

Internetrecht und Digitale Gesellschaft

Band 38

**Datenfinanzierte Apps
als Gegenstand des Datenschutzrechts**

Von

Kai-Niklas Knüppel



Duncker & Humblot · Berlin

KAI-NIKLAS KNÜPPEL

Datenfinanzierte Apps
als Gegenstand des Datenschutzrechts

Internetrecht und Digitale Gesellschaft

Herausgegeben von
Dirk Heckmann

Band 38

Datenfinanzierte Apps als Gegenstand des Datenschutzrechts

Von

Kai-Niklas Knüppel



Duncker & Humblot · Berlin

Die Rechtswissenschaftliche Fakultät der Universität Mannheim
hat diese Arbeit im Jahr 2021 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

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

Alle Rechte vorbehalten
© 2022 Duncker & Humblot GmbH, Berlin
Satz: TextFormA(r)t, Daniela Weiland, Göttingen
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-18665-5 (Print)
ISBN 978-3-428-58665-3 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

Internet: <http://www.duncker-humblot.de>

Vorwort

Die vorliegende Arbeit entstand weitestgehend während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Recht der Wirtschaftsregulierung und Medien an der Universität Mannheim und wurde im Mai 2021 bei der Juristischen Fakultät der Universität Mannheim als Dissertation eingereicht. Literatur und Rechtsprechung konnten im Anschluss bis zum Februar 2022 berücksichtigt werden.

Ich möchte mich herzlichst bei meinem Doktorvater, Herrn Prof. Dr. Ralf Müller-Terpitz, für die Betreuung meiner Arbeit sowie die angenehme Arbeitsatmosphäre an seinem Lehrstuhl bedanken. Sowohl bei der Themenfindung wie auch beim weiteren Verlauf der Erarbeitung begleitete er mich stets mit kritischen und hilfreichen Anmerkungen und Ratschlägen. Mein weiterer Dank gilt Herrn Prof. Dr. Thomas Fetzer für die schnelle Zweitbegutachtung dieser Arbeit und die hierbei aufgeworfenen konstruktiven Anmerkungen. Schließlich möchte ich Herrn Prof. Dr. Dirk Heckmann für die Aufnahme in die von ihm herausgegebene Schriftenreihe danken.

Für die Unterstützung während der Zeit der Promotion bin ich sowohl meinen Eltern wie auch zahlreichen Freunden sehr dankbar, ohne deren Unterstützung dieses Projekt sicherlich nicht derart zum Abschluss gekommen wäre. Herauszuheben ist hierbei Herr Dr. Hannes Beyerbach, der für Fragen und Ideen immer ein offenes Ohr hatte und so in großem Maße zum Gelingen dieser Arbeit beigetragen hat.

Berlin, April 2022

Kai-Niklas Knüppel

Inhaltsverzeichnis

Teil I

Datenfinanzierte Angebote als Untersuchungsgegenstand	19
§ 1 Einleitung	19
A. Stand der Forschung	21
B. Zielsetzung dieser Arbeit	22
C. Gang der Untersuchung	23
§ 2 Die Relevanz datenfinanzierter Angebote	25
A. Big Data als Grundlage für datenfinanzierte Angebote	26
I. Was bedeutet „Big Data“?	27
1. Technische Betrachtung	28
2. Ökonomische Betrachtung	29
3. Ansätze einer sozialwissenschaftlichen Betrachtung	30
II. Big Data im rechtswissenschaftlichen Kontext	30
1. Ansätze zur Klassifizierung in der Literatur	31
2. Rechtliche Einordnung von Big Data	32
B. Datenfinanzierte Angebote	33
I. Die Begrifflichkeit „datenfinanzierte Angebote“	33
1. Mobile Apps	33
a) Erwerb und Vertrieb von Apps	34
b) Kostenfreiheit	35
c) Datenerhebung	36
2. Weitere datenfinanzierte Angebote	37
a) Freeware	37
b) Web-Apps	37
3. Zwischenergebnis	38
II. Datenfinanzierung als relevantes Unterscheidungskriterium	39
1. Die Werthaftigkeit von Daten	39
a) Die abstrakte Werthaftigkeit	40
aa) Der Warencharakter personenbezogener Daten	41
bb) Die Nutzung personenbezogener Daten	42
cc) Zwischenergebnis	45

b) Die Wertschöpfung bei datenfinanzierten Angeboten	45
aa) Die Nutzung der Daten	46
bb) Die Konsequenz für datenfinanzierte Angebote	47
cc) Die Preisgabe der Daten	48
dd) Die Problematik der Kostenfreiheit	49
ee) Die Relevanz einer Abgrenzung datenfinanzierter Angebote	51
2. Legislative Berücksichtigung durch die Richtlinie (EU) 2019/770	53
a) Die Bereitstellung digitaler Inhalte	54
b) Die nationale Umsetzung der Richtlinie	55
c) Die Erhebung von Daten als Gegenleistung	55
d) Folgen für den Begriff der datenfinanzierten Angebote	56
3. Absolute und relative Rechte an Daten	57
a) Die Debatte um das sog. Dateneigentum	57
b) Die Auswirkungen auf datenfinanzierte Angebote	58
4. Zwischenergebnis	59
III. Die Kategorisierung datenfinanzierte Angebote	60
1. Der Inhalt der Angebote	60
2. Die Zurverfügungstellung der Angebote	61
3. Die Art der Datenerhebung	61
4. Die Art der Datenverarbeitung	62
a) <i>Kategorie I</i> : Sofortnutzung der Daten	62
b) <i>Kategorie II</i> : Speicherung und Nutzung der Daten	63
c) <i>Kategorie III</i> : Offenlegung der Daten	64
aa) Kategorie III a): Offenlegung innerhalb eines Konzerns	65
bb) Kategorie III b): Offenlegung an externe Dritte	66
d) Die Unterscheidung dieser Kategorien	67
5. Zwischenergebnis	67

Teil 2

Die Bewertung datenfinanzierter Angebote de lege lata	68
§ 3 Rechtliche Besonderheiten datenfinanzierter Angebote	68
A. Die Zivilrechtliche Einordnung	68
I. Die Vertragsart	69
1. Die Einordnung kostenpflichtiger (Web-)Apps	70
2. Die Einordnung entgeltfreier Angebote	70
3. Bewertung	71
II. Die Vertragsparteien	74

1. Das Merkmal der Offenkundigkeit	75
2. Vertretungsmacht und Zwischenergebnis	77
III. Einbeziehung von Allgemeinen Geschäftsbedingungen	77
B. Datenfinanzierte Angebote als Telemedien	78
I. Der sachliche Anwendungsbereich	78
II. Auswirkungen für datenfinanzierte Angebote	79
C. Die Eingrenzung des rechtlichen Untersuchungsrahmens	80
§ 4 Die Grundlagen des Datenschutzrechts	82
A. Die verfassungs- und primärrechtliche Ausgestaltung des Datenschutzes	83
I. Nationales Verfassungsrecht	83
1. Der Schutzzumfang der informationellen Selbstbestimmung	84
a) Die Eingriffsintensität	85
b) Der Ausschluss durch Einwilligung	86
c) Die Rechtfertigung von Eingriffen	86
d) Prozedurale Garantien	88
2. Mittelbare Drittwirkung und Schutzpflichten	88
a) Übertragbarkeit auf die informationelle Selbstbestimmung	90
b) Der Umfang von Schutzpflichten und der Drittwirkung	91
3. Würdigung	93
II. Primärrechtsschutz in der EU	94
1. Historische Entwicklung	95
a) Die Situation mit Inkrafttreten des Vertrags von Lissabon	95
b) Bedeutung der EMRK für den Datenschutz	97
2. Art. 8 der Grundrechte-Charta	98
a) Der Schutzbereich	100
b) Eingriffe in Art. 8 GRCh	101
c) Die Rechtfertigung oder der Ausschluss des Eingriffs	102
d) Betroffenenrechte und institutionelle Vorgaben	104
e) Drittwirkung und staatliche Schutzpflichten	105
f) Würdigung	107
3. Datenschutz nach dem AEUV	107
III. Grundrechtspositionen der Datenverarbeiter	109
1. Nationales Verfassungsrecht	109
a) Art. 12 Abs. 1 GG	110
b) Die Meinungs- und Informationsfreiheit aus Art. 5 GG	112
c) Sonstige Grundrechte der Datenverarbeiter	114
2. Europäischer Primärrechtsschutz	115

a) Europäischer Schutz der unternehmerischen Freiheit	115
aa) Art. 16 GRCh	116
bb) Schutz über Grundfreiheiten	116
b) Art. 11 GRCh	117
3. Würdigung	118
B. Die sekundärrechtliche und einfachgesetzliche Ausgestaltung des Datenschutzes	118
I. Die Datenschutz-Grundverordnung	120
1. Der Anwendungsbereich	121
a) Sachlich	121
b) Räumlich	123
2. Sonstige Grundzüge der DSGVO	123
II. Das Bundesdatenschutzgesetz	124
III. Datenschutz aus anderen Quellen	125
1. Datenschutz nach dem TTDSG	126
2. Anstehende regulatorische Veränderungen	127
C. Das Rangverhältnis der Gewährleistungen und dessen Auswirkungen	127
I. Das Verhältnis der grundrechtlichen Gewährleistungen	128
1. Die Konfliktsituation vor den Entscheidungen zum Recht auf Vergessen	129
2. Die Beschlüsse Recht auf Vergessen I und II	131
3. Das grundrechtliche Konfliktpotential im Datenschutz	132
4. Zwischenergebnis	134
II. Die Umsetzung des Datenschutzes in der DSGVO	135
III. Konfliktebereiche datenfinanzierter Angebote	137
§ 5 Grundsätze und Prinzipien des Datenschutzes	138
A. Der Anwendungsbereich der DSGVO	139
I. Die Datenverarbeitung	140
II. Der Personenbezug von Daten	141
1. Identifizierbarkeit	142
a) Methoden der Identifizierung	143
b) Voraussetzungen der Identifizierbarkeit	143
aa) Die Vorgaben der DSGVO	144
bb) Die Rechtsprechung des EuGH	145
cc) Zeitpunkt der Datenverarbeitung	146
dd) Zwischenergebnis	146
c) Die Identifizierbarkeit im digitalen Kontext	147
2. Anonymisierung und Pseudonymisierung	148
a) Anonymisierung	148

aa) Anonyme Daten	149
bb) Technische Ausgestaltung	149
b) Pseudonymisierung	151
aa) Der Personenbezug pseudonymierter Daten	153
bb) Die rechtliche Wirkung der Pseudonymisierung	154
3. Besonderheiten bei datenfinanzierten Angeboten	155
a) Vorüberlegung: Personenbezug bei Big Data	155
aa) Makro-Ebene – Probleme der Anonymisierung	156
bb) Mikro-Ebene	157
cc) Zwischenergebnis	158
b) Der Personenbezug bei datenfinanzierten Angeboten	158
aa) Personenbezug in verschiedenen Konstellationen	159
bb) Anonymisierung und Pseudonymisierung	160
(1) Sofortnutzung der Daten	160
(2) Speicherung der Daten	161
(3) Offenlegung der Daten	161
cc) Zwischenergebnis	163
III. Die datenschutzrechtliche Verantwortlichkeit	163
1. Der Verantwortliche nach Art. 4 Nr. 7 DSGVO	164
2. Verantwortlichkeit im Mehrpersonenverhältnis	165
a) Alleinige Verantwortlichkeit, Art. 4 Nr. 7 DSGVO	166
b) Gemeinsame Verantwortlichkeit, Art. 4 Nr. 7, Art. 26 DSGVO	167
c) Auftragsverarbeitung, Art. 4 Nr. 8, Art. 28 DSGVO	169
aa) Auftragsverarbeitung bei datenfinanzierten Angeboten	169
bb) Bedeutung der Auftragsverarbeitung für die folgende Untersuchung	170
d) Sonderfall: Verantwortlichkeit bei konzerninterner Datenverarbeitung	171
B. Datenschutzrechtliche Grundsätze	173
I. Rechtmäßigkeit und Transparenz	174
1. Der Grundsatz der Rechtmäßigkeit	174
2. Der Grundsatz der Transparenz	175
a) Inhaltliche Ausgestaltung	176
b) Konflikt mit Big Data	177
3. Treu und Glauben	178
4. Die Folgen für datenfinanzierte Angebote	179
II. Der Grundsatz der Zweckbindung	181
1. Die Zweckbindung nach Art. 5 Abs. 1 lit. b) DSGVO	182
a) Voraussetzungen an eine zweckgebundene Datenverarbeitung	182

aa) Festlegung des Zwecks	182
bb) Eindeutigkeit des Zwecks	183
cc) Legitimität des Zwecks	184
b) Die Zweckbindung bei der Weiterverarbeitung	184
c) Die Bedeutung für datenfinanzierte Angebote	186
2. Zweckänderungen	187
a) Art. 89 Abs. 1 DSGVO	188
b) Art. 6 Abs. 4 DSGVO	190
aa) Die Voraussetzungen von Art. 6 Abs. 4 DSGVO	191
bb) Auswirkungen auf den Grundsatz der Zweckbindung	192
3. Die Zweckbindung bei datenfinanzierten Angeboten	195
a) Die Grundproblematik bei Big Data	195
aa) Widerspruch zur Zweckbindung	195
bb) Ausnahmen von der Zweckbindung	196
cc) Bewertung	198
b) Die Übertragbarkeit auf datenfinanzierte Angebote	199
aa) Die Sofortnutzung der Daten	200
bb) Die Speicherung und Nutzung der Daten	200
cc) Die Offenlegung der Daten	201
dd) Fazit	202
III. Der Grundsatz der Datenminimierung	203
1. Der Inhalt der Datenminimierung	203
2. Die Umsetzung der Datenminimierung	205
a) Datenschutz durch Technikgestaltung	206
b) Datenschutzzfreundliche Voreinstellungen	207
c) Konkretisierungsansätze in § 19 Abs. 2 TTDSG	208
3. Die Datenminimierung bei datenfinanzierten Angeboten	208
a) Vorüberlegungen zu Big Data	209
b) Die Übertragbarkeit auf datenfinanzierte Angebote	210
IV. Weitere Datenschutzgrundsätze	212
1. Der Grundsatz der Richtigkeit	213
2. Der Grundsatz der Speicherbegrenzung	214
3. Der Grundsatz der Integrität und Vertraulichkeit	215
C. Folgen für die Verarbeitung innerhalb datenfinanzierter Angebote	215
I. Vorüberlegung: Big Data	215
II. Datenfinanzierte Angebote	217
1. Die Problematik der einzelnen Grundsätze	217
2. Ansätze zur Vereinbarkeit mit den Grundsätzen	218

§ 6 Die Rechtmäßigkeit der Datenverarbeitung	219
A. Gesetzliche Erlaubnistatbestände	221
I. Die Verarbeitung zur Erfüllung eines Vertrags	222
1. Zur Erfüllung eines Vertrags	223
2. Die Erforderlichkeit der Datenverarbeitung	224
a) Die Erforderlichkeit bei privatrechtlichen Verträgen	224
b) Die Reichweite der Erforderlichkeit	225
c) Transparenz der erforderlichen Verarbeitung	227
3. Die Bedeutung für datenfinanzierte Angebote	227
a) Die Erforderlichkeit aufgrund der Datenverarbeitung als Gegenleistung	227
b) Die Erforderlichkeit sonstiger Datenverarbeitung	229
II. Die Verarbeitung zur Verwirklichung berechtigter Interessen	230
1. Interessenabwägung	231
a) Das berechnete Interesse	232
b) Die Erforderlichkeit der Verarbeitung	233
c) Abwägung mit den Interessen der betroffenen Person	233
d) Transparenz und Widerspruchsrecht	236
2. Die Bedeutung für datenfinanzierter Angebote	237
a) Die Verarbeitung von Daten als Gegenleistung	237
b) Die direkte Verarbeitung und Speicherung der Daten	238
c) Die Offenlegung der Daten	239
III. Fazit	240
B. Die Einwilligung als Legitimationstatbestand	241
I. Die Grundproblematik des Einwilligungskonzepts	242
II. Die Voraussetzungen der Einwilligung	243
1. Die Erteilung der Einwilligung durch Willensbekundung	244
a) Durch Erklärung oder sonstige bestätigende Handlung	245
b) Die Nachweispflicht bei einer Erklärung	246
c) Sonstige eindeutige bestätigende Handlung	247
aa) Die Tauglichkeit von Opt-Out-Lösungen	247
bb) Die Nachweispflicht bei bestätigenden Handlungen	248
d) Die Einwilligungserteilung bei datenfinanzierten Angeboten	249
2. Die Bestimmtheit der Einwilligung	250
a) Inhalt und Hintergrund der Bestimmtheit	250
b) Die Reichweite der Bestimmtheit	251
aa) Zugrundeliegende Problematik	251
bb) Folgen dieses Verständnisses	253

c)	Die Ausgestaltung bei datenfinanzierten Angeboten	254
3.	Die Informiertheit und Transparenz der Einwilligung	255
a)	Die Möglichkeit zur Kenntnisnahme	256
b)	Transparenzanforderungen	257
c)	Informiertheit und Transparenz bei datenfinanzierten Angeboten	258
4.	Die Freiwilligkeit der Einwilligung	260
a)	Kartellähnliche Angebotslagen	262
b)	Die Kopplung der Einwilligung	263
aa)	Das horizontale Kopplungsverbot	264
bb)	Das vertikale Kopplungsverbot	265
(1)	Die Ablehnung eines absoluten Kopplungsverbots	266
(2)	Die Reichweite des vertikalen Kopplungsverbots	267
(3)	Das verhältnismäßige Maß des Kopplungsverbots	270
cc)	Das Kopplungsverbot im Austauschverhältnis Daten gegen Leistung	271
dd)	Maßstäbe zum Umfang der Datenpreisgabe	273
ee)	Die Notwendigkeit von Alternativen zur gekoppelten Einwilligung	275
c)	Die Freiwilligkeit bei datenfinanzierten Angeboten	275
5.	Die Widerrufbarkeit der Einwilligung	277
a)	Inhalt und Ausübung der Widerrufsmöglichkeit	277
b)	Die Rechtsfolge des Widerrufs	278
aa)	Ausgangsüberlegung: Kumulation von Rechtsgrundlagen	279
bb)	Kumulation und Wegfall von Rechtsgrundlagen	279
cc)	Die Konsequenz kumulativer Rechtsgrundlagen	281
c)	Die Widerrufbarkeit bei datenfinanzierten Angeboten	282
aa)	Das Für und Wider jederzeitiger Widerrufbarkeit	282
bb)	Würdigung	283
cc)	Folgen für datenfinanzierte Angebote	285
III.	Die Einwilligung im Kontext von Datenschutzerklärungen	286
1.	Ausgangspunkt: Art. 7 Abs. 2 DSGVO	287
a)	Der Regelungsrahmen von Art. 7 Abs. 2 DSGVO	288
b)	Anforderungen an die Erklärung	288
2.	Datenschutzerklärungen als Allgemeine Geschäftsbedingungen	290
a)	Die Rechtslage durch Inkrafttreten der DSGVO	291
b)	Folgen für die Einwilligungserklärung	292
3.	Auswirkungen auf datenfinanzierte Angebote	292
a)	Der Umfang der Inhaltskontrolle	293
b)	Die Missbrauchskontrolle der Einwilligung	294

IV. Die Einwilligung bei datenfinanzierten Angeboten	295
§ 7 Grenzüberschreitender Datenschutz	296
A. Räumlicher Anwendungsbereich der DSGVO	297
I. Das Sitz- und Niederlassungsprinzip	297
II. Das Marktortprinzip	299
1. Der Hintergrund des Marktortprinzips	300
2. Das Angebot von Daten oder Dienstleistungen	301
3. Die Beobachtung des Verhaltens betroffener Personen	303
4. Vermeintliche Schutzlücken zwischen Art. 3 Abs. 1 und 2 DSGVO	304
III. Folgen für Anbieter datenfinanzierter Angebote	305
B. Die Datenübermittlung in Drittländer	306
I. Die Datenübermittlung nach Art. 44 ff. DSGVO	307
1. Angemessenheitsbeschlüsse	308
a) Anforderungen an den Angemessenheitsbeschluss	309
b) Erlass und Wirkung des Beschlusses	310
c) Die aktuelle Umsetzung	311
2. Geeignete Garantien	311
a) Verbindliche interne Datenschutzvorschriften	313
aa) Voraussetzungen an die BCR	313
bb) BCR im Kontext datenfinanzierter Angebote	314
b) Standarddatenschutzklauseln	314
3. Ausnahmeregelungen	316
a) Einwilligungen	317
b) Übermittlung für die Erfüllung eines Vertrags	318
4. Zusammenfassung	319
II. Die Situation nach dem Schrems II-Urteil	319
1. Der Hintergrund des Verfahrens	319
2. Der Inhalt des Urteils	320
a) Die Unwirksamkeit des Privacy Shield-Beschlusses	321
b) Einschränkungen bei Standarddatenschutzklauseln	321
c) Übertragbarkeit auf verbindliche interne Datenschutzvorschriften	323
d) Weiterhin zulässige Ausnahmeregelungen	323
III. Folgen für datenfinanzierte Angebote	324
1. Die Erhebung, Verarbeitung und Speicherung	325
2. Die Offenlegung innerhalb des Konzerns	326
3. Die Offenlegung an Dritte	327

Teil 3

	Die Behandlung datenfinanzierter Angebote de lege ferenda	328
§ 8	Regulatorische Veränderungsmöglichkeiten	328
A.	Die Problematik datenfinanzierter Angebote	329
I.	Das „richtige Maß“ an Datenschutz	329
1.	Gründe für das Privacy Paradox	330
2.	Regulatorische Folgen	331
II.	Die Tiefe des Regulierungsniveaus	332
1.	Gründe für ein geringeres Regulierungsniveau	333
a)	Der Paternalismus im Datenschutz	333
aa)	Die Kritik an der aktuellen Gesetzeslage	334
bb)	Probleme durch paternalistische Regulierung	335
cc)	Die Tauglichkeit bei der Regulierung datenfinanzierter Angebote	336
b)	Weitere Gründe für ein geringeres Datenschutzniveau	337
c)	Die Regulierung über alternative Wege	339
aa)	Wettbewerbsrechtliche Regulierung	339
bb)	Die Tauglichkeit zur Regulierung datenfinanzierter Angebote	341
2.	Gründe für ein höheres Regulierungsniveau	342
a)	Die Veränderung des regulatorischen Rahmens	342
b)	Die Besonderheit datenfinanzierter Angebote	343
III.	Der Abgleich mit den Regelungen der DSGVO	344
1.	Das Verbot unter Erlaubnisvorbehalt und die Erlaubnistatbestände	345
2.	Erkennbare Schwachpunkte	346
B.	Alternative Modelle zur Monetarisierung	347
I.	Die Umsetzung der alternativen Modelle	348
1.	Die praktische und technische Umsetzung	349
2.	Die regulatorische Umsetzung	350
II.	Vorteile von Monetarisierungsmodellen	352
1.	Die erleichterte Durchsetzung eines sinnhaften Kopplungsverbots	352
2.	Die Entschärfung der jederzeitigen Widerrufbarkeit	353
III.	Offene Fragen und Nachteile solcher Modelle	354
1.	Einschränkungen der unternehmerischen Freiheit	354
2.	Die Höhe des Entgelts	356
a)	Der Wert der verarbeiteten Daten	356
b)	Konsequenzen für die Höhe des Entgelts	357
c)	Die Tauglichkeit der Umsetzung	358
IV.	Würdigung	359

C. Verbesserte Ansätze zur Transparenz	360
I. Aktuelle Transparenzregeln	361
1. Der Grundsatz der Transparenz	362
a) Informationspflichten aus Art. 13, 14 DSGVO	362
b) Transparenzpflichten aus Art. 12 Abs. 1 DSGVO	364
2. Die Transparenz bei einzelnen Erlaubnistatbeständen	365
3. Die Transparenz bei datenfinanzierten Angeboten	366
II. Die Verbesserung der Transparenzmöglichkeiten	368
1. Verarbeitungsübersichten („One-Pager“)	368
a) Der Inhalt der One-Pager	370
b) Bewertung	370
2. Die Visualisierung der Verarbeitung	372
a) Der rechtliche Ansatzpunkt	372
b) Die Bewertung der Visualisierung	374
c) Die Umsetzbarkeit	375
aa) Vergleichbare Ansätze in anderen Rechtsgebieten	376
bb) Geeignete Symbole	376
cc) Einzelne Vorschläge zu Bildsymbolen	377
(1) Entwurfsfassung des Parlaments	377
(2) Ansätze von Mehdau und das Projekt PrimeLife	379
(3) Ansatz von Specht-Riemenschneider und Bienemann	381
dd) Umsetzungschancen und -risiken	382
III. Die Stärkung der Transparenz bei datenfinanzierten Angeboten	384
D. Fazit	385
Zusammenfassung der Arbeit in Thesen	387
Literaturverzeichnis	399
Stichwortverzeichnis	416

Teil 1

Datenfinanzierte Angebote als Untersuchungsgegenstand

§ 1 Einleitung

Schon im Jahr 1983 entwickelte das Bundesverfassungsgericht im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung. Diese hat zur Prämisse, dass eine Person in ihrer Selbstbestimmung wesentlich gehemmt wird, wenn sie nicht mit hinreichender Sicherheit überschauen kann, wer was, wann und in welchem Zusammenhang über sie weiß.¹ Dieses Risiko ist angesichts der zunehmenden Digitalisierung und den zunehmenden Analyse-Möglichkeiten von Daten über „Big Data“ aktueller denn je und die gesellschaftliche und ökonomische Bedeutung von Daten wächst rasant.

Inzwischen betrifft die Gefahr – anders als damals vom Bundesverfassungsgericht angedacht – nicht nur das Verhältnis des Staates zum Bürger, sondern immer häufiger jenes zwischen privaten Unternehmen und Bürgern. Im Rahmen von Big Data werden immer größere Datenmengen angesammelt, mit denen sich nach ihrer Auswertung zum Teil präzise Informationen über einzelne Personen herausarbeiten lassen. Im Unterschied zu „analogen“ Geschäftsfeldern werden Daten nicht mehr nur als Nebenprodukt zu Dienstleistungen gesammelt, sondern gezielt erhoben, gespeichert, kumuliert und ggf. weitergegeben. Dem liegt zugrunde, dass aus der Sammlung, Aggregation und Verarbeitung der Daten aus verschiedensten Quellen eine Wertschöpfung für den Datenverarbeiter ermöglicht wird.²

Hierdurch entstehen ganze datengetriebene Geschäftszweige, bei denen Nutzerdaten eine monetäre Vergütung des Kunden ersetzen. Vor allem internetbasierte Programme und mobile Applikationen (Apps) verwenden häufig solche „datenfinanzierten“ Geschäftsmodelle, bei denen Daten das Zahlungsmittel für die Bereitstellung und Nutzung der App darstellen. Die Anzahl und Bedeutung der *datenfinanzierten Angebote*, was den in dieser Arbeit hierfür verwendeten Terminus darstellt, nimmt immer weiter zu. Deren gesellschaftliche Relevanz lässt sich schon über die Vielzahl von vermeintlich kostenlosen Angeboten in den App-Stores der beiden größten Anbieter Google und Apple verdeutlichen. Diese reichen von Messenger- und Social Media-Angeboten über Gesundheits-, Navigations-, Fitness- und

¹ BVerfGE 65, 1 (42f.) – *Volkszählung*.

² *Lammerant/De Hert*, Visions of Technology, in: Gutwirth et al, Data Protection on the Move, S. 163 (164).

Gaming-Apps bis hin zu Smart Home Anwendungen oder (Browser-)Sicherheitssoftware. Die einfach verfügbare Bereitstellung und Vielseitigkeit datenfinanzierter Angebote schafft dem Nutzer die Möglichkeit, über die Apps vielschichtige Vorteile aus der Digitalisierung zu ziehen und eine Vielzahl von Nutzerinteressen in verschiedensten Lebensbereichen zu befriedigen.

Ohne diese Vorteile marginalisieren zu wollen, liegt in der Nutzung dieser Geschäftsmodelle gleichzeitig eine Gefahr für die Selbstbestimmung der einzelnen Nutzer. Die umfangreiche Datenerhebung erlaubt technisch eine immer größere Sammlung personenbezogener Daten. Je mehr Daten erhoben werden, desto schwieriger ist es für betroffene Personen über den Inhalt ihrer preisgegebenen Daten gewahr zu sein, da jedem einzelnen Datum durch die kumulierte und unter Umständen viel spätere Verbindung mit anderen eine neue, erweiterte Aussagekraft zukommen kann.³ Deshalb rückt die Bewertung von datenfinanzierten Geschäftsmodellen immer mehr in den Fokus der Rechtswissenschaft.

In Bezug auf datenfinanzierte Angebote stellt sich diese Frage im Besonderen, da diese ganz selbstverständlich im Alltag genutzt werden. Dabei erheben und übermitteln die Apps eine Vielzahl von Daten – zum Teil ohne offensichtliche Mitteilung an den Nutzer – und die Datenverarbeitung dient vielfach kommerziellen Zwecken. Seit langem wird bemängelt, dass viele Apps persönliche Nutzerinformationen ungesichert und teilweise unbemerkt für eigene Zwecke an Dritte übertragen haben.⁴ Diese zunehmende Datenpreisgabe führt auch zu einer weitverbreiteten Sorge um die eigene Privatheit.⁵ Auch mit Verabschiedung und Inkrafttreten der Datenschutz-Grundverordnung⁶ bleibt diese Problematik um die Nutzung personenbezogener Daten präsent, da die Geschäftsmodelle und die datenschutzrechtliche Compliance vieler App-Anbieter weiterhin Fragen aufwerfen.⁷

³ *Boehme-Neßler*, Das Ende der Anonymität, DuD 2016, 419 (420 f.). Diese Datenverwendung wird von den Nutzern auch durchaus kritisch gesehen, vgl. *Engels*, Datenschutzpräferenz von Jugendlichen in Deutschland, S. 12 ff.

⁴ Vgl. etwa bereits im Jahr 2012 *Pauly*, Welche Apps ihre Daten ausspähen, Stiftung Warentest v. 31. 5. 2012, abrufbar unter: www.test.de/Datenschutz-bei-Apps-Welche-Apps-Ihre-Daten-ausspaehen-4378643-0/.

⁵ 82 % der Deutschen haben laut einer repräsentativen Studie durchaus Bedenken um ihre Privatheit; gleichzeitig unternehmen allerdings nur wenige Maßnahmen, um ihre Privatheit zu verteidigen, vgl. *Kozyreva et al.*, Künstliche Intelligenz in Online-Umgebungen, S. 12.

⁶ Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden: „DSGVO“).

⁷ *Baumgartner*, in: *Baumgartner/Ewald*, Apps und Recht, Rn. 185. Anschaulich zur möglicher Datennutzung *Peitz*, Unsere Daten müssen wir selbst schützen, Zeit online vom 23. 5. 2018, abrufbar unter: www.zeit.de/digital/datenschutz/2018-05/dsgvo-datenschutz-nutzer-internet-facebook. Vgl. als aktuellen Fall etwa *Kan*, The Cost of Avast's Free Antivirus: Companies Can Spy on Your Clicks, PC Mag v. 27. 1. 2020, abrufbar unter: www.pcmag.com/news/the-cost-of-avasts-free-antivirus-companies-can-spy-on-your-clicks.

A. Stand der Forschung

Die Bedeutung von Daten nimmt wirtschaftlich und gesellschaftlich einen immer höheren Stellenwert ein. Diese Entwicklung lässt sich auch in der Rechtswissenschaft wiederfinden. Die vergleichsweise junge DSGVO wird dabei in zahlreichen wissenschaftlichen Auseinandersetzungen aus den unterschiedlichsten Blickwinkeln betrachtet. Gerade die Auswirkungen der Digitalisierung auf das Datenschutzrecht werden vielfach erörtert.⁸ Das Geschäftsmodell von Daten als Gegenleistung wird in der rechtswissenschaftlichen Literatur ebenfalls zunehmend zum Thema. Gerade datenfinanzierte Apps werden in der datenschutzrechtlichen Literatur immer umfangreicher analysiert. So wurde etwa die Begrifflichkeit des „datenfinanzierten Angebots“ bereits von Kugelman verwendet.⁹ Dabei werden als Synonyme für Datenfinanzierung häufig auch „kostenlose Apps“, das Austauschverhältnis „Daten gegen Leistung“, die „Datenpreisgabe gegen Nutzung eines Software Dienstes“ oder „datengetriebene Geschäftsmodelle“ verwendet. Eine Beschäftigung mit der Thematik findet auch auf abstrakter Ebene in Gestalt der Fragestellung statt, ob dem aktuelle Datenschutzregime für das Sonderverhältnis datenfinanzierter Dienste wirksame Regulierungsmöglichkeiten innewohnen.

Allen rechtswissenschaftlichen Publikationen ist dabei gemein, dass sie Teilbereiche der nachfolgenden Arbeit sehr genau untersuchen. Mit der Fokussierung auf mobile Applikationen finden sich in der rechtswissenschaftlichen Literatur etwa hauptsächlich Handbücher, die solche Apps aus verschiedensten Gesichtspunkten rechtlich bewerten.¹⁰ Zu den Folgen der Digitalisierung für die informationelle Selbstbestimmung sind ebenfalls einige Monografien erschienen, die die Privatheit zunehmender Digitalisierung behandeln.¹¹ Auch existieren eine Vielzahl von Schriften zu den einzelnen abstrakten Teilbereichen des Datenschutzes, insbesondere zu Fragen der Freiwilligkeit der Einwilligung.¹²

Zur Wirkung des Datenschutzrechts auf das Privatrechtsverhältnis bildet die Habilitationsschrift Buchners¹³ die maßgebliche Grundlage, die konzeptionell die Entwicklung eines privatrechtlichen Datenschutzes auf Grundlage der Entscheidung der Beteiligten anhand eines privatautonomen Interessenausgleichs anstrebt.

⁸ Vgl. etwa *Specht-Riemenschneider/Werry/Werry* (Hrsg.), *Datenrecht in der Digitalisierung*; *Körper/Immenga* (Hrsg.), *Daten und Wettbewerb in der digitalen Ökonomie*.

⁹ *Kugelman*, DuD 2016, 566.

¹⁰ Etwa *Baumgartner/Ewald* (Hrsg.), *Apps und Recht*; *Solmecke/Taeger/Feldmann* (Hrsg.), *Mobile Apps. Rechtsfragen und rechtliche Rahmenbedingungen*.

¹¹ Vgl. etwa *Hermstrüwer*, *Informationelle Selbstgefährdung*; *Sandfuchs*, *Privatheit wider Willen?*.

¹² Vgl. etwa *Bunnenberg*, *Privates Datenschutzrecht. Vor allem zum Konzept der Einwilligung* finden sich zahlreiche weitere Monografien, u. a. *Radlanski*, *Das Konzept der Einwilligung in der datenschutzrechtlichen Realität*; *Rogosch*, *Die Einwilligung im Datenschutzrecht*.

¹³ *Buchner*, *Informationelle Selbstbestimmung im Privatrecht*.