzer (MAU) im August 2017 (in Millionen), abrufbar unter https://de.statista.com/statistik/daten/studie/181086/umfrage/die-weltweit-groessten-social-networks-nach-anzahl-der-user/ (abgerufen am 13.10.2017).

Statista GmbH, Reichweite der größten Social Networks nach dem Anteil der Unique User in Deutschland im 1. Halbjahr 2016, abrufbar unter https://de.statista.com/statistik/daten/studie/157885/umfrage/reichweite-der-groessten-social-networks-in-deutschland/ (abgerufen am 13.10.2017).

Statista GmbH, Statistiken zum Instant-Messaging-Dienst Snapchat, abrufbar unter https://de.statista.com/themen/2546/snapchat/ (abgerufen am 13.10.2017).

Steinrötter, Björn, Kollisionsrechtliche Bewertung der Datenschutzrichtlinien von IT-Dienstleistern. Uneinheitliche Spruchpraxis oder bloßes Scheingefecht?, MMR 2013, 691–694.

Strahilevitz, Lior/Kugler, Matthew B., Is Privacy Policy Language Irrelevant to Consumers?, 45 J. Legal Stud. S69–S95.

Streinz, Rudolf (Hrsg.), EUV/AEUV. Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Auflage, München 2012 (zitiert: *Bearbeiter(in)*, in: Streinz, EUV/AEUV).

Subrahmanyam, Kaveri/Reich, Stephanie M./Waechter, Natalia/Espinoza, Guadalupe, Online and offline social networks: Use of social networking sites by emerging adults, J Appl Dev Psychol 2008, 420–433.

Sydow, Gernot (Hrsg.), Europäische Datenschutz-Grundverordnung. Handkommentar, Baden-Baden 2017 (zitiert: *Bearbeiter(in)*, in: Sydow, DSGVO).

Sydow, Gernot/Kring, Markus, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug. Konkurrierende Leitbilder für den europäischen Rechtsrahmen, ZD 2014, 271–276.

Taeger, Jürgen/Gabel, Detlev (Hrsg.), Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Auflage, Frankfurt a. M. 2013 (zitiert: *Bearbeiter(in)*, in: Taeger/Gabel, BDSG).

The American Law Institute (Hrsg.), Restatement of the Law Second, Torts. Volume 3, St. Paul, Minn. 1977.

Thüsing, Gregor/Schmidt, Maximilian/Forst, Gerrit, Das Schriftformerfordernis der Einwilligung nach § 4a BDSG im Pendelblick zu Art. 7 DS-GVO, RDV 2017, 116–122.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

Tsesis, Alexander, The Right to be Forgotten and Erasure: Privacy, data brokers, and the indefinite retention of data, 49 Wake Forest Law Review 433–484.

Twitter Inc., Annual Report 2016, abrufbar unter https://investor.twitterinc.com/annuals-proxies.cfm (abgerufen am 13.10.2017).

ULD, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook (19. August 2011), abrufbar unter https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf (abgerufen am 13.10.2017).

ULD, Positionspapier des ULD zum Urteil des EuGH vom 6.10.2015, C-362/14 (14.10.2015), abrufbar unter https://www.datenschutzzentrum.de/uploads/internationales/20151014_ULD-Positionspapier-zum-EuGH-Urteil.pdf (abgerufen am 13.10.2017).

Vitale, Angela, The EU Privacy Directive and the Resulting Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet, 35 Vand. J. Transnat'l L. 321–358.

Voigt, Paul/Alich, Stefan, Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Websitenbetreiber, NJW 2011, 3541–3544.

Vulin, Danica, Ist das deutsche Schriftformerfordernis zu viel des Guten? Überlegungen zur Umsetzung der europäischen Vorgaben im BDSG, ZD 2012, 414–418.

Walser, Rahel, „Darf ich dein Portemonnaie anschauen?“, in: Neumann-Braun/Autenrieth (Hrsg.), Freundschaft und Gemeinschaft im Social Web. Baden-Baden 2011, S. 83–86.

Wandtke, Artur-Axel/Bullinger, Winfried (Hrsg.), Praxiskommentar zum Urheberrecht, 4. Auflage, München 2014 (zitiert: *Bearbeiter(in)*, in: Wandtke/Bullinger, UrhR).

Warren, Samuel D./Brandeis, Louis D., "The Right to Privacy", 4 Harv. L. Rev. 193–220.

Wedde, Peter, EU-Datenschutz-Grundverordnung. EU-DSGVO. Kurzkommentar mit Synopse BDSG/EU-DSGVO, Frankfurt a. M. 2016 (zitiert: *Wedde*, DSGVO).

Weichert, Thilo, EU-US-Privacy-Shield – Ist der transatlantische Datentransfer nun grundrechtskonform? Eine erste Bestandsaufnahme, ZD 2016, 209–217.

Weichert, Thilo, Wer ist für was im Internet verantwortlich?, ZD 2014, 1–2.

Weinhold, Robert, EuGH: Dynamische IP-Adresse ist personenbezogenes Datum – Folgen der Entscheidung für die Rechtsanwendung, ZD-Aktuell 2016, 05366.

Willmann, Helmut/Messinger, Heinz/Langenscheidt-Redaktion (Hrsg.), Langenscheidts Großwörterbuch der englischen und deutschen Sprache. „Der Kleine Muret-Sanders“. Englisch-Deutsch. Berlin, München 1985.

Wirz, Dominic, Nähe-orientiertes Handeln in den Weiten des Web, in: Neumann-Braun/Autenrieth (Hrsg.), Freundschaft und Gemeinschaft im Social Web. Baden-Baden 2011, S. 134–135.

Schröder, Birgit/Hawxwell, Anne/Münzing, Heike, Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins. Zum Arbeitspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Aktualisierte Fassung vom 7. Oktober 2011. Wissenschaftliche Dienste des Deutschen Bundestages, Az. WD 3- 3000 - 306/11 neu, abrufbar unter

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

https://www.datenschutzzentrum.de/uploads/facebook/WissDienst-BT-Facebook-ULD.pdf (abgerufen am 13.10.2017).

Wissenschaftlicher Dienst des Schleswig-Holsteiner Landtages, „Facebook-Kampagne" des ULD. Stellungnahme. Umdruck 17/2988 (24. Oktober 2011), abrufbar unter http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2988.pdf (abgerufen am 13.10.2017).

Wolber, Tanja, Werbung mit Adressen aus Online-Bestellungen, CR 2003, 859–862.

Wolff, Heinrich Amadeus/Brink, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 19. Edition, München 2017 (zitiert: *Bearbeiter(in)*, in: BeckOK DatenschutzR).

Wolff, Heinrich Amadeus, Schriftliche Stellungnahme zu dem Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und - Umsetzungsgesetz EU – DSAnpUG-EU) – BT-Drs. Drucksache 18/11325. als Vorbereitung für die öffentliche Anhörung vor dem Innenausschuss des Deutschen Bundestages am Montag, den 27. März 2017, von 10:30 bis 12:30 Uhr im Paul-LöweHaus, Raum E400, Konrad-Adenauer-Straße 1, 10557 Berlin, abrufbar unter http://www.cr-online.de/18-4-824-e-data.pdf (abgerufen am 13.10.2017).

Wulf, Hans Markus, Webseiten-Analyse und Datenschutz: Die dynamische IP-Adresse als personenbezogenes Datum, DB 2017, 111–115.

https://doi.org/10.5771/9783845287737
Generiert durch Otto-Friedrich-Universität Bamberg, am 13.07.2020, 18:56:19.
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.