

PHILIP RADLANSKI

Das Konzept der Einwilligung
in der datenschutzrechtlichen
Realität

Internet und Gesellschaft

5

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von
Jeanette Hofmann, Ingolf Pernice,
Thomas Schildhauer und Wolfgang Schulz

5



Philip Radlanski

Das Konzept der Einwilligung
in der datenschutzrechtlichen
Realität

Mohr Siebeck

Dr. Philip Radlanski, LL.M., geboren 1985; 2005–2011 Studium der Rechtswissenschaft in Regensburg und Sheffield, UK; 2011–2014 wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht an der Universität Regensburg (Prof. Dr. Jürgen Kühling, LL.M.); 2012–2013 Master-Studium am King's College London, UK (LL.M. in Intellectual Property and Information Law); 2015 Promotion; 2014–2016 Referendariat am Kammergericht Berlin.

ISBN 978-3-16-154062-2 / eISBN 978-3-16-160500-0 unveränderte eBook-Ausgabe 2021
ISSN 2199-0344 (Internet und Gesellschaft)

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

© 2016 Mohr Siebeck Tübingen. www.mohr.de

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

Das Buch wurde von eplene in Kirchheim/Teck gesetzt, von Gulde-Druck in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Meinen Eltern

Vorwort

Diese Arbeit ist während meiner Zeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht an der Universität Regensburg entstanden. Ich werde diese Zeit als überaus motivierend, inspirierend und von großer Kollegialität geprägt in Erinnerung behalten.

Zuerst bedanken möchte ich mich beim Lehrstuhlinhaber, Herrn Prof. Dr. Jürgen Kühling, LL.M. (Brüssel), meinem Doktorvater. Er war es, der vor einigen Jahren mein Interesse für Informations- und Datenschutzrecht geweckt, und mich seitdem stets optimal unterstützt und gefördert, aber auch gefordert hat. Durch seine nahbare Art, seinen ansteckenden Optimismus, seinen Enthusiasmus für die wissenschaftliche juristische Arbeit und seinen Pragmatismus hat er am Lehrstuhl ein perfektes Klima geschaffen, in fachlicher wie auch in persönlicher Hinsicht. Sein Input aus zahlreichen Besprechungen und Diskussionen war von unschätzbarem Wert und ist natürlich in diese Arbeit eingeflossen. Von ihm habe ich auch über das Fachliche hinaus viel gelernt – vielen Dank!

Ein großer Dank gilt auch Herrn Prof. Dr. Jörg Fritzsche für die Erstellung des Zweitgutachtens. Auch von ihm wurde ich während meiner Zeit als studentischer Mitarbeiter an seinem Lehrstuhl hervorragend gefördert.

Außerdem bedanke ich mich bei Herrn Perry Keller, LL.M. (Harvard), und Herrn Dr. Jan Oster, LL.M. (Berkeley), beide vom King's College London, UK. Mit ihnen habe ich dort während meines LL.M.-Studiums, das ich in den Jahren 2012/13 eingeschoben habe, regelmäßig datenschutzrechtliche Diskussionen geführt, die mir die Anfertigung der in dieser Arbeit enthaltenen Ausführungen zum englischen Recht erheblich erleichtert haben. Besonderer Dank gebührt in diesem Zusammenhang dem Deutschen Akademischen Austauschdienst (DAAD), der mein LL.M.-Studium mit einem Jahresstipendium unterstützt hat.

Weiterhin möchte ich mich bei Frau Prof. Dr. Katherine J. Strandburg von der New York University, NY/USA, bedanken. Als ich im Frühjahr 2012 für drei Monate in New York war, hat sie mich, nachdem ich ihr vom Thema dieser Arbeit berichtet hatte, unkompliziert in die an der NYU wöchentlich zusammenkommende *Privacy Research Group* eingeladen. Dort konnte ich zwölf Wochen lang mit ihr, anderen Datenschutzrechtlern und IT-Praktikern diskutieren und einen Einblick in das US-amerikanische Verständnis von Datenschutz bekommen. Besonderer Dank geht an Frau Prof. Dr. Helen Nissenbaum, ebenfalls

Mitglied der *PRG*, die sich außerhalb der Forschungsgruppe Zeit genommen hat, ein Exposé dieser Arbeit ausgiebig mit mir zu diskutieren.

Außerdem möchte ich mich bei meinem ehemaligen Lehrstuhlkollegen Dr. Manuel Klar für wertvolle Anregungen zu dieser Arbeit bedanken. Dank gebührt auch Dr. Bardia Kian, LL.M. (LSE), mit dem ich insbesondere während unseres gemeinsamen Jahres in London oft über die datenschutzrechtlichen Implikationen des Cloud Computings diskutiert habe. Meinem ehemaligen Kollegen Dr. Philipp Kircher möchte ich für wichtige Hinweise zum gesundheitsrechtlichen Teil dieser Arbeit danken. Weiterhin gebührt Johanna Munzinger Dank für die Korrekturlektüre des Manuskripts.

Last but not least bedanke ich mich bei meinen Eltern, die mich seit jeher mit all ihrer Großzügigkeit und Liebe bedingungslos unterstützen – bei allem, was ich mir vornehme, so auch bei dieser Arbeit. Ohne ihren Rückhalt und ihre Hilfe hätte ich noch nicht einmal die Voraussetzungen erlangt, um mit dieser Arbeit überhaupt beginnen zu können. Ihnen ist diese Arbeit gewidmet.

Die Arbeit wurde im Februar 2015 von der Fakultät für Rechtswissenschaft der Universität Regensburg als Dissertation angenommen. Die mündliche Prüfung fand am 12.05.2015 in Regensburg statt.

Sydney, im Oktober 2015

Philip Radlanski

Inhaltsverzeichnis

<i>Erstes Kapitel: Einführung</i>	1
A. Motive und Zielrichtung der Untersuchung	1
I. Stand der Forschung	1
1. Bisherige Publikationen	2
2. Bisher unerforschte Fragestellungen	3
II. Schwerpunkt der Untersuchung	3
1. Referenzgebiete	4
a. Arbeitswelt	4
b. Neue Medien	5
c. Gesundheitsbereich	5
2. Äußere Einflüsse	5
a. EU-rechtliche Perspektive	5
b. Globale Perspektive	7
B. Gang der Untersuchung	8
 <i>Zweites Kapitel: Grundstrukturen der Einwilligung</i>	 10
A. Begriffsdefinition	10
B. Voraussetzungen für eine wirksame Einwilligung	11
I. Freiwilligkeit	12
1. Gefährdung durch vis absoluta und vis compulsiva	13
2. Gefährdung durch Drohung	13
3. Gefährdung durch Machtasymmetrie	14
4. Gefährdung durch Abhängigkeit von einem Produkt oder einer Dienstleistung	14
5. Gefährdung durch übermäßige Anreize	14
6. Gefährdung durch sozialen Druck	15
7. Zusammenfassung	16
II. Informiertheit	16
 <i>Drittes Kapitel: Die datenschutzrechtliche Realität</i>	 18
A. Allgemeines	18
I. Formulärmäßige Einwilligungen	18

1. Definition von Opt-in und Opt-out	18
2. Verhalten der Betroffenen	20
II. Kommerzialisierung der Einwilligung	21
B. Referenzgebiete	21
I. Arbeitswelt	22
1. Machtasymmetrie aufgrund struktureller Unterlegenheit	22
2. Angewiesenheit des Betroffenen auf einen Arbeitsplatz	22
3. Legitimierung des Datenumgangs durch Betriebsvereinbarungen	23
II. Neue Medien	23
1. Digitale Datenverarbeitungsprozesse und deren Risiken	24
a. Big Data	24
(1) Definition	24
(2) Verarbeitungsmethode: Data Mining	25
(a) Definition	25
(b) Beispielfälle	26
(aa) Finanzsektor	26
(bb) Marketing	26
(cc) Kriminalitätsprävention	27
b. Cloud Computing	28
c. Datenverarbeitungen beim Internetsurfen	30
(1) Cookies	30
(2) Internetsuchmaschinen	30
(3) Behavioural Advertising	31
d. Verarbeitung von Geodaten	31
e. Vorschau: Ubiquitous Computing	33
2. Koppelung von Angeboten an die Einwilligung des Betroffenen	34
III. Gesundheitsbereich	34
 <i>Viertes Kapitel: Rechtsrahmen</i>	 36
A. Inter- und supranationale Vorgaben	36
I. Völkerrechtlicher Rechtsrahmen	36
II. Supranationaler Rechtsrahmen der EU	39
1. Primärrechtlicher Rechtsrahmen der EU	39
a. EU-Grundrechtecharta	39
b. EU-Gründungsverträge	39
2. Sekundärrechtlicher Rechtsrahmen der EU	40
a. Status Quo	40
(1) Mindeststandard oder Vollharmonisierung?	40
(2) Datenschutzrichtlinie 95/46/EG	43
(a) Wortlaut	43
(aa) „Ohne jeden Zweifel“	43
(bb) „Ohne Zwang“ und „in Kenntnis der Sachlage“	44
(cc) „Ausdrücklich“	44

(b) Telos	45
(c) Genese	45
(d) Systematik	46
(3) Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG	47
(4) Konkretisierung durch die Rechtsprechung	49
(5) Zwischenergebnis	50
b. Novellierung	50
(1) Vorschlag der Kommission für eine Datenschutzgrundverordnung	51
(a) Wortlaut	51
(b) Telos	53
(c) Systematik	53
(aa) Allgemeines	53
(bb) Andere Legitimationsgrundlagen	55
(2) Reaktionen auf den Vorschlag der Kommission	55
(a) Reaktionen auf europäischer Ebene	55
(aa) Artikel-29-Datenschutzgruppe	55
(bb) Europäischer Datenschutzbeauftragter	56
(cc) Albrecht-Report	57
(b) Reaktionen der Mitgliedstaaten	58
(3) DSGVO-LIBE	59
(a) Abkehr vom Ungleichgewicht	60
(b) Koppelungsverbot und Zweckbindung	60
(c) Neufassung der Definition sensibler Daten	61
(d) Sonstige Neuerungen	61
c. Zwischenergebnis zum supranationalen Rechtsrahmen	62
B. Deutscher Rechtsrahmen	63
I. Verfassungsrecht	63
1. Bundesverfassungsrecht	64
a. Gesetzgebungskompetenz	64
b. Grundrechte	64
(1) Das Recht auf informationelle Selbstbestimmung	65
(a) Das Volkszählungsurteil des BVerfG als Ausgangspunkt	65
(b) Schutzbereich	67
(c) Mittelbare Drittwirkung und Schutzpflichtendimension	68
(d) Eingriff	69
(e) Grundrechtliche Qualifikation der Einwilligung	70
(aa) Grundrechtsverzicht?	70
(bb) Grundrechtsausübung?	71
(2) Das „Computergrundrecht“	71
(a) Eingriff in den Schutzbereich	71

(b) Abgrenzung zum Recht auf informationelle Selbstbestimmung	73
(3) Das Fernmeldegeheimnis	74
(a) Eingriff in den Schutzbereich	74
(b) Abgrenzung zum Recht auf informationelle Selbstbestimmung	76
2. Landesverfassungsrecht	77
II. Allgemeiner einfachgesetzlicher Rechtsrahmen	77
1. Bundesebene	78
a. § 4a Abs. 1 BDSG – Allgemeine Norm	78
(1) Wortlaut	78
(a) „Freie Entscheidung“	78
(aa) Gefährdung durch Machtasymmetrie	79
(bb) Gefährdung durch Abhängigkeit	81
(cc) Gefährdung durch übermäßige Anreize	82
(dd) Gefährdung durch sozialen Druck	87
(ee) Zusammenfassung	91
(b) Informationspflichten („hinzuweisen“)	92
(aa) Zweck des Datenumgangs	92
(bb) Folgen der Verweigerung	93
(c) „Schriftform“	93
(d) „Besonders hervorzuheben“	95
(2) Telos	96
(a) Freiwilligkeit	97
(aa) Ausschluss der Einwilligungsmöglichkeit	97
(bb) Widerruf	99
(cc) Koppelungsverbot	100
(dd) Beschränkung der Vertretungsmöglichkeit	102
(ee) Altersgrenze	102
(ff) Sonstige Instrumente	104
(b) Informiertheit	104
(c) Schriftform	106
(d) Besondere Hervorhebung	106
(e) Bestimmtheit	107
(3) Genese	108
(4) Systematik	109
(a) Schriftform	109
(aa) Keine Europarechtswidrigkeit	109
(bb) Elektronische Form	110
(cc) Rechtsfolge eines Verstoßes	111
(b) Besondere Hervorhebung	111
(c) Bestimmtheit	112
(d) Andere Legitimationsgrundlagen	113

(e) Anwendungsbereich	113
(aa) Übermittlung in unsichere Drittstaaten	114
(bb) Entfallen der Vorabkontrolle	115
(cc) Zweckänderung	115
(dd) Umgang mit gesperrten Daten	116
(ee) Veröffentlichung im Rahmen wissenschaftlicher Forschung	116
(f) Rechtsnatur der Einwilligung	117
(aa) Einseitige Erklärung oder schuldvertragliche Einwilligung?	117
(bb) Rechtsgeschäftliche Erklärung, geschäftsähnliche Handlung, Realakt?	120
(5) Auslegungsergebnis	122
b. § 4a Abs. 3 BDSG – Besondere Arten personenbezogener Daten .	123
2. Länderebene	124
III. Rechtliche Regelungen in den Referenzgebieten	124
1. Arbeitswelt	125
a. Prekäre Freiwilligkeit aufgrund strukturellen Ungleichgewichts .	125
(1) Äußerer Druck in Bewerbungssituation rechtlich irrelevant? .	126
(2) Abhängigkeitsverhältnis rechtlich irrelevant?	127
(3) Zusammenhang zu Beschäftigungsverhältnis erforderlich? ..	127
(4) Parallele zum Fragerecht des Arbeitgebers?	128
(5) Das BAG-Urteil vom 11. 12. 2014.	129
b. Legitimationsmöglichkeit durch Betriebsvereinbarung	130
(1) Betriebsvereinbarungen als „andere Rechtsvorschrift“ i. S. d. § 4 Abs. 1 BDSG?	130
(2) Zuungunstenabweichungsmöglichkeit?	131
(a) Auffassung des BAG	131
(b) Literaturmeinungen	132
c. Zwischenzeitlich geplante Novellierung des Beschäftigtendatenschutzes	134
2. Neue Medien	135
a. Gesetzliche Regelungen	136
(1) Telemediendatenschutz	136
(2) Telekommunikationsdatenschutz	137
(a) § 95 TKG – Bestandsdaten	138
(b) § 96 TKG – Verkehrsdaten	138
(c) § 98 TKG – Standortdaten	139
(d) § 105 Abs. 2 S. 2 TKG – Komfortauskunft	140
b. Konkretisierung durch die Rechtsprechung	140
(1) Die „Apple“-Entscheidung des LG Berlin	140
(2) Die „Google“-Entscheidung des LG Berlin	144
(3) Die „Facebook“-Entscheidung des KG Berlin	146

(4) Zusammenfassung	147
3. Gesundheitsbereich	148
a. Geltung der allgemeinen Vorschriften	148
b. Sozialdatenschutz	149
c. Einzelfälle	150
(1) Behandlungssituation	150
(a) Hausärztliche Behandlung	150
(b) Integrierte Versorgung	151
(2) Outsourcing	152
(a) Outsourcing der Abrechnung bei Privatpatienten	152
(b) Outsourcing der Abrechnung bei gesetzlich Versicherten	154
(aa) Das BSG-Urteil vom 10.12.2008	154
(bb) Folgen des BSG-Urteils	155
(3) Medizinische Forschung	156
(a) Allgemeines Datenschutzrecht	156
(b) Spezialgesetzliche Normen	157
(c) Novellierung des EU-Rechtsrahmens	157
(4) Privates Versicherungsrecht	157
(5) E-Health	158
C. Ausgewählte ausländische Rechtsrahmen	158
I. Vereinigtes Königreich	158
1. Völkerrechtliche Quellen	159
2. Nationales Recht	159
a. The Data Protection Act 1998	160
(1) (Einfache) personenbezogene Daten	161
(a) Definition	161
(b) Informiertheit	161
(c) Freiwilligkeit	161
(aa) Druck und unbilliger Einfluss	162
(bb) Reluctant Consent	162
(aaa) Definition	162
(bbb) Abgrenzung	163
(cc) Zwischenergebnis zur Freiwilligkeit	164
(d) Form der Erklärung	164
(2) Sensible Daten („Sensitive Personal Data“)	166
b. The Privacy and Electronic Communications (EC Directive) Regulations 2003	166
3. Anwendungspraxis	167
a. Bindungs- und Steuerungswirkung der ICO-Leitfäden	167
b. Auslegung der Einwilligung durch das ICO	168
(1) Allgemeines	168
(2) Einwilligung im Kontext des Arbeitslebens	168
4. Zusammenfassung	170

II. Vereinigte Staaten von Amerika	171
1. Verfassungsrecht	172
a. Bundesverfassungsrecht	172
(1) Vierter Verfassungszusatz	172
(2) Konkretisierung durch die Rechtsprechung	173
(a) Eingriff in den Schutzbereich	173
(b) Einwilligung	174
(aa) Freiwilligkeit	174
(bb) Informiertheit	175
(cc) Vertretungsmöglichkeit	176
b. Landesverfassungsrecht	176
2. Einfaches Recht	177
a. Grundsatz: Datenverarbeitung ohne Einwilligung zulässig	177
b. Gesetze, die eine Einwilligung erfordern	178
(1) Bundesrecht	178
(a) Privacy Act (1974)	178
(b) Driver's Privacy Protection Act (1994)	179
(c) Health Insurance Portability and Accountability Act (1996)	180
(d) Gramm-Leach-Bliley Act (1999)	181
(e) Electronic Communications Privacy Act (1986)	181
(f) Children's Online Privacy Protection Act (1998)	182
(g) Vorschau: Data Security and Breach Notification Act (2013)	182
(2) Landesrecht am Beispiel Kaliforniens	183
(a) California Medical Privacy Law	184
(aa) Anwendungsbereich	184
(bb) Grundsätzliches Einwilligungserfordernis	184
(cc) Besondere Einwilligungserfordernisse	184
(aaa) Sensible Daten	185
(bbb) Forschung	185
(ccc) Werbung	186
(cc) Ausnahmen vom Einwilligungserfordernis	186
(b) California Online Privacy Protection Act	187
(aa) Möglichkeit für Minderjährige, Inhalte zu löschen	187
(bb) Geplante Vorgaben für Privacy Policies	187
c. Guidelines, die eine Einwilligung empfehlen	188
(1) Federal Trade Commission	188
(a) Aufgabenbereich	189
(b) Behavioural Advertising Principles der FTC	189
(2) Consumer Privacy Bill of Rights des Weißen Hauses	189
d. Common-Law-Rule: Invasion of Privacy	190
e. Zusammenfassung	191

<i>Fünftes Kapitel: Probleme, offene Fragen und Lösungsvorschläge</i> . . .	192
A. Unzulänglichkeit des Rechtsrahmens in Anbetracht der Realität	192
I. Allgemeine Probleme	192
1. Strukturelle Unzulänglichkeiten	193
a. Verbot mit Erlaubnisvorbehalt	193
(1) Kritik am Verbot mit Erlaubnisvorbehalt	193
(2) Stellungnahme	193
b. Kategorisierung nach Datentyp	194
(1) Problem: Kategorisierung nach Typus ist nicht überzeugend	194
(2) Lösungsvorschlag: Risikoabhängige Kategorisierung	196
(a) Vorstellung des Konzepts	196
(aa) Abstellen auf das Risiko einer Datenverarbeitung	196
(bb) Bildung von Kategorien	197
(aaa) Erster Schritt: Bildung von Risikostufen	198
(bbb) Zweiter Schritt: Zuweisung von Fallkonstellationen	199
(cc) Praktische Umsetzung	199
(b) Schwachstellen der risikoabhängigen Kategorisierung	200
(3) Zwischenergebnis	201
c. Verhältnis der verschiedenen Legitimationsgründe zueinander	201
(1) Problem: Verhältnis der Legitimationsgründe ist unklar	201
(a) Gleichrangigkeitsverhältnis ist problematisch	202
(b) Bisher vorgeschlagene Lösungswege	202
(c) Unzulänglichkeiten bisheriger Lösungsvorschläge	203
(2) Neuer Lösungsvorschlag: Subsidiarität der Einwilligung	204
(a) Vorstellung des Konzepts	204
(b) Plädoyer für diesen Ansatz	205
(aa) Meinung bereits ansatzweise im Vordringen	206
(bb) Beschränkung der Einwilligung ist positiver Effekt	206
(cc) Betroffener wird nicht entmündigt	207
(aaa) Alternative: Vertragsfreiheit	207
(bbb) Vorteile eines Alternativitätsverhältnisses zur Einwilligung	207
(c) Praktische Umsetzung	209
(3) Zwischenergebnis	209
2. Probleme bei der praktischen Umsetzung	210
a. Überforderung durch Überangebot in der Multioptionengesellschaft	210
b. Freiwilligkeitsdefizite	212
(1) Problem: Verschiedene Einflüsse beeinträchtigen Freiwilligkeit	212
(2) Lösungsvorschläge	212

(a)	Abstimmung von Formulklauseln mit Aufsichtsbehörden	212
(b)	Flächendeckendes Opt-in	213
(c)	Zeitliche Befristung der Einwilligung	214
(d)	Anerkennung des <i>reluctant consent</i>	215
(e)	Anlegen eines objektiven Maßstabs	215
(aa)	Vorstellung des Konzepts	215
(bb)	Plädoyer für diesen Ansatz	216
(cc)	Unzulänglichkeiten dieses Ansatzes	218
(dd)	Zwischenergebnis	218
(f)	Sektorspezifischer Teilausschluss der Einwilligungsmöglichkeit	219
(aa)	Unterscheidung nach Lebens- oder Rechtsbereich ..	219
(bb)	Unterscheidung nach Datentyp	220
(cc)	Unterscheidung nach Risiko	220
(g)	Vollständiger Ausschluss der Einwilligungsmöglichkeit ..	220
(3)	Zwischenergebnis	221
c.	Informationsdefizite	221
d.	Problem: Desinteresse	222
II.	Spezielle Referenzgebiete	223
1.	Arbeitswelt	223
a.	Strukturelle Ungleichheit	223
b.	Legitimationswirkung von Betriebsvereinbarungen	223
2.	Neue Medien	225
a.	Cookies	225
b.	Standortdaten	227
c.	Übermittlung in Drittstaaten	227
3.	Gesundheitsbereich	229
a.	Allgemeines strukturelles Problem	229
b.	Zeitliche Entzerrung von Behandlung und Einwilligung als Lösung?	230
(1)	Übermittlung an Abrechnungsstellen	230
(2)	Teilnahme an Forschungsvorhaben	231
B.	Gesamtlösungsvorschlag	232
I.	Vorstellung eines ganzheitlichen Vorschlags	232
1.	Beschränkung des Anwendungsbereichs	232
2.	Verschärfung der Wirksamkeitsanforderungen	233
a.	Einführung eines objektiven Maßstabs	233
b.	Zeitliche Entzerrung der Einwilligungserklärung	233
c.	Übrige Anforderungen	235
II.	Analyse des gesetzgeberischen Handlungsbedarfs	235
1.	Restrukturierung der Legitimationsgrundlagen	235
2.	Einführung eines objektiven Maßstabes	235

3. Zeitliche Entzerrung	236
4. Übrige Vorgaben	237
5. Formulierungsvorschlag	237
<i>Sechstes Kapitel: Fazit und Ausblick</i>	239
Literaturverzeichnis	243
Monographien und Aufsätze	243
Offizielle Dokumente	254
Nachrichtenbeiträge und Sonstiges	256
Stichwortverzeichnis	261

Erstes Kapitel

Einführung

Die vorliegende Arbeit stellt das Konzept der Einwilligung unter Berücksichtigung der gegenwärtigen datenschutzrechtlichen Realität auf den Prüfstand. Sie behandelt damit ein Thema, das sowohl fundamentale Fragestellungen wie das Recht auf informationelle Selbstbestimmung¹ als auch bereichsspezifische Details, wie beispielsweise die Frage nach der Sensibilität von automatisiert erfassten Ortungsdaten eines Smartphones², zu klären hat.

A. Motive und Zielrichtung der Untersuchung

Im deutschen Datenschutzrecht ist es grundsätzlich verboten, personenbezogenen Daten anderer zu erheben, zu verarbeiten oder zu nutzen („Datenumgang“), es sei denn, es ist erlaubt.³ Jeder rechtmäßige Datenumgang muss sich daher auf eine Legitimationsgrundlage stützen können. Eine mögliche Legitimationsgrundlage ist hierbei die Einwilligung des Betroffenen.

I. Stand der Forschung

Zum Thema der datenschutzrechtlichen Einwilligung existieren bereits eine Reihe von Vorarbeiten.

Es wird im Folgenden auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

¹ Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Näheres siehe unten, S. 65 ff.

² Siehe hierzu unten, S. 31 ff.

³ Sogenanntes „Verbot mit Erlaubnisvorbehalt“, siehe hierzu 4. Kapitel, B. II. 1. Der Begriff ist aus verwaltungsrechtlicher Sicht genau genommen unglücklich gewählt, da er suggeriert, es ginge hierbei um eine behördliche Erlaubnis (vgl. *Petri ZD-Aktuell* 2013, 03161; *Scholz/Sokol*, in: *Simitis* (Hrsg.), *BDSG § 4 Rn. 3*). Eine solche ist im Datenschutzrecht aber gerade nicht erforderlich, wenn ein Legitimationsgrund greift. Der Begriff hat sich allerdings im Datenschutzrecht durchgesetzt und wird daher auch in dieser Untersuchung in diesem Sinne verwendet.

1. Bisherige Publikationen

Mit seiner Habilitationsschrift „Informationelle Selbstbestimmung im Privatrecht“ behandelte Buchner bereits im Jahre 2006 einen Bereich, der auch die datenschutzrechtliche Einwilligung betrifft. Er spricht sich dafür aus, neben dem öffentlich-rechtlichen Datenschutz auch einen privatrechtlichen Datenschutz zu etablieren, der den Interessen der Beteiligten mittels eines privatautonom Interessenausgleichs gerecht wird. Das von Buchner vorgeschlagene Modell unterscheidet sich daher vom derzeit herrschenden Konzept der datenschutzrechtlichen Einwilligung.

Zum Zeitpunkt der Fertigstellung dieser Untersuchung lagen außerdem bereits drei Dissertationen zum Themengebiet vor.⁴

Liedke gibt in seiner Arbeit mit dem Titel „Die datenschutzrechtliche Einwilligung“ aus dem Jahr 2012 einen kompakten Überblick über diejenigen Themen, die bei der datenschutzrechtlichen Einwilligung im deutschen Recht gemeinhin als problematisch angesehen werden.⁵ Er bildet hierzu zwei Schwerpunkte: In einem ersten Teil („Allgemeiner Teil“) stellt er Rechtsnatur, Reichweite und Anforderungen der Einwilligung dar. Außerdem setzt er sich mit der Frage der Widerruflichkeit der Einwilligung, insbesondere der elektronischen Einwilligung, auseinander. Ein zweiter Teil („Besonderer Teil“) ist speziellen Problembereichen gewidmet. Hier wird die datenschutzrechtliche Einwilligung im Beschäftigungsverhältnis und in der Werbung beleuchtet.

Die Dissertation von Rogosch aus dem Jahr 2013 trägt den Titel „Die Einwilligung im Datenschutzrecht“. Sie verfolgt in ihrer Arbeit die These, dass die rechtliche Konzeption der Einwilligung in Deutschland inkonsistent sei.⁶ Hierzu beschreibt sie zunächst unter weitestgehender Ausklammerung EU-rechtlicher Vorgaben die anwendbaren deutschen Vorschriften, bevor sie die einzelnen Wirksamkeitsvoraussetzungen darstellt. Sie schließt mit der Handlungsempfehlung, die Wirksamkeitsvoraussetzungen der Einwilligung zu vereinheitlichen.⁷

Lindner hat ebenfalls im Jahre 2013 ein Werk mit dem Titel „Die datenschutzrechtliche Einwilligung nach §§ 4 Abs. 1, 4a BDSG – ein zukunftsfähiges Institut?“ vorgelegt.⁸ Nach einer Darstellung der europarechtlichen und deutschen Vorgaben arbeitet er die Rechtsfragen, die sich aus dem derzeitigen Einwilligungskonzept ergeben, heraus. So beschäftigt er sich beispielsweise mit Mindestangaben, die datenschutzrechtliche Allgemeine Geschäftsbedingungen enthalten müssen, und erklärt die Folgen einer unwirksamen Einwilligungs-

⁴ Liedke, Einwilligung; Lindner, Einwilligung; Rogosch, Einwilligung.

⁵ Vgl. hierzu auch die Besprechung von *Vulin*, ZD-Aktuell 2012, 03119.

⁶ Vgl. hierzu auch die Besprechung von *Petri*, ZD-Aktuell 2013, 03161.

⁷ Rogosch, Einwilligung, S. 190.

⁸ Vgl. hierzu auch die Besprechung von *Gruber*, DuD 2013, 682.

erklärung. Er schließt mit der Erkenntnis, dass die Einwilligung eine eigenständige und gleichrangige Rechtsgrundlage für die Legitimation von Datenumgang ist, deren zentrales Regelungsinstrument die Informiertheit des Betroffenen ist. De lege ferenda empfiehlt er, eine elektronische Form der Einwilligung vorzusehen und macht weitere Vorschläge zur Form der Einwilligung.

Der Schwerpunkt der bisher veröffentlichten monografischen Untersuchungen liegt in der Prüfung der Einwilligungsanforderungen. Während sich die Arbeiten teilweise auf die Beschreibung und Diskussion der geltenden Rechtslage, Literatur und Rechtsprechung beschränken,⁹ machen andere Autoren durchaus Vorschläge für Veränderungen hinsichtlich der Wirksamkeitsvoraussetzungen der datenschutzrechtlichen Einwilligung.¹⁰ Dass die Einwilligung als Ausdruck des Rechts auf informationelle Selbstbestimmung Bestand haben muss und darüber hinaus einen äußerst weiten Anwendungsbereich aufweist, wird hierbei stets vorausgesetzt.

2. Bisher unerforschte Fragestellungen

Bisher nicht hinreichend untersucht worden ist allerdings die Frage nach der konzeptionellen Legitimierung des Einwilligungsinstruments. Von der Feststellung, dass eine Einwilligung frei und informiert abgegeben worden sein muss, wird in den Vorarbeiten stets direkt zur Frage übergeleitet, wie diese beiden Voraussetzungen in der konkreten rechtlichen Ausformung sichergestellt werden können.

Vorher zu klären wäre allerdings, ob man in der datenschutzrechtlichen Realität überhaupt davon ausgehen sollte, dass Freiwilligkeit und Informiertheit grundsätzlich möglich sind, und nur der Sicherung durch (Verfahrens-)Vorgaben bedürfen.

II. Schwerpunkt der Untersuchung

Leitfrage der vorliegenden Untersuchung ist also: Ist das Konzept der Einwilligung als solches angesichts der datenschutzrechtlichen Realität überhaupt tragfähig? Diese Arbeit untersucht das Konzept der Einwilligung demnach auf einer abstrakteren Ebene. Sie stellt nicht sofort die Frage nach dem *Wie* einer Einwilligung, sondern zunächst nach dem *Ob*.

Hierzu muss als Erstes die datenschutzrechtliche Realität, der das Konzept der Einwilligung gerecht werden soll, untersucht und ihre Risiken aufgezeigt werden.¹¹ Anschließend sind die Anforderungen, die eine wirksame Einwil-

⁹ Liedke, Einwilligung.

¹⁰ Lindner, Einwilligung; Rogosch, Einwilligung.

¹¹ Siehe hierzu unten, S. 18 ff.

ligung nach derzeitiger Rechtslage erfüllen muss, herauszuarbeiten.¹² Hierzu reicht es nicht, ausschließlich den deutschen Rechtsrahmen zu analysieren. Stattdessen müssen alle relevanten Vorgaben auf inter- und (vor allem) supranationaler Ebene beleuchtet werden.¹³ Denn das deutsche Datenschutzrecht ist maßgeblich durch europäisches Sekundärrecht überformt. Überdies steht auf europäischer Ebene eine Novellierung eben dieses sekundärrechtlichen Rechtsrahmens kurz bevor, die wertvolle Einblicke in das europäische Verständnis des Konzepts der Einwilligung erlaubt.¹⁴ Schließlich enthalten die datenschutzrechtlichen Vorgaben bezüglich der Einwilligung oft unbestimmte Rechtsbegriffe, zu deren Auslegung auch andere Rechtsgebiete und – als Vergleich – auch andere Rechtsordnungen¹⁵ als die deutsche herangezogen werden können.

Bei der Untersuchung werden dabei Themen, die von den vorangegangenen Veröffentlichungen bereits behandelt worden sind, nicht im Fokus stehen oder gänzlich ausgespart. Ebenfalls keine tragende Rolle spielt die Unterscheidung in öffentliche und nicht-öffentliche Stellen – auch die geplante Novellierung des europäischen Datenschutzrechts wird nach derzeitigem Stand eine derartige Unterscheidung weiterhin nicht vornehmen.

1. Referenzgebiete

Das Konzept der datenschutzrechtlichen Einwilligung wird besonders in bestimmten Lebensbereichen auf die Probe gestellt. Daher werden drei dieser Bereiche in der vorliegenden Untersuchung besonders herausgestellt und ihre datenschutzrechtlichen Implikationen im Hinblick auf die Einwilligung untersucht. Hierbei handelt es sich um die Arbeitswelt, die Neuen Medien, und den Gesundheitsbereich.

a. Arbeitswelt

Die Arbeitswelt¹⁶ zeichnet sich durch eine strukturelle Ungleichheit zwischen Arbeitgeber und Arbeitnehmer aus. Dies gilt insbesondere während des Bewerbungsprozesses, in dem der Bewerber sich gegen Konkurrenten durchsetzen muss, setzt sich aber auch während des Arbeitsverhältnisses fort. Überdies nimmt die Arbeit einen beträchtliche Zeit im Leben des Betroffenen ein, sodass eventuelle Probleme erhebliche Auswirkungen haben können. Im Hinblick auf die datenschutzrechtliche Einwilligung stellt sich in der Arbeitswelt also vor allem das Problem der Freiwilligkeit.

¹² Siehe hierzu unten, S. 36 ff.

¹³ Siehe hierzu unten, S. 36 ff.

¹⁴ Siehe hierzu unten, S. 50 ff.

¹⁵ Siehe hierzu unten, S. 158 ff.

¹⁶ Siehe hierzu unten, S. 22 f.; S. 125 ff.; S. 223 f.

b. Neue Medien

Neue Medien¹⁷ sind mittlerweile allgegenwärtig. Die wenigsten wissen allerdings, wie sie genau funktionieren und können daher die Risiken, die mit der Nutzung verbunden sind, bestenfalls erahnen. Daher ist schon fraglich, ob die Betroffenen hinreichend informiert sind, um eine Einwilligung zu treffen. Außerdem werden Neue Medien zunehmend unersetzlich. Sind die Betroffenen allerdings auf die Nutzung Neuer Medien angewiesen, so stellt sich die Frage der Freiwilligkeit einer mit der Nutzung verknüpften datenschutzrechtlichen Einwilligung.

c. Gesundheitsbereich

Im Gesundheitsbereich¹⁸ sind die relevanten personenbezogenen Daten oft sensibel, das heißt, sie stellen ein erhebliches Risiko für den Betroffenen dar. Allein aus diesem Grund bedarf es einer genaueren Untersuchung, inwiefern und inwieweit die datenschutzrechtliche Einwilligung des Betroffenen eine taugliche Legitimationsgrundlage für einen entsprechenden Umgang ist. Außerdem stellt sich auch im Gesundheitsbereich die Frage der Freiwilligkeit, etwa, wenn der Betroffene glaubt, seine Verweigerung der datenschutzrechtlichen Einwilligung führe zu einer Verschlechterung der Behandlungsqualität. Überdies befindet sich der Betroffene im Krankenhaus oft in einer Ausnahmesituation, in der ihm die Frage nach seiner datenschutzrechtlichen Einwilligung völlig nebensächlich vorkommen kann.

2. Äußere Einflüsse

Diese Thematik der datenschutzrechtlichen Einwilligung ist allerdings keine nationale, sondern in allen entsprechend entwickelten Regionen der Welt zu beobachten. Daher hat die Frage, ob das Konzept der Einwilligung in der datenschutzrechtlichen Realität (noch) tragfähig ist, eine supranationale und sogar globale Dimension.

a. EU-rechtliche Perspektive

Im Januar 2012 hat die Europäische Kommission einen Entwurf für eine Datenschutzgrundverordnung¹⁹ vorgestellt, die bei Inkrafttreten einen europaweit einheitlichen Standard auch für die Wirksamkeit der datenschutzrechtlichen Einwilligung verankern wird (Art. 7 des Entwurfes). Dieser Entwurf wurde

¹⁷ Siehe hierzu unten, S. 23 ff.; S. 135 ff.; S. 225 ff.

¹⁸ Siehe hierzu unten, S. 34 f.; S. 148 ff.; S. 229 ff.

¹⁹ Siehe hierzu unten, S. 51 ff.

mittlerweile in einer umfangreich überarbeiteten Version vom EU-Parlament angenommen. Nach Verabschiedung der Datenschutzgrundverordnung wird dieser einheitliche Standard nach einer zweijährigen Übergangsfrist verbindlich werden.

Aber bereits heute stellt sich bei der Untersuchung des status' quo die Frage, inwieweit das Datenschutzrecht europarechtlich zwingend vorgegeben ist. Spätestens mit einer Entscheidung²⁰ des Europäischen Gerichtshofs (EuGH) vom November 2011 deutet vieles darauf hin, dass im Hinblick auf die Zulässigkeitsvoraussetzungen von Datenumgang bereits jetzt eine Vollharmonisierung herrscht, sodass von den Mitgliedstaaten lediglich Konkretisierungen vorgenommen werden dürfen.²¹

Die europäische Harmonisierung – gleich, ob bereits bestehend oder erst mit der Datenschutzgrundverordnung vollständig erreicht – kann für den datenschutzrechtlichen Standard in Deutschland allerdings eine Bedrohung darstellen.²² Deutschland verfügt grundsätzlich²³ über einen sehr hohen datenschutzrechtlichen Standard; die vom Bundesverfassungsgericht (BVerfG) aufgestellten Anforderungen an Form und Inhalt von datenschutzrechtlichen Regelungen sind, jedenfalls im öffentlichen Bereich, so präzise wie in wohl keinem anderen Rechtsgebiet.²⁴ Eine Harmonisierung zwischen den europäischen Mitgliedstaaten kann nun auf mehrere Arten erfolgen: Die übrigen Mitgliedstaaten könnten sich dem hohen deutschen Standard anpassen. Dann würde sich aus deutscher Sicht nichts ändern, da der datenschutzrechtliche Standard im Ergebnis gleich bliebe – er würde dann nur nicht mehr maßgeblich im Bundesdatenschutzgesetz (BDSG), sondern in der Datenschutzgrundverordnung verankert sein. Stattdessen könnten sich alle Mitgliedstaaten auch dem Staat mit dem niedrigsten Standard nähern – das würde aber ein Zurückfallen hinter den heutigen Stand bedeuten und ist auch nicht ernsthaft zu erwarten. Schließlich könnte aus den verschiedenen Datenschutzniveaus aller Mitgliedstaaten ein Mittelwert im Form eines Konsens gefunden werden, der dann in der Datenschutzgrundverordnung für alle Mitgliedstaaten verbindlich verankert wird. Aus deutscher Sicht würde dies allerdings ein Absinken des heutigen Stan-

²⁰ *EuGH*, Urt. v. 24. 11. 2011 – Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) und Federación de Comercio Electrónico y Marketing Directo (FECEDM) (C-469/10) gegen die Administración del Estado.

²¹ Siehe hierzu unten, S. 40 ff.

²² Siehe hierzu *Kühling*, Europäisierung des Datenschutzrechts, S. 32 ff., der die Gefahr einer faktischen Schutznivellierung als Folge der Europäisierung des Datenschutzrechts als eher gering einschätzt.

²³ Dass diese Aussage nicht für alle Bereiche gilt, zeigt diese Untersuchung im Hinblick auf die hier ausgewählten Referenzgebiete, in denen nur wenige verfassungsrechtliche Vorgaben existieren, vgl. hierzu unten, S. 125 ff.; S. 135 ff.; S. 148 ff.

²⁴ *Kühling*, Die Verwaltung 2011, 525 (526); näher erläuternd *Kühling/Seidel/Sivridis*, Datenschutzrecht, S. 55 f.

dards bedeuten, da dieser jedenfalls über dem gegebenenfalls neu gefundenen Mittelwert liegt. Und genau darin besteht die zumindest theoretisch denkbare Bedrohung des deutschen Datenschutzniveaus durch die europäische Harmonisierung. Diese Arbeit untersucht diese Bedrohung in Bezug auf das Konzept der Einwilligung, indem sie der Frage nachgeht, ob und inwieweit es hinsichtlich der Reichweite, des Stellenwerts und der Anforderungen der datenschutzrechtlichen Einwilligung Unterschiede zwischen dem Vereinigten Königreich, das exemplarisch als Vergleichsland herangezogen wird, und Deutschland gibt, und wie diese unterschiedlichen Auffassungen gegebenenfalls Niederschlag in einer einheitlichen europarechtlichen Vorgabe finden können, die weder eine individuelle Lockerung noch eine individuelle Verschärfung durch die Mitgliedstaaten erlaubt.²⁵

b. Globale Perspektive

In globaler Hinsicht stellt sich die spannende Frage, wie es sich datenschutzrechtlich auswirkt, dass beispielsweise US-amerikanische IT-Unternehmen wie Apple oder Google ihre in den USA präkonfigurierte Hardware auf dem deutschen Markt anbieten, die Nutzer bei der Inbetriebnahme in Datenerhebung und -verarbeitung „einwilligen“, und der US-Konzern dann aufgrund seiner voreingestellten Konfiguration des Gerätes gewisse Daten (wie beispielsweise den Aufenthaltsort eines Smartphones²⁶) vorbei am deutschen und europäischen Datenschutzrecht, in die USA übermittelt. Gleiches gilt nicht nur für Hardware, sondern auch für Dienstleistungen, die US-amerikanische Anbieter in Deutschland und Europa anbieten, die allerdings eine Übermittlung von personenbezogenen Daten in die USA vorsehen. Eine neue Dimension bekam dieser Aspekt durch die Enthüllungen des Wistleblowers Edward Snowden, der aufdeckte, dass US-amerikanische Geheimdienste wie die NSA im Rahmen des PRISM-Programms Zugriff auf diese Datensammlungen hatten (oder noch haben).²⁷ Auch diese Gefahren und Einflüsse müssen bei der Frage, ob das Konzept der Einwilligung in der datenschutzrechtlichen Realität (noch) tragfähig ist, berücksichtigt werden.

²⁵ Siehe hierzu unten, S. 158 ff.

²⁶ Siehe hierzu unten, S. 31 f.

²⁷ Siehe hierzu unten, S. 28 f.

B. Gang der Untersuchung

Im zweiten Kapitel werden zunächst gewisse Grundmechanismen der datenschutzrechtlichen Einwilligung „vor die Klammer gezogen“. Deren Verständnis ist erforderlich, um die nachfolgenden Ausführungen zu verstehen. Hier werden, unabhängig vom Wortlaut bestimmter Regelungen, grundlegendere Aspekte des Konzepts der Einwilligung untersucht: Welche Komponenten weist eine wirksame Einwilligung auf?²⁸ Welchen Einwirkungen sind diese Komponenten ausgesetzt?²⁹

Anschließend wird die datenschutzrechtliche Realität dargestellt, und herausgearbeitet, welche Herausforderungen diese Realität an das Datenschutzrecht stellt (drittes Kapitel). Hierbei wird insbesondere auf drei Gebiete eingegangen, die im Folgenden als Referenzgebiete dienen sollen, um das Konzept der Einwilligung einer konkreteren Prüfung unterziehen zu können: Die Arbeitswelt,³⁰ der Bereich der Neuen Medien³¹ und der Gesundheitsbereich³².

Das vierte Kapitel widmet sich der Untersuchung des bestehenden Rechtsrahmens. Hierbei wird systematisch anhand der verschiedenen Regelungsebenen vorgegangen: Zunächst wird der inter- und supranationale Rechtsrahmen³³ untersucht, was insbesondere im Hinblick auf die anstehende Novellierung³⁴ des supranationalen Rahmens in Form der Datenschutzgrundverordnung aufschlussreich ist. Anschließend werden die deutschen Vorschriften und Entscheidungen unter die Lupe genommen, und zwar zunächst das Verfassungsrecht³⁵ und anschließend das allgemeine Bundes- und Landesrecht,³⁶ bevor sich den Spezialregelungen der drei Referenzgebiete, also der Arbeitswelt³⁷, den Neuen Medien³⁸, und dem Gesundheitsbereich³⁹, zugewandt wird. Um die eingangs dargestellten Einflüsse von außerhalb angemessen bearbeiten zu können, erfolgt anschließend eine Darstellung des Konzepts der datenschutzrechtlichen Einwilligung im Vereinigten Königreich⁴⁰ und in den Vereinigten Staaten von Amerika⁴¹.

²⁸ Siehe hierzu unten, S. 11 ff.

²⁹ Siehe hierzu unten, S. 13 ff.

³⁰ Siehe hierzu unten, S. 22 f.

³¹ Siehe hierzu unten, S. 23 ff.

³² Siehe hierzu unten, S. 34 f.

³³ Siehe hierzu unten, S. 36 ff.

³⁴ Siehe hierzu unten, S. 50 ff.

³⁵ Siehe hierzu unten, S. 63 ff.

³⁶ Siehe hierzu unten, S. 77 ff.

³⁷ Siehe hierzu unten, S. 125 ff.

³⁸ Siehe hierzu unten, S. 135 ff.

³⁹ Siehe hierzu unten, S. 148 ff.

⁴⁰ Siehe hierzu unten, S. 158 ff.

⁴¹ Siehe hierzu unten, S. 171 ff.

Im fünften Kapitel werden die offenen Fragen und Probleme, die sich aus der Zusammenschau von Realität und Rechtsrahmen ergeben, herausgearbeitet. Hierbei handelt es sich sowohl um allgemeine Probleme⁴² als auch um in den in dieser Arbeit besonders beleuchteten Referenzgebieten jeweils spezifische Probleme⁴³. Dargestellt werden sowohl die strukturellen Unzulänglichkeiten⁴⁴ als auch Probleme bei der Anwendung des Konzepts in der Praxis⁴⁵. Nach Darstellung der jeweiligen Problematik werden Lösungsvorschläge entwickelt und diskutiert, bevor ein Gesamtlösungsvorschlag vorgestellt wird.

Das sechste Kapitel schließt die Arbeit mit Schlussbetrachtungen ab.

⁴² Siehe hierzu unten, S. 192 ff.

⁴³ Siehe hierzu unten, S. 223 ff.

⁴⁴ Siehe hierzu unten, S. 193 ff.

⁴⁵ Siehe hierzu unten, S. 210 ff.

Zweites Kapitel

Grundstrukturen der Einwilligung

Bevor im vierten Kapitel für das Konzept der Einwilligung maßgebliche Rechtsrahmen untersucht werden können, sind in diesem Kapitel zunächst einige Grundstrukturen dieses Konzepts zu klären. Ein „vor-die-Klammer-Ziehen“ ist deshalb indiziert, weil es sich bei diesen Strukturen um grundlegende Eigenschaften der Einwilligung handelt, die unabhängig von einer konkreten Ausgestaltung durch eine datenschutzrechtliche Vorschrift existieren und sich hieraus allgemeine Grundprobleme ergeben, deren Herausstellung sinnvoll erscheint, bevor der Rechtsrahmen der datenschutzrechtlichen Einwilligung untersucht wird. Es soll in diesem Kapitel also nicht darum gehen, bereits konkrete Anforderungen an eine wirksame Einwilligung zu untersuchen oder zu formulieren, sondern stattdessen auf abstrakterer Ebene die maßgeblichen Komponenten einer Einwilligung herauszustellen.

A. Begriffsdefinition¹

Vom Wortlaut her beschreibt der Begriff *Einwilligung* zunächst lediglich ein bestimmtes menschliches Verhalten: Der Einwilligende hat einen zustimmenden, erlaubenden Willen gebildet und äußert diesen.² Die Willensbildung läuft für die Umwelt unbemerkt ab, sodass die anschließende Äußerung das einzig Messbare ist. Nur ein wahrnehmbares Verhalten kann Rechtsfolgen auslösen,³ daher kann hierfür nur dieser zweite Schritt, die Willensäußerung⁴, maßgeblich sein. Durch sie interagiert der Einwilligende mit der Außenwelt und diese kann

¹ Hinsichtlich der verwendeten Begriffe richtet sich diese Arbeit der Einheitlichkeit wegen nach den Begriffsdefinitionen des § 3 Abs. 1 BDSG.

² So auch A. Geiger, NVwZ 1989, 35 (36).

³ So jedenfalls nach der objektiven Theorie, bei der es gerade nicht auf die „unerkennbare subjektive ‚Bestimmung‘ des Verhaltens durch den Erklärenden“ ankommt, sondern stattdessen entscheidend ist, „ob der rechtsgeschäftliche Wille unmittelbar aus der auf einen rechtlichen Erfolg gerichteten Sprache (...) oder mittelbar aus anderen Indizien erschlossen werden muss“, Armbrüster, in: MüKo BGB, Vor § 116 Rn. 6.

⁴ Natürlich kann in normativer Hinsicht auch ein Nichtäußern rechtlich relevant sein, jedoch führt dies dann unmittelbar zu der Frage, ob ein gebildeter Wille nur nicht geäußert wird, oder überhaupt kein Wille gebildet wurde. Zur konkreten Ausgestaltung siehe unten, S. 18 ff.

Stichwortverzeichnis

- Abhängigkeit von einem Produkt und/oder einer (Dienst-)Leistung 14, 81, 212
Abhängigkeitsverhältnis 54, 127
Abmahnung 22
Abrechnungsstelle 152, 154, 229
Albrecht-Report 57
Algorithmus 27
Allgemeines Persönlichkeitsrecht 65, 122, 128, 171, 174
Apple 7, 29, 31, 140, 227
Apps 32, 35, 158, 182
Arbeitgeber/Arbeitnehmer 38, 54, 79, 98, 125, 162, 169, 206, 219, 223
Arbeitsplatz 22, 80, 125, 169, 212
Arbeitsverhältnis 129, 162
Arrival and Departure Information System (ADIS) 179
Artikel-29-Datenschutzgruppe 45, 48, 55
Ashley Madison 194, 225
ASNEF-Entscheidung 42, 110,
Automated Targeting System (ATS) 179
- Barack Obama 189, 210
Behavioural Advertising 31, 189
Bestandsdaten 30, 138, 145
Betriebsrat 23, 129, 224
Betriebsvereinbarung 23, 61, 130, 223,
Bewegungsprofil 31, 195
Bewerber 79, 125, 169, 171, 191, 212, 219
Bewerbung 37
Big Data 24, 222
BITKOM 24
- California Effect 183
Checkbox 19, 56, 106, 146
Cloud Computing 28, 114, 196, 228
Computergrundrecht 71, 174
Cookies 30, 48, 225
- Data Mining 25, 198, 222
Datenerhebung 7, 33, 73, 174
Datenhändler 27
Datenpool 25, 32, 157
- Datenschutzgrundrecht 39, 176
Datenschutzgrundverordnung 5, 51, 157, 168, 241
Datenschutzstandard 23, 63, 241
Datenvolumen 24
Delegationsverbot 61
Deutsche Telekom AG 49
Drittanbieter 32, 35
Drittländer 47, 227
- E-Health 158
Edward Snowden 7, 29
Endgerät 30, 48, 74, 139, 144
Energiewirtschaft 24
Erlaubnisvorbehalt 1, 35, 39, 78, 113, 133, 159, 171, 177, 193, 227
EU-Mitgliedsstaaten 6, 40, 51, 58, 110, 123, 197
EU-Parlament 51, 57, 59
EU-Sekundärrecht 40, 135, 195, 226, 239
Europäische Kommission 5, 50, 62, 226
Europäischer Datenschutzbeauftragter 56
- Facebook 23, 29, 34, 148, 200
Fapping, The 29
Federal Trade Commission (FTC) 188
Finanzwelt 24, 26, 181, 213
Formulareinwilligung 20, 221
Fragebogen 15, 82
Fremddaten 49
Frequent Locations 31, 227
Funkzelle 31, 139, 227
- Geburtsstermin 27
Gedanken-, Gewissens- und Religionsfreiheit 37
Generali 35
Geodaten 31, 144, 188
George Carlin 223
Gesellschaft 66, 210
Gesetzgebungskompetenz 64
Gesundheitsbereich 5, 24, 34, 148, 219
Gewinnspiel 15, 82, 88

- Globale Einwilligung 141
 Google 7, 29, 33, 144, 173
 GoYellow 49
 GPS-Chips 31, 129, 139, 144, 227
 Grundrechtsverzicht 70, 174

 Hardware 7, 29
 Harmonisierung 6, 40, 241

 iCloud 29
 informationelles Selbstbestimmungsrecht 23, 86, 98, 224
 Informationspflicht 16, 92
 Integrierte Versorgung 151, 229
 Internet 24, 28, 30, 33, 48, 56, 60, 72, 90, 106, 120, 136, 144, 177
 IP-Adresse 30
 iPhone 31, 142

 Kalifornien 183, 191
 Kassenärztliche Vereinigung 154
 Kommerzialisierung 21, 117, 122, 234
 Krankenhaus 5, 79, 154, 186, 195
 Krankenkasse 79
 Krankenversicherung 152, 180, 186
 Krankheit 34, 186
 Kreditech 26
 Kreditkarte 27, 183
 Kreditwürdigkeit 26
 Kriminalitätsprävention 27

 Lauterkeitsrecht 15, 85, 89, 91, 122
 Lebensversicherung 79

 Machtasymmetrie 14, 22, 79, 122, 125
 Marketing 26, 143, 166, 181, 186
 Martin Scorsese 179
 Mautsysteme 24
 MediaMarkt 87
 Medizinische Tests 34, 185
 Metadaten 24
 Mikrokreditgeber 26
 Mindeststandard 40, 132
 Minority Report 27
 Mobbing 22
 Mobiltelefon 31, 73
 Multioptionsgesellschaft 210

 Navigationsgerät 32
 Neue Medien 23, 135, 225

 Objektiver Maßstab 215
 Opt-in, Opt-out 19, 48, 106, 147, 213

 Outsourcing 152, 154, 231

 Patientendaten 35, 154
 Payback 82, 213
 Peter Gross 210
 Philip K. Dick 27
 Polizei 28, 175
 Precobs 28
 Predictive Policing 27
 PRISM-Programm 7, 29, 227
 Privacy Policy 187, 189
 Privatautonomie 47, 119, 207, 230, 240
 Privatpatient 152
 Profiling 27
 Protected Health Information (PHI) 180

 Rechnernetzwerk 72
 Recht auf informationelle Selbstbestimmung 65, 73, 76, 86, 96, 102, 127, 207, 232
 Reluctant consent 59, 162, 215

 SCHUFA 26, 213
 Schwangerschaft 27
 Smart-Meter-Anwendungen 24
 Smartphone 7, 16, 98, 188, 195
 SMS 114, 166, 199
 Social-Media/soziale Netzwerke 23, 26, 34, 146
 Sozialdaten 149, 154
 Sozialer Druck 15, 79, 87, 122
 Standortdaten 31, 137, 139, 143, 195, 227
 Steven Spielberg 27
 Straftäter 28
 Strafverfolgung 26, 145
 Strukturelle Ungleichheit 22, 79, 91, 122, 125

 Target 27
 Targeted Advertising 21, 26, 31, 186
 Tatort 28
 Tchibo 88
 Telekommunikationsanbieter 24, 138, 196
 Telemedien 109, 136, 141, 158
 Telemonitoring 158
 Telix AG 49
 Third-Party-Apps 32
 Tracking 226
 TTIP 241

 Übermäßige Anreize 14, 82, 86, 91, 101
 Ubiquitous Computing 33

- Ungleichgewicht 22, 52, 54, 58, 60, 62, 80,
125, 129, 162, 196
- Verbraucher 83, 86, 108, 146, 188, 190, 222
- Verkehrsdaten 138, 166
- Versicherungsrecht 79, 157
- Volkszählungsurteil 65, 69, 196
- Vollharmonisierung 40
- Vorstellungsgespräch 14
- Webhosting 28
- Website 30, 48, 136, 182, 187, 190
- Werbestrategie 27
- Werbung 21, 27, 87, 138, 142, 147, 166,
186, 189
- Wettbewerbsrecht 83, 89, 141, 213
- Willensäußerung 11
- Willensbildung 16, 79, 91
- Zeitliche Entzerrung 230, 233, 236
- Zwangslage 13, 83, 155, 208, 230
- Zweifelsfreiheit 44, 165

