ANDREAS SATTLER

Informationelle Privatautonomie

Jus Privatum
264

Mohr Siebeck

JUS PRIVATUM

Beiträge zum Privatrecht

Band 264

Andreas Sattler

Informationelle Privatautonomie

Synchronisierung von Datenschutz- und Vertragsrecht

Mohr Siebeck

Andreas Sattler, geboren 1982; Studium der Rechts- und Wirtschaftswissenschaften in Bayreuth und Nottingham (LL.M.); Promotionsstipendium der DFG und Mitgliedschaft im DFG-Graduiertenkolleg „Geistiges Eigentum und Gemeinfreiheit", Universität Bayreuth; Dissertation (Emanzipation und Expansion des Markenrechts, Mohr Siebeck, 2015); Rechtsanwalt im Bereich IT-Recht bei CMS Hasche Sigle, Stuttgart; Akademischer Rat a.Z. am Lehrstuhl für Bürgerliches Recht, Recht des Geistigen Eigentums und Wettbewerbsrecht an der Ludwig-Maximilians-Universität München; Habilitation; Lehrbefähigung für die Fächer Bürgerliches Recht, Immaterialgüterrecht, deutsches und europäisches Wirtschaftsrecht und Datenrecht; Gründung und Co-Leitung des Center for Intellectual Property Law, Information and Technology (CIPLITEC); seit April 2022: Vertretung des Lehrstuhls für Zivil- und Wirtschaftsrecht, Medien- und Informationsrecht an der Albert-Ludwigs-Universität Freiburg.

Gedruckt und als Open Access Dokument zugänglich gemacht mit der freundlichen Unterstützung des *LMU Open Access Fonds*, des *LMU Post Doc Fonds*, der *Johanna und Fritz Buch Gedächtnisstiftung e.V.* und der Studienstiftung *ius vivum e.V.*

ISBN 978-3-16-161905-2 / eISBN 978-3-16-161906-9
DOI 10.1628/978-3-16-161906-9

ISSN 0940-9610 / eISSN 2568-8472 (Jus Privatum)

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

© 2022 Mohr Siebeck Tübingen. www.mohrsiebeck.com

Dieses Werk ist lizenziert unter der Lizenz „Creative Commons Namensnennung – Keine Bearbeitungen 4.0 International" (CC BY-ND 4.0). Eine vollständige Version des Lizenztextes findet sich unter: https://creativecommons.org/licenses/by-nd/4.0/deed.de

Das Buch wurde von Gulde Druck aus der Garamond gesetzt, in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

Vorwort

Daten werden seit einigen Jahren als „neues Gold“ oder „Öl des 21. Jahrhunderts“ bezeichnet. Diese Vergleiche hinken. Im Gegensatz zu Gold und Öl sind Daten immaterielle Güter. Infolgedessen ist ihre Nutzung weder ausschließlich noch rival. Ohne rechtliche Zuweisung beruht die Möglichkeit zur Datennutzung lediglich auf einem faktischen Zugang, allgemein zugängliche Daten kann jedermann nutzen (keine Ausschließbarkeit). Die Nutzung durch eine Person hindert nicht die zeitgleiche Nutzung dieser Daten durch weitere Personen (keine Rivalität). Kurzum: Aufgrund ihrer immateriellen Eigenschaften können Daten eine sehr vielseitig nutzbare Ressource sein.

Dies erklärt, warum Daten zunehmend in den Fokus der Gesetzgeber im europäischen Mehrebenensystem geraten und warum die Gesetzgeber nach Wegen suchen, um die Nutzung von Daten zu fördern; stets in der Erwartung, dass dadurch die wirtschaftliche Effizienz, die technische Innovation und damit letztlich der volkwirtschaftliche Wohlstand gesteigert werden. Die Vorschläge für Ansprüche auf Datenzugang und Datenüberlassung (Data Act), aber auch das Konzept einer Datentreuhand (Data Governance Act) sind aktuelle Beispiele dafür, dass der unionale Gesetzgeber nach Mechanismen sucht, um den „Datenschatz“ zu heben. Dabei bezieht der Gesetzgeber zunehmend auch personenbezogene Daten ein. Er folgt damit der wirtschaftlichen Realität. Zahlreiche Dienstleistungen der Betreiber von mehrseitigen Plattformen, insbesondere von Suchmaschinen oder Kommunikationsnetzwerken, werden derzeit maßgeblich durch personalisierte Werbung finanziert. Diese basiert auf dem Einsatz von Tracking-Technologien und der Erstellung von Interessenprofilen anhand des Online-Verhaltens der Nutzer/innen. Weil diese omnipräsenten Geschäftsmodelle bei der Verabschiedung der DS-GVO jedoch weitgehend ausgeblendet wurden und zudem auch nicht berücksichtigt wurde, dass zahlreiche prominente Persönlichkeiten die vermögenswerten Bestandteile ihrer Persönlichkeitsrechte kommerziell verwerten, befindet sich die DS-GVO auf einem Kollisionskurs mit dem Schuldrecht und der ökonomischen Realität. Der Konflikt zwischen der staatlichen Pflicht zum Schutz der informationellen Selbstbestimmung einerseits und der gleichzeitigen Achtung der Privatautonomie der Datensubjekte und der datenverarbeitenden Unternehmen andererseits ist mittlerweile offenkundig. Dennoch besteht derzeit kein überzeugender rechtlicher Rahmen, der die grundrechtliche Pflicht zum Schutz der Datensubjekte und die

wirtschaftliche Realität zum Ausgleich bringt. Diese schwierige Aufgabe wird stattdessen an die Rechtsanwender und damit insbesondere an den EuGH überantwortet.

Die vorliegende Arbeit macht einen Vorschlag, wie dieses Spannungsverhältnis aus dem Schutz von Datensubjekten und der Anerkennung von personenbezogenen Daten als Objekt vertraglicher Austauschbeziehungen aufgelöst werden kann. Dabei bewahrt der Vorschlag den tradierten Rahmen des Rechts auf informationelle Selbstbestimmung, erweitert aber den Handlungsspielraum für Datensubjekte und solche datenverarbeitende Unternehmen, die keine dominanten Gatekeeper sind. Infolgedessen ermöglicht das nachfolgend vorgeschlagene Modell einer abgestützten informationellen Privatautonomie die Synchronisierung von Datenschutz- und Vertragsrecht.

Die Arbeit lag der Juristischen Fakultät der Ludwig-Maximilians-Universität München im Wintersemester 2021/22 als Habilitationsschrift vor. Sie hat entscheidend von einer Reihe von Personen profitiert. Mein Dank gilt in erster Hinsicht meinem akademischen Lehrer, Herrn Professor Ansgar Ohly, der sich früh für dieses Thema begeistern konnte und mir für diese Untersuchung ideale Bedingungen und größtmögliche Freiheiten am Lehrstuhl gewährt hat. Herrn Professor Hans Christoph Grigoleit danke ich herzlich für die sehr zügige Erstellung des Zweitgutachtens und wertvolle inhaltliche Hinweise und Anregungen. Herrn Professor Herbert Zech und Herrn Professor Matthias Leistner danke ich für zahlreiche anregende Gespräche und Diskussionen zum Thema. Herrn Professor Franz Hofmann und Herrn Professor Martin Stierle danke ich für die gute und freundschaftliche Zusammenarbeit an der LMU. Der Druck und die Zugänglichmachung als Open-Access-Publikation wurden großzügig durch den LMU Open Access Fonds, den LMU PostDoc Fonds, die Johanna und Fritz Buch Gedächtnis-Stiftung und die Studienstiftung ius vivum gefördert.

Besonders herzlich danke ich meiner Familie. Meine Frau und mein Sohn mussten mit mir durch die düsteren Täler schreiten, die eine Habilitationsschrift regelmäßig mit sich bringt. Ihnen ist diese Arbeit gewidmet.

Stuttgart, im Mai 2022 Andreas Sattler

Inhaltsübersicht

Vorwort V
Inhaltsverzeichnis IX

Einführung 1

1. Kapitel: Grundrechtliche Gewährleistung von informationeller Privatautonomie 15

A. Dominanz der abwehrrechtlichen Dimension der Grundrechte 17
B. Asymmetrische Grundrechtssensibilität der DS-GVO 32
C. Gefährdung der informationellen Privatautonomie 57
D. Fazit: Privatrechtssensible Auslegung der DS-GVO 66

2. Kapitel: Subsidiarität der Interessenabwägung 73

A. Die Interessenabwägung als Generalklausel 75
B. Erleichterung der Datenverarbeitung durch eine Interessenabwägung 96
C. Herausforderungen einer Datenverarbeitung auf Grundlage der Interessenabwägung 99
D. Fazit: Funktion als Schrittmacher 139

3. Kapitel: Entlastungsfunktion der vertragsakzessorischen Datenverarbeitung 143

A. Komplexes Verhältnis zum nationalen Schuldrecht 145
B. Erleichterungen durch eine vertragsakzessorische Datenverarbeitung 148
C. Herausforderungen der vertragsakzessorischen Datenverarbeitung . 152
D. Fazit: Entlastungsfunktion von Art. 6 Abs. 1 lit. b DS-GVO 202

4. Kapitel: Die Einwilligung als Nukleus des europäischen Datenschuldrechts 205

A. Vorrang der Einwilligung 206
B. Die Einwilligung zwischen Unter- und Übermaßverbot 230
C. Stufenleiter der Einwilligung 247
D. Fazit 273

5. Kapitel: Stufenmodell der Erlaubnistatbestände 277

A. Erste Stufe: Enge Auslegung der Interessenabwägung 278
B. Zweite Stufe: Enge Auslegung der Vertragsakzessorietät 287
C. Dritte Stufe: Flexibilisierung des Einwilligungstatbestands 297
D. Übersicht zum Stufenmodell 356

6. Kapitel: Erforderliche Abstützungen der informationellen Privatautonomie 359

A. Standardisierte Kennzeichnung und Privacy Score 361
B. Kontroll-Cockpit für datenschutzrechtliche Erklärungen 381

Zusammenfassung 413

Literaturverzeichnis 425
Stichwortverzeichnis 461

Inhaltsverzeichnis

Vorwort V
Inhaltsübersicht VII

Einführung 1

I. Gegenstand und Zielsetzung 1
II. Forschungsstand 8
III. Gang der Untersuchung 11

1. Kapitel: Grundrechtliche Gewährleistung von informationeller Privatautonomie 15

A. Dominanz der abwehrrechtlichen Dimension der Grundrechte 17

I. Das RaiS als Grundlage des deutschen Datenschutzrechts 19
1. Industrialisierung und technischer Fortschritt 20
2. Prägender Einfluss der (Rechts-)Soziologie 21
3. Prägung durch Erfahrungen der nationalsozialistischen Diktatur 23
4. Extensive Auslegung der verfassungsgerichtlichen Urteile 24
II. Folgenlose Kritik am einheitlichen Schutzansatz 26
1. Kritik am rechtssoziologisch determinierten Zeitgeist 27
2. Kritik an der überschießenden Umsetzung des RaiS 28
3. Fazit: Fehlende privatrechtliche Unterfütterung des Datenschutzes 30

B. Asymmetrische Grundrechtssensibilität der DS-GVO 32

I. Wirkung europäischer Grundrechte im Privatrechtsverhältnis . . . 34
II. Schutz- und Gewährleistung durch Art. 7 und Art. 8 GRCh 36
1. Keine Abgrenzung der Schutzbereiche durch den EuGH 37
2. Keine (klare) Schutzbereichsabgrenzung in der Literatur 39
3. Geringe Berücksichtigung der aktiven Entfaltungsfreiheit 41
a) Achtung des Privat- und Familienlebens, Art. 7 GRCh 41
b) Schutz personenbezogener Daten, Art. 8 GRCh (Art. 16 AEUV) 43
aa) Schutzbereich des Art. 8 GRCh 43
bb) Primärrechtlicher Vorrang der Einwilligung 46
III. Schutz der unternehmerischen Freiheit, Art. 16 GRCh 48

IV. Schutz der allgemeinen Handlungsfreiheit von Datensubjekten . . . 50
V. Informationelle Privatautonomie und gerichtliche Kooperation . . . 53

C. Gefährdung der informationellen Privatautonomie 57

I. Begriffliche Bezeichnung als Zuspitzung 58
II. Konstitutionalisierung des sekundärrechtlichen Datenschutzes . . . 58
1. Verarbeitungsverbot als Einhaltung des Untermaßverbots 59
2. Verstoß gegen das Übermaßverbot (Verhältnismäßigkeit) 60
3. Anerkennung der Kommerzialisierung (Daten als Gegenleistung) 64

D. Fazit: Privatrechtssensible Auslegung der DS-GVO 66

2. Kapitel: Subsidiarität der Interessenabwägung 73

A. Die Interessenabwägung als Generalklausel 75

I. Berechtigte Interessen des Verantwortlichen oder Dritter 76
1. Begrenzung des Drittinteresses zugunsten einer Datenverarbeitung 77
2. Irrelevanz von Drittinteressen zulasten einer Datenverarbeitung 79
II. Erforderlichkeit der Datenverarbeitung zur Interessenwahrung . . . 80
III. Kein Überwiegen der Interessen des Datensubjekts 82
1. Dichotomie der Interessen 82
2. Formulierung zugunsten der Rechtmäßigkeit 83
3. Fehlen von Abwägungskriterien 84
a) Persönliche Eigenschaften von Datensubjekten 85
b) Erwartungshorizont der Datensubjekte 86
c) Öffentlich zugängliche personenbezogene Daten 87
IV. Option zur Herstellung der Entscheidungszuständigkeit 89
1. Einordnung des Widerspruchsrechts 90
a) Widerspruchsbegründung 91
b) Rechtsfolge: Qualifizierte Interessenabwägung 92
2. Kollision mit der Widerruflichkeit der Einwilligung 93

B. Erleichterung der Datenverarbeitung durch eine Interessenabwägung 96

I. Erleichterung: Flexible Reaktion auf die ubiquitäre Datenverarbeitung 97
II. Erleichterung: Reagibilität auf die Multi-Relationalität 98

C. Herausforderungen einer Datenverarbeitung auf Grundlage der Interessenabwägung 99

I. Herausforderung: Paradoxon aus Unsicherheit und geringer Flexibilität 99
1. Fehlende Konkretisierung der Interessenabwägung 100
a) Art. 6 Abs. 1 lit. f DS-GVO als missglückte Generalklausel . . . 101
b) Nachteile einer Typisierung durch Richterrecht 103
c) Interimistische Maßnahmen zur Konkretisierung 105

2. Restriktive Anwendung für personalisierte Direktwerbung 107
a) Technische Grundlagen automatisierter personalisierter Werbung 108
b) Restriktive Auslegung von Art. 6 Abs. 1 lit. f für Direktwerbung 111
aa) Ausgangspunkt: Personalisierte Werbung als anerkanntes Interesse 112
bb) Korrektur: Keine Direktwerbung durch Werbenetzwerke 115
3. Erweiterung des Anwendungsbereichs der Interessenabwägung 118
a) Verarbeitung besonders sensibler personenbezogener Daten . . 119
b) Verarbeitung von besonders sensiblen Daten im Kontext des IoT 123
c) Besonders sensible Daten als Trainingsdaten für ML 127
aa) Maschinelles Lernen: Trainieren statt Programmieren . . 128
bb) Trainieren von ML auf Grundlage einer Interessenabwägung 130
II. Herausforderung: Gefahr eines Unterlaufens der Einwilligung . . . 134
III. Herausforderung: Geringere faktische Kontrolldichte 136

D. Fazit: Funktion als Schrittmacher 139

3. Kapitel: Entlastungsfunktion der vertragsakzessorischen Datenverarbeitung 143

A. Komplexes Verhältnis zum nationalen Schuldrecht 145

B. Erleichterungen durch eine vertragsakzessorische Datenverarbeitung 148

I. Nationales Schuldrecht als Entdeckungsverfahren 148
II. Nationales Vertragsrecht als Differenzierungsfeld 150

C. Herausforderungen der vertragsakzessorischen Datenverarbeitung . . 152

I. Herausforderung: Überfordernde Angemessenheitskontrolle 153
1. Eingeschränkte Kontrolle des vertraglichen Synallagmas 155
a) Gründe für die Reduktion der gerichtlichen Kontrolldichte . . 156
b) Marktversagen als Grenze der reduzierten Kontrolldichte . . . 158
2. Personenbezogene Daten und Marktversagen 161
a) Mangelnde Aufmerksamkeit für den Hauptgegenstand 161
b) Personenbezogene Daten als Leistung – ein Zitronenmarkt . . 164
c) Geringe Kompensation durch eine aufmerksame Minderheit . . 166
d) Keine abschließende Regelung durch die Klausel-RL 168
e) Fehlender Maßstab für eine gerichtliche Angemessenheitskontrolle 170
3. Verdrängung der Klausel-RL durch die DS-GVO 174
a) Verhältnis von Klausel-RL und DS-GVO 174
b) Höhere Flexibilität der DS-GVO gegenüber der Klausel-RL . . 177

II. Herausforderung: Gefährdung des einheitlichen Datenschutzrechts 180
1. Geringe Regelungsdichte des Art. 6 Abs. 1 lit. b DS-GVO 180
2. Gefahr einer Umgehung der Anforderungen an die Einwilligung 182
3. Keine Überwindung der Defizite der Einwilligung 184
4. Komplexität und Fehleranfälligkeit der Rechtsfindung 185
5. Art. 6 Abs. 1 lit. b als Gefährdung der Regelungsziele der DS-GVO 187
6. Notwendigkeit umfassender Angleichung des Datenschuldrechts 191
III. Herausforderung: Keine Synchronisierung von DS-GVO und DID-RL 193
1. Keine Synchronisierung durch den europäischen Gesetzgeber . . 193
2. Mehrdeutige Stellungnahme des EDSA 196
3. Art. 6 Abs. 1 lit. b als potenzieller Fluchtweg aus der DID-RL . . 198

D. Fazit: Entlastungsfunktion von Art. 6 Abs. 1 lit. b DS-GVO 202

4. Kapitel: Die Einwilligung als Nukleus des europäischen Datenschuldrechts 205

A. Vorrang der Einwilligung 206

I. Gründe für einen Vorrang der Einwilligung 206
1. Datenschutz als Individualschutz 206
2. Systematik der DS-GVO 208
3. Einheitlichkeit der Rechtsanwendung 210
4. Unionsautonomie 212
II. Voraussetzungen der Einwilligung 214
1. Einwilligungsfähigkeit als Spezifikation der Freiwilligkeit 214
2. Bestimmtheit und Zweckbindung 216
3. Informiertheit 219
4. Freiwilligkeit der Einwilligungserteilung 221
5. Widerruflichkeit der Einwilligung 224

B. Die Einwilligung zwischen Unter- und Übermaßverbot 230

I. Grenzen des Übermaßverbots für Art. 7 Abs. 4 DS-GVO 231
1. Strenges Kopplungsverbot als Marktzutrittsbarriere 235
2. Kommerzialisierung durch Datensubjekte als Unternehmer . . . 236
II. Grenzen des Übermaßverbots für die sog. freie Widerruflichkeit . . 237
1. Die freie Widerruflichkeit als Marktzutrittsbarriere 239
2. Kommerzialisierung durch Datensubjekte als Unternehmer . . . 241
III. Fazit 245

C. Stufenleiter der Einwilligung 247

I. Die Grenzen der schlichten, einseitigen Einwilligung 247

II. Die Einwilligung in der Stufenleiter der Gestattungen 249
1. Schlichte Einwilligung und schuldrechtliche Gestattung 250
2. Die schuldrechtliche Gestattung als Stabilisierung von Beziehungen 257
III. Das Verhältnis zwischen Einwilligung und Vertrag 261
1. Die Argumente für eine Trennung der Einwilligung vom Vertrag 261
a) Trennung zwischen Einwilligung und Vertrag in der DS-GVO 262
b) Trennung zwischen Einwilligung und Vertrag in der DID-RL 263
2. Die Einwilligung als Bestandteil vertraglicher Vereinbarungen . . 268
a) Der deutsche Streit über die Rechtsnatur der Einwilligung . . . 268
b) Die Einwilligung als Instrument der Synchronisierung 269
c) Konsequenzen der Ausdifferenzierung des Einwilligungsbegriffs 271

D. Fazit 273

5. Kapitel: Stufenmodell der Erlaubnistatbestände 277

A. Erste Stufe: Enge Auslegung der Interessenabwägung 278

I. Art. 6 Abs. 1 lit. f DS-GVO als Schrittmacher 279
II. Wesentliche Herausforderungen für die Interessenabwägung 281
1. Keine personalisierte Werbung durch Werbenetzwerke 282
2. Begrenzung der Informationspflicht aus Art. 21 Abs. 4 DS-GVO 284
3. Sensible personenbezogene Daten und Interessenabwägung . . . 286

B. Zweite Stufe: Enge Auslegung der Vertragsakzessorietät 287

I. Grundsatz: Beschränkung auf unterstützende Verarbeitungen . . . 288
II. Erste Herausforderung: Personalisierung digitaler Produkte 290
1. Kern der Abgrenzungsschwierigkeit 291
2. Keine Lösungsvorschläge durch den Gesetzgeber 292
III. Zweite Herausforderung: Einbeziehung von Dienstleistern 295

C. Dritte Stufe: Flexibilisierung des Einwilligungstatbestands 297

I. Gründe für eine Flexibilisierung 297
II. Flexibilisierung der Freiwilligkeit der Einwilligung 298
1. Kriterium: Marktmacht des Verantwortlichen 300
a) Strenges anbieterbezogenes Kopplungsverbot 301
b) Marktbezogenes Kopplungsverbot 302
c) Art. 7 Abs. 4 als generalklauselartiges Berücksichtigungsgebot 303
aa) Keine Angemessenheitskontrolle der Leistungsbeziehung 303
bb) Freiwilligkeit als Ursache kompetenzieller Konflikte . . . 306
cc) Kartellrechtsakzessorische und asymmetrische Anwendung 311
2. Kriterium: Eigenschaften des Datensubjekts 316
a) Einwilligung durch Kinder 316

b) Unternehmerisch handelnde Datensubjekte 319
3. Kriterium: Situationsadäquates Verhalten des Verantwortlichen 321
4. Fazit 324
III. Flexibilisierung der Widerruflichkeit der Einwilligung 328
1. Teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO 331
2. Kriterien für eine teleologische Reduktion 332
a) Marktmacht des Verantwortlichen 332
b) Unternehmerisch handelnde Datensubjekte 334
c) Als Verbraucher handelnde Datensubjekte 336
aa) Freie Widerruflichkeit als Anreiz für die sofortige Verwertung 337
bb) Zeitweise bindende Einwilligung und Datenaltruismus . . 340
3. Abstützungen einer Disposition über Art. 7 Abs. 3 S. 1 DS-GVO 341
a) Keine Disposition gegenüber marktmächtigen Verantwortlichen 342
b) Befristung der Unwiderruflichkeit im B2C-Verhältnis 343
c) Keine stillschweigende Verlängerung des Widerrufsausschlusses 345
d) Jederzeitiger Widerruf aus wichtigem Grund 347
aa) Widerrufsgründe aus der Sphäre des Verantwortlichen . . 348
bb) Widerrufsgründe aus der Sphäre des Datensubjekts 348
4. Fazit: Abgestützte Abdingbarkeit der sog. freien Widerruflichkeit 351

D. Übersicht zum Stufenmodell 356

6. Kapitel: Erforderliche Abstützungen der informationellen Privatautonomie 359

A. Standardisierte Kennzeichnung und Privacy Score 361

I. Fehlende Voraussetzungen für das Informationsmodell 361
II. Unionweit einheitliche Kennzeichnung 363
1. Rechtsgrundlage für eine unionsweite Standardisierung 363
2. Reichweite der Rechtsgrundlage für eine Standardisierung 365
3. Notwendigkeit einer mehrstufigen Darstellung von Information 366
a) Tatsächliche Verständlichkeit und verfügbare Vollständigkeit 367
b) Stufenweise Verbindlichkeit der Kennzeichnungskombination 369
c) Erste Informationsstufe: Kennzeichen-Kombination 370
4. Die Verarbeitungsgrundlage als zentrales Kriterium 373
III. Klassifikation als Anwendungsbereich für ML 377
IV. Fazit 379

B. Kontroll-Cockpit für datenschutzrechtliche Erklärungen 381

I. Kontroll-Cockpit als Ausgangspunkt für PIMS 383
II. Gesetzliche Anknüpfungspunkte in der DS-GVO 385

1. Einwilligung und Einwilligungswiderruf 386
a) Einwilligungserteilung 386
aa) Informiertheit der Einwilligung 386
bb) Differenziertheit der Einwilligung 389
cc) Ausdrücklichkeit der Einwilligung 391
b) Einwilligungswiderruf 393
aa) Einfachheit des Einwilligungswiderrufs 393
bb) Differenziertheit des Einwilligungswiderrufs 395
cc) Informationspflichten nach Einwilligungswiderruf 397
2. Widerspruch gegen die Datenverarbeitung, Art. 21 DS-GVO . . . 398
a) Widerspruchserklärung 399
b) Begründung des Widerspruchs 403
c) Informationspflichten 405
d) Fazit 405
3. Datenschutz durch Technikgestaltung, Art. 25 Abs. 1 DS-GVO 406
a) Pflicht und Anreiz für die Implementierung eines Kontroll-Cockpits 406
b) Mindestanforderungen an ein Kontroll-Cockpit 408
III. Übersicht der Mindestanforderungen an ein Kontroll-Cockpit . . . 409

Zusammenfassung 413

I. Hauptthese 413
II. Hauptthese 414
III. Hauptthese 416
IV. Hauptthese 417
V. Hauptthese 418
VI. Hauptthese 421

Literaturverzeichnis 425
Stichwortverzeichnis 461

Einführung

I. Gegenstand und Zielsetzung

Der rechtliche Schutz vor einer Verarbeitung von personenbezogenen Daten (verkürzt: Datenschutzrecht) ist ein sehr konfliktreiches Rechtsgebiet. Untersucht man das Datenschutzrecht aus privatrechtlicher Perspektive, so sind zwei große Konflikte besonders augenfällig.

Erstens befinden sich das Datenschutzrecht und die besonders erfolgreichen Geschäftsmodelle mehrseitiger Plattformen auf einem Kollisionskurs. Die amerikanischen Unternehmen *Google* (*Alphabet*), *Amazon*, *Facebook* (*Meta Platforms*), *Apple* und *Microsoft* (zusammengefasst: GAFAM) und ihre chinesischen Wettbewerber *Baidu*, *Alibaba* und *Tencent* (zusammengefasst: BAT) stehen stellvertretend für Geschäftsmodelle, die in einem großen Ausmaß auf der Verarbeitung von personenbezogenen Daten ihrer Endnutzer (und Dritter) für ein Profiling beruhen. Dieses Profiling, das durch den Einsatz von Techniken der sog. Künstlichen Intelligenz stetig verbessert wird, liefert die Grundlage dafür, Werbekunden gegen Geld eine personalisierte oder zumindest stratifizierte Werbung gegenüber den Endnutzern anbieten zu können.

Die Kollision zwischen dem Datenschutzrecht und den Geschäftsmodellen mehrseitiger Plattformen ist nicht neu. Solange Plattformbetreiber bei Verstößen gegen das Datenschutzrecht jedoch kaum ökonomische Konsequenzen zu befürchten hatten, genügte es aus ihrer Sicht, den Schutz personenbezogener Daten am Horizont zu beobachten. Das Datenschutzrecht zwang die großen Plattformbetreiber zu keinen oder allenfalls sehr geringen Anpassungen ihrer Geschäftsmodelle.

Am 25.05.2018 hat sich dieses Bild verändert. Obwohl das Potenzial für *tatbestandliche* Konflikte seit der Anwendbarkeit der DS-GVO[1] kaum zugenommen hat – die DS-GVO behält wesentliche Regelungsinhalte der Datenschutz-RL von 1995[2] bei – ist für die datenschutzrechtlich Verantwortlichen das Risiko, also die Kombination aus der Entdeckungswahrscheinlichkeit von Rechtsver-

---

[1] Verordnung (EU) 2016/679 v. 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119, v. 04.05.2016, S. 1 ff.

[2] Richtlinie 95/46/EG v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, v. 23.11.1995, S. 31 ff.

stößen und der Höhe des potenziellen Bußgelds, mit der DS-GVO grundlegend gestiegen. Indem das potenzielle Bußgeld proportional mit dem ökonomischen Erfolg des Verantwortlichen steigt, bewahrt das Datenschutzrecht seine Relevanz auch mit zunehmender Größe des datenschutzrechtlich Verantwortlichen.

Unabhängig davon, ob die Auslegung und Anwendung der DS-GVO in der Praxis ein ausreichendes Mindestmaß an Rechtssicherheit bietet,[3] ob die Kriterien und Details für die Bestimmung eines angemessenen und abschreckenden Bußgelds im Einzelfall überzeugen und ob es sinnvoll und ökonomisch tragfähig ist, den gleichen Regelungsansatz auf andere Rechtsverstöße auszudehnen.[4] Es bestehen keine Zweifel: Die potenzielle Höhe eines Bußgelds gemäß Art. 83 DS-GVO hat die alte Erkenntnis bestätigt, dass die Steuerungsfunktion des Rechts maßgeblich von effektiven Mechanismen zu dessen Durchsetzung abhängt.[5] Um Kollisionen mit der DS-GVO und potentiell hohe Bußgeldbescheide zu vermeiden,[6] sind die Plattformbetreiber zunehmend gezwungen, ihre Geschäftsmodelle, jedenfalls aber die rechtliche Beziehung zu ihren Endnutzern anzupassen.

---

[3] Erst im Jahr 2021 erreichten den EuGH erste Auslegungsfragen von fundamentaler Bedeutung: *OLG Düsseldorf*, Vorlagebeschl. v. 24.03.2021, Kart 2/19 (V) = NZKart 2021, 306 ff.; *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[4] Vgl. Art. 26 (Geldbußen) des Vorschlags der EU-Kommission für eine Verordnung über bestreitbare und faire Märkte im digitalen Sektor (Gesetz über digitale Märkte) vom 15.12.2020, COM(2020) 842 final (englisch: Digital Markets Act oder kurz: DMA-Vorschlag); sowie Art. 42 (Sanktionen) des Vorschlags der EU-Kommission für eine Verordnung über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG vom 15.12.2020, COM(2020) 825 final (englisch: Digital Service Act oder kurz: DSA-Vorschlag).

[5] Die Frage, wer neben den Datensubjekten und im Auftrag der betroffenen Datensubjekte (Art. 80 Abs. 1 DS-GVO) zusätzlich gemäß Art. 80 Abs. 2 und Art. 84 Abs. 1 DS-GVO zur Durchsetzung von Ansprüchen aus UWG und UKlaG aktivlegitimiert sein sollte, hat der BGH dem EuGH vorgelegt: *BGH*, Beschl. v. 28.05.2020, I ZR 186/17 = GRUR 2020, 896 (Rn. 35 ff.) – *App-Zentrum*; Für eine Begrenzung auf qualifizierte Verbände: *Köhler*, WRP 2018, 1269 (1272); *ders.*, WRP 2019, 1279 (1283); *Ohly*, GRUR 2019, 686 (688 f.); für eine durch die DS-GVO unbeeinflusste Aktivlegitimation von Mitbewerber nach dem UWG: *Uebele*, GRUR 2019, 694 (697 f.).

[6] Die luxemburgische Datenschutzbehörde (CNPD) verhängte gegen die europäische Tochter von *Amazon* mit Sitz in Luxemburg ein (nicht rechtskräftiges) Bußgeld in Höhe von 746 Mio. Euro (https://www.heise.de/news/Datenschutz-Rekordstrafe-von-746-Millionen-Euro-fuer-Amazon-in-Luxemburg-6152051.html, zuletzt abgerufen am 19.05.2022). Die französische Datenschutzbehörde (CNIL) verhängte 2019 – jeweils nur für Frankreich – eine Strafe von 50 Mio. Euro gegen *Google* (https://www.heise.de/news/DSGVO-Verstoesse-Conseil-d-Etat-bestaetigt-50-Millionen-Strafe-gegen-Google-4790235.html, zuletzt abgerufen am 19.05.2022) sowie im Dezember 2020 in Höhe von 100 Mio. Euro gegen *Google* und 35 Mio. Euro gegen *Amazon* (https://www.heise.de/news/Frankreich-Datenschuetzer-verhaengen-Millionen-Bussgelder-gegen-Google-und-Amazon-4985956.html, zuletzt abgerufen am 19.05.2022). Der Hamburgische Datenschutzbeauftragte hat wegen Verstößen gegen die DS-GVO im Beschäftigungsverhältnis für Deutschland ein Bußgeld von knapp 35,3 Mio. Euro gegen *Hennes & Mauritz* (H&M) verhängt (https://www.heise.de/news/DSGVO-Deutsche-Rekordbusse-von-35-3-Millionen-Euro-gegen-H-M-4917437.html, zuletzt abgerufen am 19.05.2022).

Besonders deutlich wird dies an dem Sachverhalt, der einem Vorlagebeschluss des *ÖOGH* zum *EuGH* zugrunde liegt.[7] Darin geht es maßgeblich darum, ob *Facebook* (jetzt: *Meta Platforms*) die personenbezogenen Daten der Endnutzer – soweit es sich dabei nicht um besonders sensible personenbezogene Daten handelt – vertragsakzessorisch und somit auf Grundlage des Nutzungsvertrags i. V. m. Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig verarbeiten kann, oder ob insoweit spezifische Einwilligungen der Endnutzer erforderlich sind. Dem Vorlagebeschluss des *ÖOGH* ging ein Urteil des *OLG Wien* voraus, in dem dieses das Profiling für personalisierte Werbung durch *Facebook* auf Grundlage eines in der österreichischen Rechtsordnung nicht ausdrücklich geregelten, also atypischen Schuldverhältnisses für rechtmäßig erachtet hatte. Nach Ansicht des *OLG Wien* ist diese Datenverarbeitung (auch) zur Finanzierung des Angebots von *Facebook* und damit zur Erfüllung dieses atypischen Nutzungsvertrags i. S. d. Art. 6 Abs. 1 lit. b DS-GVO erforderlich.[8]

Die Antwort des *EuGH* auf die nun erfolgte Vorlage des *ÖOGH* wird grundlegende Auswirkungen auf die Geschäftsmodelle der Betreiber von solchen mehrseitigen Plattformen haben, die Datensubjekten digitale Produkte bereitstellen und dieses Angebot finanzieren, indem sie mit Hilfe von personenbezogenen Daten Profile über ihre Endnutzer erstellen und diese im Verhältnis zu ihren Werbekunden für personalisierte Werbeansprache monetisieren. Abhängig davon, welche datenschutzrechtliche Grundlage der *EuGH* für solche Austauschverhältnisse zwischen Datensubjekten und Verantwortlichen heranzieht, kommt es für die Rechtmäßigkeit dieser Geschäftsmodelle auf die unionsrechtlich vereinheitlichten Anforderung an die datenschutzrechtliche Einwilligung oder auf das lediglich teilweise harmonisierte nationale Vertragsrecht der Mitgliedstaaten an.[9]

Zweitens wird anhand des Vorlagebeschlusses des *ÖOGH* auch deutlich, dass sich das europäische Datenschutzrecht und das nationale Schuldrecht der Mitgliedstaaten auf einem Kollisionskurs befinden. Die europäische DS-GVO ist weder mit dem nationalen Schuldrecht noch den privatrechtlichen Grundprinzipien synchronisiert.

Sprachlich lässt sich diese Dominanz der DS-GVO daran festmachen, dass die schuldrechtlich zutreffende Bezeichnung von personenbezogenen Daten als „Gegenleistung" einem postmodernen Sakrileg gleichgestellt wird.[10] In voraus-

---

[7] *ÖOGH*, Vorlagebeschl. v. 22.07.2021, 6 Ob 56/21k – *Schrems* [*III*].

[8] *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 27. Diese Ansicht ist nicht überzeugend, hierzu unten: Kapitel 3 C.II.4./5 und III.3.

[9] Obwohl es wenig überrascht, dass *Meta Platforms* (ehemals: *Facebook*) häufig beklagte Partei ist, birgt dieses Vorlageverfahren die Gefahr, dass der EuGH sich die Folgen seiner Entscheidung für andere, kleinere Verantwortliche zu wenig bewusst macht.

[10] *EDSB*, Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, 14.03.2017, S. 10/Nr. 17; sowie: Rede von *Giovanni Buttarelli* (ehemaliger EU-Datenschutz-Beauftragter), verfügbar unter

eilender *political correctness* meidet der europäische Gesetzgeber deshalb mittlerweile[11] diesen Begriff, ohne dadurch den tatsächlich bestehenden Konflikt zwischen Datenschutz- und Schuldrecht zu lösen.[12] Zwar soll mit dem europäischen Data Act auch die Nutzung von personenbezogenen Daten verbessert werden; wie dieses Ziel sich jedoch mit den Anforderungen der DS-GVO synchronisieren lässt, bleibt einstweilen offen.[13]

Rechtlich bringen Art. 3 Abs. 8 der Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL)[14] und § 327q BGB[15] diese Dominanz der DS-GVO zum Ausdruck. Zwar versucht der deutsche Gesetzgeber das nationale Schuldrecht gegenüber der DS-GVO zu immunisieren. Gemäß § 327q Abs. 1 BGB soll die Abgabe einer datenschutzrechtlichen Erklärung des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Weil jedoch per-

---

https://edps.europa.eu/sites/edp/files/publication/17-01-12_digital_content_directive_sd_en.pdf, zuletzt abgerufen am 19.05.2022 („So, even if some people treat personal data as commodity, under EU law it cannot be a commodity. There might well be market for personal data, just like there is, tragically, a market for live human organs.")

[11] Anders noch *EU-Kommission* Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM/2015/0634 final. (Art. 3 Abs. 1 des Vorschlags erstreckte den Anwendungsbereich auf „alle Verträge, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalte bereitstellt oder sich hierzu verpflichtet und der Verbraucher *als Gegenleistung* einen Preis zahlt oder aktiv eine andere Gegenleistung als Geld in Form *personenbezogener* oder anderer *Daten erbringt*".

[12] Ohne Bezugnahme auf die zu diesem Zeitpunkt bereits verabschiedete, aber noch nicht umsetzungspflichtige Richtlinie (EU) 2019/770 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DID-RL) kam das *OLG Wien* zu einer anderen Beurteilung. Danach sei es insbesondere „legitim, dass ein marktwirtschaftlich operierendes Unternehmen, das für bestimmte Dienstleistungen kein Geld verrechnet, im Rahmen der Gesetze auf anders geartete Finanzierungsquellen zurückgreift. […]. Denn nur diese Datenverwertung ermöglicht maßgeschneiderte Werbung, die das von der Beklagten geschuldete „personalisierte Erlebnis" in wesentlichem Maße prägt und der Beklagten zugleich die für den Aufrechterhaltung der Plattform und die Erzielung eines Gewinns notwendigen Einkünfte verschafft." *OLG Wien*, Urt. v. 07.12.2020 (nicht rechtskräftig), GZ 11 R 153/20f, 11 R 154/20b-99 S. 28. Zur fehlenden Synchronisierung zwischen DS-GVO und DID-RL, unten Kapitel 3 C.III.2.

[13] *Europäische Kommission*, Inception of Assessment, Ref. Ares(2021)3527151 v. 28.05. 2021, S. 7 (Likely impacts on fundamental rights): „Since personal data […] fall into the scope of some elements of this initiative (e. g. improving usability of data linked to natural persons), the measure will be designed in a way that fully complies with the existing rules on personal data protection and ePrivacy".

[14] ABl. v. 22.05.2019, L 136/1. Art. 3 Abs. 8 DID-RL lautet: „Das Unionsrecht betreffend den Schutz personenbezogener Daten gilt für alle personenbezogenen Daten, die im Zusammenhang mit Verträgen gemäß Absatz 1 verarbeitet werden. Insbesondere lässt diese Richtlinie die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG unberührt. Im Fall von Widersprüchen zwischen Bestimmungen dieser Richtlinie und dem Unionsrecht zum Schutz personenbezogener Daten ist letzteres maßgeblich."

[15] Eingeführt durch das Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen v. 25.06. 2021, BGBl. 2021 Teil I Nr. 37, 30.06.2021, 2123 ff.

sonenbezogene Daten tatsächlich und rechtlich zunehmend als Leistungsgegenstand behandelt und vereinbart werden und einige der derzeit ökonomisch besonders erfolgreichen Geschäftsmodelle von *GAFAM* und *BAT* – in unterschiedlichem Ausmaß – auf dem Zugang zu personenbezogenen Daten beruhen, entspricht dieser schlichte Abgrenzungsversuch in § 327q Abs. 1 BGB eher einem Wunschdenken, als dem Anspruch, die tatsächliche Realität rechtlich abzubilden.[16]

Indem § 327q Abs. 3 BGB alle Ersatzansprüche des *Unternehmers* gegen den *Verbraucher* wegen Abgabe einer datenschutzrechtlichen Erklärung ausschließt, die eine Einschränkung der rechtmäßigen Datenverarbeitung bewirkt, hat der deutsche Gesetzgeber zwar zu einem kräftigen Befreiungsschlag ausgeholt, um den gordischen Knoten aus europäischem Datenschutz- und nationalem Schuldrecht zumindest im B2C-Verhältnis zu lösen. Auf den zweiten Blick erinnert dieser Befreiungsversuch des Gesetzgebers jedoch an den verzweifelten Versuch des *Laokoon*, sich aus dem Griff der Schlangen zu befreien. § 327q BGB ist nicht in der Lage, den tatsächlich bestehenden Konflikt zwischen einer jederzeit und grundlos widerruflichen Einwilligung und dem schuldrechtlichen Prinzip des *do ut des* befriedigend aufzulösen.[17] Eine solche Lösung ist aber jedenfalls in Fällen erforderlich, in denen Datensubjekte ihre personenbezogenen Daten bewusst dafür einsetzen, um ihr monetäres Konsumbudget zu schonen (Verbraucher) oder um selbst Gewinne zu erwirtschaften (Unternehmer).

Die Ursache dafür, dass das Datenschutzrecht und das Schuldrecht sich auf Kollisionskurs befinden, ist leicht zu identifizieren. Beginnend mit dem ersten BDSG von 1977[18] beruht das deutsche und im Anschluss hieran das europäische Datenschutzrecht auf einem Verarbeitungsverbot mit Erlaubnisvorbehalt (§ 3 Abs. 1 BDSG von 1977 – jetzt: Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO). Das Schuldrecht hingegen beruht auf einer Erlaubnis mit Verbotsvorbehalt (§§ 311, 241 BGB).[19]

---

[16] Insbesondere dürfte damit auch noch nicht „jedweder Diskussion um eine mögliche Einschränkung des Widerrufsrechts […] ein Riegel vorgeschoben" worden sein. So aber: *Spindler*, MMR 2021, 528 (530). Hierzu unten Kapitel 5 C.III.

[17] Zum hier unterbreiteten Vorschlag eines befristeten Ausschlusses der Widerruflichkeit durch teleologische Reduktion von Art. 7 Abs. 3 S. 1 DS-GVO unten Kapitel 5 C.III, sowie zuvor: *Sattler*, JZ 2017, 1036 (1041 f.). Sollte der EuGH der Rechtsauffassung von *Facebook*, des LG Wien und des OLG Wien folgen, würde das Geschäftsmodell von *Facebook* und anderen durch personalisierte Werbung finanzierten Kommunikationsplattformen nicht nur gemäß Art. 6 Abs. 1 lit. b DS-GVO weitgehend den Vorgaben der DS-GVO entgehen, sondern es entstünden auch schwerwiegende Abgrenzungsschwierigkeiten zum Anwendungsbereich der DID-RL bzw. von §§ 327 ff. BGB. Hierzu Kapitel 3 C.III.3.

[18] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung v. 27.01.1977, BGBl. I Nr. 7 S. 201 ff.

[19] Pointiert: *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, S. 153 (159: „Datenverarbeitung durch Private wird umstandslos einem staatlichen Grundrechtseingriff gleichgestellt und einem umfassenden Rechtfertigungsgebot unterworfen […]. Strukturell ist das nichts anderes als eine ins Horizontalverhältnis gekippte, unmittelbare Grundrechtsbindung Privater").

Kurzum: Bislang ist es weder dem europäischen noch dem – insoweit durch Unionsrecht gebundenen deutschen – Gesetzgeber gelungen, das Datenschutzrecht und das Schuldrecht zu synchronisieren. Auch das dem unternehmerisch handelnden Verantwortlichen gemäß § 327q Abs. 2 BGB eingeräumte, komplexe Kündigungsrecht für den Fall, dass ein als Verbraucher handelndes Datensubjekt die Datenverarbeitung für die Zukunft beendet, ist lediglich ein erster – deutscher – Versuch, diese Kollision abzumildern. Ein *Datenschuldrecht*,[20] das auch personenbezogene Daten als Leistungsgegenstand anerkennt und die ökonomische Realität rechtlich abbildet oder sogar gestaltet, lässt sich auf dieser Grundlage jedoch nicht entwickeln.

Es ist eine banale Erkenntnis, dass die Verarbeitung von personenbezogenen Daten ubiquitär ist. Sie ist zentral für Entwicklungen, die derzeit mit den schillernden Chiffren „Big Data"[21] und „künstliche Intelligenz" (KI)[22] umschrieben werden. Beiden Entwicklungen ist gemeinsam, dass sie die Verarbeitung von personenbezogenen Daten nicht voraussetzen, ihre Vorteile aber insbesondere durch eine Verarbeitung von Daten mit Personenbezug entfalten können.

Zwar sind anonymisierte Daten im Kontext von Big Data und KI nicht wertlos, solange ein abstrakter und damit wissenschaftlicher Erkenntnisgewinn angestrebt wird. Allerdings knüpfen auch der wissenschaftliche, jedenfalls aber der ökonomische Wert von Datenanalysen häufig an den Personenbezug als eine wesentliche semantische Ebene von maschinenlesbar codierter Information (kurz: personenbezogenes Datum) an.[23] Deshalb liegt der Fokus der Arbeit nicht auf der – primär technisch spannenden – Frage, wie eine Verarbeitung von personenbezogenen Daten durch Methoden der Anonymisierung effektiv vermieden oder das Risiko der Verarbeitung durch Pseudonymisierung (Art. 4 Nr. 5 DS-GVO) und Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) verringert werden kann. Vielmehr steht die Frage im Zentrum, inwieweit die Auslegung und Anwendung der DS-GVO eine rechtmäßige und rechtssichere Verarbeitung von personenbezogenen Daten im Privatrechtsverhältnis[24] ermöglicht, ohne dabei gegen das gemäß Art. 8 GRCh (Schutz personenbezogener Daten)

---

[20] Begriffsprägend *Schmidt-Kessel*, Daten als Gegenleistung in Verträgen über die Bereitstellung digitaler Inhalte, BMJV, 03.05.2016, https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 19.05.2022.

[21] Aus rechtlicher Perspektive: *Leistner/Antoine/Sagstetter*, Big Data, 2021.

[22] Mit technischer Einführung: *Zech*, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, Gutachten für den 73. Deutschen Juristentag, 2020.

[23] Zum Informationsbegriff: *Wiebe*, in: Fiedler/Ullrich (Hrsg.), Information als Wirtschaftsgut, 1997, S. 93 (99 ff.); *Zech*, Information als Schutzgegenstand, 2012, S. 14 ff./114. f./441.

[24] Die Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen (Art. 88 DS-GVO i. V. m. § 26 BDSG) weist Besonderheiten auf und bleibt unberücksichtigt: Hierzu: m. w. N.: *Neighbour*, in: Sassenberg/Faber (Hrsg.), Industrie 4.0 und IoT, 2020, S. 277 ff.; *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, 2019.

und gemäß Art. 7 GRCh (Privatsphäre) zu gewährleistende Untermaßverbot zu verstoßen.

Notwendig ist eine privatrechtssensible Auslegung deshalb, weil zunehmend deutlich wird, dass der europäische Gesetzgeber bei Verabschiedung der DS-GVO die rechtliche und ökonomische Realität in den Mitgliedstaaten nur unzureichend erfasst hat. Die DS-GVO nimmt zu wenig Rücksicht auf die tatsächliche Verwertung der vermögenswerten Bestandteile von Persönlichkeitsrechten, die wiederum eine Verarbeitung von personenbezogenen Daten voraussetzt.[25]

Die Notwendigkeit, bei dieser privatrechtssensiblen Auslegung und Anwendung der DS-GVO auf die Unionsgrundrechte zurückzugreifen, ist der Vielzahl der unbestimmten Rechtsbegriffe in der DS-GVO geschuldet. Diese erschweren die gerichtliche und behördliche Rechtsanwendung derzeit fundamental. Infolgedessen ist es auch für die Wissenschaft eine zentrale Herausforderung *de lege lata* und – soweit dies nicht mehr möglich ist – auch *de lege ferenda* Vorschläge für die Ausgestaltung eines Datenschuldrechts zu unterbreiten, das die informationelle Privatautonomie der Datensubjekte stärkt, dabei aber die multipolaren Grundrechtskonstellationen hinreichend berücksichtigt.[26]

Das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände zur Gewährleistung einer abgestützten informationellen Privatautonomie stellt bereits begrifflich die Privatautonomie und insbesondere die Vertragsfreiheit als ihre wichtigste Ausprägung in den Mittelpunkt. Dabei weicht der Begriff der informationellen Privatautonomie von dem bekannten Begriff der informationellen Selbstbestimmung ab. Letztere ist bereits seit dem *Volkszählungsurteil* des *BVerfG*[27] bekannt.

Diese begriffliche Unterscheidung ist jedoch kein bloßes Glasperlenspiel. Im Gegenteil: Die Gewährleistung einer abgestützten informationellen Privatautonomie ist Ausdruck eines Perspektivenwechsels und dient dazu, Grundannahmen des geltenden Datenschutzrechts kritisch zu hinterfragen, soweit personenbezogene Daten als Gegenstand eines vertraglichen Synallagmas vereinbart werden.

Im Zentrum des hier vorgeschlagenen Stufenmodells der Erlaubnistatbestände für das Privatrechtsverhältnis steht die datenschutzrechtliche Einwilligung, die ihrerseits in zwei Stufen ausdifferenziert wird. Infolgedessen ist dieses Stufenmodell in der Lage, eine Synthese aus dem datenschutzrechtlichen Verbot und der schuldrechtlichen Erlaubnis herzustellen und dadurch einem künftiges

---

[25] Zuletzt mit dieser Kritik, jedoch aus Perspektive einer Stärkung von Verbraucherrechten: *Wendehorst*, JZ 2021, 974 (984: „die DSGVO [ist] überhaupt nicht auf den Schutz vermögensrechtlicher Verbraucherinteressen […] zugeschnitten“).

[26] Mit dieser Forderung an die Privatrechtswissenschaft: *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 372.

[27] BVerfGE 65, 1 (43) = NJW 1984, 419 ff. – *Volkszählung*.

Datenschuldrecht den Boden zu bereiten. Dadurch gewährleistet das nachfolgend vorgeschlagene Stufenmodell der Erlaubnistatbestände die unionsgrundrechtlich verankerte abgestützte informationelle Privatautonomie und ermöglicht die Umsetzung von drei wesentlichen Zielen, ohne dabei den Schutz der Datensubjekte wesentlich zu beeinträchtigen:

Erstens wird die bisherige Kommerzialisierung der vermögenswerten Bestandteile von Persönlichkeitsrechten (wieder) ermöglicht, soweit diese auf eine Verarbeitung von personenbezogenen Daten angewiesen ist.

Zweitens werden personenbezogene Daten – wie von der *EU-Kommission* immer wieder und zuletzt im Kontext des Data Act gefordert – für Innovation und Wachstum im Binnenmarkt nutzbar gemacht, ohne dabei über die Präferenzen der Datensubjekte hinwegzugehen.

Drittens hilft dieses Stufenmodell und insbesondere die kartellrechtsakzessorische und damit asymmetrische Auslegung und Anwendung des Einwilligungstatbestands dabei, die durch die DS-GVO entstandenen Marktzutrittsbarrieren für KMU zu senken.

II. Forschungsstand

Spätestens seit Anfang der 1970er Jahre fordert der technische Fortschritt im Bereich der automatischen Datenverarbeitung den Schutz des Individuums vor einer Verarbeitung personenbezogener Daten immer wieder heraus.[28] Nach einer frühen kritischen Auseinandersetzung mit den ersten deutschen Gesetzen zum Schutz von natürlichen Personen vor einer Verarbeitung von personenbezogenen Daten[29] stagnierte das Interesse, das Privatrechtswissenschaftler dem Datenschutzrecht entgegenbrachten.[30] Das Feld wurde weitgehend dem Verwaltungs- und insbesondere dem Verfassungsrecht überlassen.[31]

---

[28] Hierzu frühzeitig: *Kilian*, Personalinformationssysteme in deutschen Großunternehmen, 1967; *ders.*, Juristische Entscheidung und Elektronische Datenverarbeitung, 1974; *Steinmüller/Lutterbeck/Malmann/Harbort/Kolb/Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826; *Steinmüller*, EDV und Recht: Einführung in die Rechtsinformatik und das Recht der Informationsverarbeitung, Juristische Arbeitsblätter 1970; *ders.* (Hrsg.), Informationsrecht und Informationspolitik, 1976.

[29] Kapitel 1 A.II.

[30] Zu den wenigen Ausnahmen zählen: *Ebnet*, Der Informationsvertrag, 1995; *A. Wagner*, Binäre Information als Gegenstand des Rechtsverkehrs, 1999; *Kilian*, CR 2002, 921 ff.; *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006; *Unseld*, Die Kommerzialisierung personenbezogener Daten, 2010; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012; *Sandfuchs*, Privatheit wider Willen?, 2015. Zudem ist *Spiros Simitis*, der erste Hessische Datenschutzbeauftragte und Herausgeber des langjährigen Standardkommentars zum BDSG, von Hause aus Privatrechtwissenschaftler.

[31] Hierzu: *Sattler*, in: Bakhoum u. a. (Hrsg.), 2018, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 2018, S. 27 ff.

Obwohl einige wissenschaftliche Beiträge einen vermittelnden Ansatz wählen,[32] leidet die rechtswissenschaftliche Auseinandersetzung weiterhin unter einem – auch institutionell durch die zahlreichen Datenschutzbehörden begünstigten – Übergewicht der öffentlich-rechtlichen Perspektive. Dennoch hat die privatrechtlich ausgerichtete Forschung gerade in den letzten Jahren wegweisende Untersuchungen hervorgebracht.

Besonders hervorzuheben sind die Arbeiten von *Benedikt Buchner*,[33] *Louisa Specht-Riemenschneider*,[34] *Carmen Langhanke*,[35] *Philipp Hacker*[36] *und Jan Niklas Bunnenberg*.[37] Die nachfolgende Analyse profitiert von dieser Forschung und baut hierauf teilweise auf. Dennoch unterscheidet sich das hier vorgeschlagene Stufenmodell der Erlaubnistatbestände und die dadurch gewährleistete abgestützte informationelle Privatautonomie in mehreren wesentlichen Punkten vom bisherigen Forschungsstand.

Der Untersuchungsgegenstand der Arbeiten von *Benedikt Buchner*, *Louisa Specht-Riemenschneider* und *Carmen Langhanke* war das alte BDSG, so dass mit der Anwendbarkeit der DS-GVO – trotz deren weitreichender Kontinuität zur Datenschutz-RL von 1995 – eine Neubewertung erforderlich ist. Zudem gehen alle vorgenannten Autorinnen und Autoren – mit Ausnahme von *Benedikt Buchner* – von einer jederzeitigen und grundlosen Widerruflichkeit der datenschutzrechtlichen Einwilligung aus. Infolgedessen dominiert das Datenschutzrecht das Schuldrecht in einer Weise, die – zumindest im B2B-Verhältnis – nach hier vertretener Ansicht nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar ist. *Benedikt Buchner* wiederum spart das Verhältnis zwischen Datenschutzrecht und AGB-Recht weitgehend aus.[38]

Weil alle bisherigen Arbeiten von einer Dominanz des Datenschutzrechts gegenüber dem Schuldrecht ausgehen,[39] bleibt – jedenfalls nach hier vertretener Auffassung – nicht viel vom Grundsatz der Privatautonomie, einschließlich der Möglichkeit zur Selbstbindung, übrig.

---

[32] *Masing*, NJW 2012, 2305 ff.; *Kingreen/Kühling*, JZ 2015, 213 ff.; *von Lewinski*, Die Matrix des Datenschutzrechts, 2014.

[33] Die informationelle Selbstbestimmung im Privatrecht, 2006.

[34] *Specht*, Die Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012.

[35] Daten als Leistung, 2018.

[36] Datenprivatrecht, 2020.

[37] Privates Datenschutzrecht, 2020.

[38] Das ist im Ergebnis wenig schädlich, weil infolge der seit 2018 vorrangig anzuwenden Grundsätze aus Art. 5 Abs. 1 DS-GVO der AGB-Kontrolle lediglich geringe Bedeutung zukommt. Hierzu: Kapitel 3 C.I.3.; a. A. *Hacker*, Datenprivatrecht, 2020, 417 ff. (430 ff.), sowie *Wendehorst*, JZ 2021, 974 (983 f.).

[39] Für eine stärkere Berücksichtigung schuldrechtlicher Grundsätze: *Metzger*, JIPITEC 2017, 2 (6 f.); *ders.*, AcP 216 (2016), 817 (833); *ders.*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, S. 25 (36 ff.).

Jan Niklas Bunnenberg will der Bindungswirkung einer Erklärung von Datensubjekten nur dann gemäß Art. 6 Abs. 1 lit. b DS-GVO (sog. vertragsakzessorische Datenverarbeitung) einen Vorrang vor dem Widerrufsinteresse des Datensubjekts einräumen, wenn das Interesse des Verantwortlichen infolge einer Abwägung im Einzelfall ausnahmsweise überwiegt.[40] Dieser Ansatz überzeugt systematisch nicht, weil er die beiden Erlaubnistatbestände gemäß Art. 6 Abs. 1 lit. b DS-GVO (vertragsakzessorische Datenverarbeitung) und gemäß Art. 6 Abs. 1 lit. f DS-GVO (Datenverarbeitung infolge einer Interessenabwägung) im Ergebnis vermengt und stets auf eine *ex post*-Interessenabwägung im Einzelfall angewiesen ist.[41]

Philipp Hacker ordnet die frei widerrufliche Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) als schuldrechtliche Bedingung für die Leistungserbringung durch den Verantwortlichen ein.[42] Infolgedessen verschmelzen Software und Recht potenziell zu dem von *Lawrence Lessig* konstatierten „Code is Law".[43] Allerdings soll es dem Verantwortlichen im Fall eines allzu „opportunistischen Widerrufs" der Einwilligung durch das Datensubjekt ausnahmsweise möglich sein, die Datenverarbeitung auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO fortzusetzen.[44] Sofern personenbezogene Daten vertraglich als Leistungsgegenstand vereinbart werden, soll deren Verarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig sein, soweit dieses Synallagma einer gerichtlichen Angemessenheitskontrolle standhält.[45]

Obwohl sich die von *Hacker* und in dieser Arbeit bearbeitete Thematik teilweise überschneidet, wird nachfolgend eine andere Lösung vorgeschlagen. Die Skepsis gegenüber einer gerichtlichen Angemessenheitsprüfung des vertraglichen Synallagmas mündet in den nachfolgend herausgearbeiteten Vorschlag einer abgestützten informationellen Privatautonomie, der im Unterschied zu

---

[40] *Bunnenberg*, Privates Datenschutzrecht, 2020, S. 264 f.

[41] Das Interesse des Datensubjekts am Widerruf der Einwilligung (Art. 6 Abs. 1 lit. a i. V. m. Art. 7 Abs. 3 S. 1 DS-GVO) wird mit einer Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO) kombiniert und soll anschließend die Fortsetzung der Datenverarbeitung auf Grundlage eines bindenden Vertrags gemäß Art. 6 Abs. 1 lit. b ermöglichen. Hierzu unten Kapitel 3 B.II.

[42] *Hacker*, ZfPW 2019, 148 (172 ff.); *ders.*, Datenprivatrecht, 2020, S. 228 f.; so auch *Rafał Mańko*, Contracts for the supply of digital content and digital services, Bericht des Wissenschaftlichen Dienstes des EU-Parlaments (EPRS) vom 27.11.2017, S. 8 („The report deletes the term *counter-performance*, criticized by the EDPS, and replaces it with the term *condition*"), verfügbar unter http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/614707/EPRS_BRI%282018%29614707_EN.pdf, zuletzt abgerufen am 19.05.2022; *EDSA*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, v. 04.05.2020, Nr. 37; ähnlich: *Riehm*, in: Pertot (Hrsg.), Rechte an Daten, 2020, S. 194 f. Hierzu: Kapitel 4 A.II.5.

[43] *Lessig*, Code is law, 1999.

[44] *Hacker*, Datenprivatrecht, 2020, S. 278. In diese Richtung auch bereits: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 272 ff.

[45] *Hacker*, Datenprivatrecht, 2020, S. 445 ff./473 ff. Zu den Bedenken an einer praktischen Umsetzung dieses Ansatzes: Kapitel 3 C.I.2.e. und C.I.3. Zu den Nachteilen für die unionsweit einheitliche Wirkung der DS-GVO: Kapitel 3 C.II.

Hacker und zu *Bunnenberg* auf einem Vorrang der Einwilligung vor den anderen datenschutzrechtlichen Erlaubnistatbeständen beruht. Statt über Art. 6 Abs. 1 lit. b DS-GVO (*Bunnenberg*) oder Art. 6 Abs. 1 lit. f DS-GVO (*Hacker*) eine Notlösung im Einzelfall zu suchen, wird den Beteiligten die Gestaltung ihrer Rechtsbeziehungen zunächst überlassen, das Datensubjekt dabei jedoch durch mehrere Instrumente abgestützt.

Insofern knüpft das nachfolgend herausgearbeitete Stufenmodell der Erlaubnistatbestände grundsätzlich an die von *Benedikt Buchner* betonte Bedeutung der datenschutzrechtlichen Einwilligung an. Im Unterschied zur Arbeit von *Benedikt Buchner* genügt es nach hier vertretener Auffassung jedoch, wenn neben der schlichten und jederzeit widerruflichen Einwilligung lediglich die schuldrechtliche Gestattung als zweite Stufe der Einwilligung anerkannt wird.[46] Zudem werden im fünften und sechsten Kapitel diejenigen Maßnahmen herausgearbeitet, die notwendig sind, um die informationelle Privatautonomie der Datensubjekte so abzustützen, dass sowohl der Schutz der Datensubjekte (Art. 1 Abs. 2 DS-GVO) gewährleistet als auch der freie Verkehr personenbezogener Daten im europäischen Binnenmarkt (Art. 1 Abs. 3 DS-GVO) ermöglicht wird.

Infolgedessen kann mit dem nachfolgend unterbreiteten Vorschlag das Desiderat einer „Ertüchtigung der Einwilligung“[47] erreicht und die „fehlende vertragsrechtliche Unterfütterung“[48] der DS-GVO nachträglich durch Auslegung kompensiert werden.

III. Gang der Untersuchung

Die Arbeit ist in sechs Kapitel gegliedert. Das *erste Kapitel* analysiert wesentliche Merkmale der Entstehungsgeschichte des Datenschutzrechts. Es dient nicht als disparate „Einleitungshistorie“, sondern offenbart, warum das Datenschutzrecht auf einen Kollisionskurs zum Schuldrecht geraten ist. Zudem wird deutlich, dass die DS-GVO einer unionsgrundrechtskonformen Auslegung bedarf, die nicht einseitig an Art. 8 Abs. 1 GRCh (Schutz personenbezogener Daten) und Art. 7 GRCh (Schutz der Privatsphäre) ausgerichtet werden darf, sondern ebenfalls die unternehmerische Freiheit der Verantwortlichen und der Datensubjekte (Art. 16 GRCh) und die allgemeine Vertragsfreiheit (Art. 6 Abs. 3 EUV) gewährleistet.

Dies ist erforderlich, damit die datenschutzrechtlichen Verarbeitungsverbote in Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO mit Blick auf die unternehmerische Freiheit (Art. 16 GRCh) und den allgemeinen Rechtsgrundsatz der Vertragsfrei-

---

[46] Kapitel 4 C.II.
[47] Mit dieser Forderung: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 403.
[48] *Staudenmayer*, ZEuP 2019, 663 (676).

heit (Art. 6 Abs. 3 EUV) nicht gegen das Übermaßverbot und damit gegen den Verhältnismäßigkeitsgrundsatz verstoßen (Art. 52 Abs. 1 S. 2 GRCh), sondern im Wege der praktischen Konkordanz in eine abgestützte informationelle Privatautonomie der Datensubjekte münden.

Anschließend werden die in der DS-GVO für das Privatrechtsverhältnis vorrangig vorgesehenen Erlaubnistatbestände daraufhin analysiert, inwieweit sie geeignet sind, die informationelle Privatautonomie der Datensubjekte zu verwirklichen, ohne das unionsgrundrechtlich gemäß Art. 8 Abs. 1 GRCh und Art. 7 GRCh zu gewährleistende Untermaß zu verletzen.

Im *zweiten Kapitel* wird die Möglichkeit zur rechtmäßigen Datenverarbeitung auf Grundlage einer Interessenabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO analysiert. Neben den Vorteilen dieser nur im Privatrechtsverhältnis anwendbaren Generalklausel werden deren Nachteile offenkundig. Paradoxerweise ist die Vorschrift einerseits potenziell zu weit geraten, soweit sie eine Direktwerbung, einschließlich Profiling, *de lege lata* privilegiert. Andererseits ist sie zu eng geraten, weil auch eine Verarbeitung besonders sensibler personenbezogener Daten – im Fall von Spontanäußerungen und für das Trainieren von sog. künstlicher Intelligenz – auf Grundlage einer Interessenabwägung *de lege ferenda* ermöglicht werden sollte.

Im *dritten Kapitel* wird die vertragsakzessorische Datenverarbeitung gemäß Art. 6 Abs. 1 lit. b DS-GVO untersucht. Obwohl dieser Erlaubnistatbestand auf den ersten Blick am besten für die Entwicklung eines Datenschuldrechts geeignet scheint, ist er nach hier vertretener Auffassung durch eine restriktive Auslegung auf die Funktion zu beschränken, den Tatbestand der Einwilligung und infolgedessen die Aufmerksamkeits- und Entscheidungskapazitäten der Datensubjekte zu entlasten.

Im *vierten Kapitel* wird herausgearbeitet, warum die Einwilligung am besten dafür geeignet ist, die informationelle Privatautonomie der Datensubjekte zu gewährleisten. Im Privatrechtsverhältnis ist der Einwilligung ein Vorrang vor den anderen Erlaubnistatbeständen einzuräumen.

Im *fünften Kapitel* münden die zuvor gefundenen Ergebnisse in ein Stufenmodell der Erlaubnistatbestände für das Privatrechtsverhältnis. Dieses Stufenmodell ermöglicht eine abgestützte informationelle Privatautonomie, setzt aber voraus, dass die sog. freie Widerruflichkeit der Einwilligung (Art. 7 Abs. 3 S. 1 DS-GVO) – im Grundsatz – dispositiv ist und die Anforderungen an die Freiwilligkeit der Einwilligung (Art. 7 Abs. 4 DS-GVO) flexibel als Berücksichtigungsgebot und nicht – wie derzeit zumeist vertreten – im Sinne eines strengen Kopplungsverbots angewendet wird. Soweit Datensubjekte als Unternehmer handeln, ist diese Flexibilisierung zwingend, um den Grundsatz der Verhältnismäßigkeit zu wahren. Indem diese Flexibilisierung des Einwilligungstatbestands zugleich in kartellrechtsakzessorischer und damit asymmetrischer Weise beschränkt wird, werden zwei Ziele verwirklicht.

Erstens wird die informationelle Privatautonomie der Datensubjekte gegenüber sog. *Gatekeeper*n bzw. Unternehmern mit überragender marktübergreifender Bedeutung für den Wettbewerb abgestützt. *Zweitens* wird vermieden, dass Art. 7 Abs. 3 S. 1 und Art. 7 Abs. 4 DS-GVO als Marktzutrittsbarrieren wirken und dadurch die Wettbewerbsposition von KMU insbesondere gegenüber *GAFAM* und (künftig) gegenüber *BAT* verschlechtern.

Im *sechsten Kapitel* werden zwei wesentliche Maßnahmen als Abstützungen der informationellen Privatautonomie vorgeschlagen. Weil die europäische Gesetzgebung auf das sog. Informationsmodell[49] und das dezentrale Instrument der Einwilligung setzt, ergibt sich hieraus eine Folgenverantwortung. Die informationelle Privatautonomie muss mittelfristig durch eine Kombination aus farblicher Kennzeichnung und *Privacy Score* und die Implementierung eines *Kontroll-Cockpits* zusätzlich „materialisiert" werden. Die Arbeit schließt mit einer Zusammenfassung in sechs Haupt- und insgesamt 30 (Unter-)Thesen.

[49] Hierzu instruktiv: *Grundmann*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 4. Aufl. 2021, S. 264 Rn. 41 ff.; umfassend: *Grigoleit*, Vorvertragliche Informationspflichten, 1997; *Fleischer*, Informationsasymmetrien im Vertragsrecht, 2001.

1. Kapitel

Grundrechtliche Gewährleistung von informationeller Privatautonomie

Der Begriff der *informationellen Privatautonomie* dürfte Experten für Verfassungsrecht irritieren. Aus der deutschen verfassungsgerichtlichen Perspektive ist das *Recht auf informationelle Selbstbestimmung* (RaiS) seit 1983 etabliert, so dass der Begriff der informationellen Privatautonomie ein fehlerhaftes Verständnis nahelegt. Bestätigt wird diese Einschätzung durch eine Suche in juristischen Datenbanken. Sie fördert eine Fehlanzeige zu Tage.[1] Dennoch lässt sich die hier vorgeschlagene Flexibilisierung und Privatrechtssensibilisierung der DS-GVO mit dem Begriff der informationellen Privatautonomie auf den Punkt bringen.

Die begriffliche Abgrenzung der informationellen Privatautonomie zur informationellen Selbstbestimmung[2] und den im Anschluss hieran vom *BVerfG* entwickelten IT-Grundrechten[3] ist bewusst gewählt. Diese Abweichung dient dazu, bereits sprachlich eine erkennbare Unterscheidung zum grundrechtlichen Schutz der informationellen Selbstbestimmung vorzunehmen.

Der Begriff hat einen weiteren Vorteil: Weder der europäische Gesetzgeber noch der *EuGH* kennen das Recht auf informationelle Selbstbestimmung.[4] Infolgedessen kann der Begriff und die Gewährleistung der informationellen Privatautonomie originär in der DS-GVO und den europäischen Grundrechten verortet werden.[5]

---

[1] Eine Suchanfrage mit dem Stichwort „informationelle Privatautonomie" in der Datenbank Beck-Online (Datum 28.08.2021) erzielt einen Treffer, der eine beiläufige Verwendung des Begriffs enthält: *Schantz*, NJW 2016, 1841 (1845).

[2] Begriffsprägend: *Steinmüller u.a.* Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, 84 (93: „Recht auf Selbstbestimmung über Individualinformation"); Zum Recht auf informationelle Selbstbestimmung: *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung?, 1987, S. 25; *di Fabio*, in: Maunz/Dürig, GG, 2001, Art. 2 Rn. 173 („interpretatorische Fortschreibung des Selbstdarstellungsschutzes aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG").

[3] Zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität (eigengenutzter) informationstechnischer Systeme: *Hoffmann-Riem*, JZ 2008, 1009 ff.

[4] Für eine Vermeidung des Begriffs, auch weil diesem eine für Art. 8 GRCh abzulehnende herrschaftsrechtliche Konzeption zugrunde liegt: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 105 ff.

[5] Allerdings ist zu beachten, dass eine grundrechtliche Gewährleistung von Privatautonomie als Ausdruck der allgemeinen Handlungsfreiheit und Vertragsfreiheit auf Ebene der Unionsgrundrechte unterentwickelt ist: *Herresthal*, ZEuP 2014, 238 (265: „Schwerwiegender Konstruktionsfehler der Grundrechtecharta").

Die vorgeschlagene begriffliche Unterscheidung zwischen dem deutschen Recht auf informationelle Selbstbestimmung und der unionsrechtlichen Gewährleistung der informationellen Privatautonomie ist nur auf den ersten Blick trivial oder ein bloßes Spiel mit Worten. Der Begriff ist nicht das privatrechtlich geprägte Pendant zum deutschen Recht auf informationelle Selbstbestimmung.[6] Vielmehr ist er Ausdruck eines Perspektivenwechsels[7] und Ausgangspunkt einer privatrechtlichen Betrachtung des weitgehend unionsrechtlich determinierten Datenschutzrechts.[8] Zugleich bildet die informationelle Privatautonomie den Nukleus eines Datenschuldrechts, dessen Leistungsgegenstand auch personenbezogene Daten sein können. Damit dient die informationelle Privatautonomie dazu, die fehlende „vertragsrechtliche Unterfütterung der DS-GVO"[9] nachträglich im Wege der Auslegung und Anwendung zu korrigieren.[10]

Obwohl die nachfolgend vorgeschlagene abgestützte informationelle Privatautonomie eine Analyse der DS-GVO aus privatrechtlicher Perspektive ermöglichen soll, ist es dennoch erforderlich, zunächst auf das deutsche Recht auf informationelle Selbstbestimmung und seine relevanten unionsrechtlichen Funktionsäquivalente einzugehen. Dadurch werden grundlegende Strukturen des Datenschutzrechts offengelegt, die bis heute prägend sind und die es erschweren, den monolithischen Block „DS-GVO" mit den Bedingungen der automatisierten und künftig autonomen Datenverarbeitung in einen sinnvollen Ausgleich zu bringen.[11]

---

[6] Hierzu bereits: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006, S. 76 f.

[7] Diesen Perspektivenwechsel ebenfalls fordernd: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 401 („Bei der Konzeption der DSGVO wurde vielfach, auf Jahrzehnte alte Grundsätze und Prinzipien zurückgegriffen, die für die heutige Praxis nur noch teilweise tragen.").

[8] Letztlich verbleiben im Kontext der Öffnungsklauseln der DS-GVO – insbesondere Art. 85 DS-GVO – um „Korridorlösungen, innerhalb derer die Mitgliedstaaten eigenständige Entscheidungen treffen können", wenngleich diese an die Konventionsrechte der EMRK gebunden sind: Hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 366.

[9] *Staudenmayer*, ZEuP 2019, 663 (676).

[10] Damit soll auch das Spannungsverhältnis aufgelöst werden, das sich bereits aus Sicht der unionsgrundrechtlichen Bewertung der DS-GVO ergibt. So scheut beispielweise *Nikolaus Marsch* mehrfach davor zurück, Vorschriften der DS-GVO als zu unbestimmt oder als Verstoß gegen die Verhältnismäßigkeit klar zu benennen. So mit Blick auf Art. 6 Abs. 1 lit. f DS-GVO: „einen nicht unerheblichen Eingriff in die Grundrechte des Datenverarbeiters dar. Ob dieser wenig zielgenaue Eingriff durch den bloßen Verweis auf die potenzielle Gefährlichkeit von Datenverarbeitungsmaßnahmen zu rechtfertigen ist, scheint mehr als fraglich" (*ders.*, Das Europäische Datenschutzgrundrecht, 2018, S. 264 f.); sowie zu den Ansprüchen des Datensubjekts auf Auskunft, Löschung und Berichtigung: „Nur als Ergebnis einer Interessenabwägung können sich gegen Private gerichtete Auskunfts- und Einwirkungsrechte somit als in bestimmten Konstellationen grundrechtlich geboten erweisen, nicht jedoch im Sinne einer dieser Abwägung vorausliegenden Rechtsposition" (S. 267). Allerdings räumt *Marsch* dem EU-Gesetzgeber auf Grundlage von Art. 8 Abs. 1 GRCh einen weiten „Korridor" zur Regulierung und Strukturierung privater Datenverarbeitungsmaßnahmen ein (S. 260/268).

[11] So mit Blick auf Art. 4 Nr. 1 DS-GVO: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 226 („Eine *beschränkende Auslegung* des Begriffs der personenbezogenen Daten fällt nach

Das Recht auf informationelle Selbstbestimmung wurde aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet und hat das deutsche Datenschutzrecht über Jahrzehnte geprägt. Der Blick auf die Entstehungsgeschichte des Datenschutzrechts verdeutlicht, dass für diesen Schutz von Menschen vor einer Verarbeitung personenbezogener Daten zu wenig zwischen der vertikalen und der horizontalen Bedeutung von Grundrechten differenziert wurde. Auch die DS-GVO und das BDSG basieren – wie die vorherigen deutschen Datenschutzgesetze und die europäische Datenschutz-RL (1995)[12] – primär auf einem abwehrrechtlichen Verständnis von Grundrechten (A).

Der europäische Gesetzgeber berücksichtigte kaum den in der deutschen Grundrechtslehre bekannten Unterschied zwischen einer Grundrechtsbindung staatlicher Stellen einerseits und den im Privatrechtsverhältnis lediglich bestehenden staatlichen Gewährleistungspflichten andererseits. In der Folge greift der unionsrechtliche Datenschutz in die unternehmerische Freiheit der Verantwortlichen und die persönliche Freiheits- und Verantwortungssphäre der Datensubjekte ein (B).

Ausdruck dieser potenziellen Gefährdung der informationellen Privatautonomie ist das einfachgesetzliche Verbot einer Verarbeitung von personenbezogenen Daten (C). Die hier vorgeschlagene abgestützte informationelle Privatautonomie ist mit den primärrechtlichen Vorgaben vereinbar und bietet einen Ansatzpunkt, um die DS-GVO (und künftig: ePrivacy-VO und Data Act) so auszulegen und weiterzuentwickeln, dass die individuelle Gestaltungsfreiheit durch einen Vorrang der Einwilligung gestärkt wird, ohne dabei das gemäß Art. 8 Abs. 1 GRCh (Art. 16 Abs. 1 AEUV) und Art. 7 GRCh grundrechtlich gebotene Untermaß zu unterschreiten (D).

A. Dominanz der abwehrrechtlichen Dimension der Grundrechte

Nicht nur den mit der grundrechtlichen Terminologie vertrauten Spezialisten des Verfassungsrechts dürfte der Begriff der informationellen Privatautonomie irritieren. Ähnlich irritiert dürften Spezialisten für das Immaterialgüterrecht und das Medienrecht – noch immer – sein, wenn sie erfahren, dass der europä-

dem derzeit geltenden Verständnis schwer. Diese schon auf der ersten Stufe des Anwendungsbereichs vollkommen ausgeuferte Reichweite datenschutzrechtlicher Regulierung ist *kritikwürdig*" [Hervorhebungen im Original.]. Mit Überlegungen für eine Reduktion der Anforderungen für KMU: Mitteilung der EU-Kommission, Datenschutz als Grundpfeiler der Teilhabe der Bürgerinnen und Bürger und des Ansatzes der EU für den digitalen Wandel – zwei Jahre Anwendung der Datenschutz-Grundverordnung, 24.06.2020 COM(2020) 264 S. 12/19 ff. (Evaluierung DS-GVO).

[12] Richtlinie 95/46/EG v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 v. 23.11.1995, S. 31 ff.

ische Gesetzgeber weite Teile des allgemeinen Persönlichkeitsrechts (APR) und des Rechts am eigenen Bild – abgesehen von äußerungsrechtlichen Konstellationen – in den Anwendungsbereich der DS-GVO und damit unter das Primat des Unionsrechts gebracht hat.[13] Lediglich im Bereich der Öffnungsklauseln, insbesondere gemäß Art. 85 Abs. 2 (sog. Medienprivileg) kann das *BVerfG* versuchen,[14] ein nationales äußerungsrechtliches Persönlichkeitsrecht neben der DS-GVO aufrecht zu erhalten.[15]

Im Immaterialgüterrecht wurde über mehrere Jahrhunderte diskutiert und gestritten, welche unkörperlichen Güter als Immaterialgüterrechte und welche als Persönlichkeitsrechte geschützt sind.[16] Es folgte eine jahrzehntelange Diskussion darüber, ob und inwieweit Persönlichkeitsrechte trotz ihrer unverbrüchlichen Verbindung zu einem Individuum als Vermögensrechte kommerzialisiert werden können.[17] Die Publikationen zu diesem Rechtsgebiet füllen Bibliotheken. Diese Arbeiten sind infolge der DS-GVO nicht obsolet. Allerdings

---

[13] Mit der frühzeitigen Warnung, dass die DS-GVO in wichtigen Bereichen wie der Internetkommunikation zur Unanwendbarkeit des Rechts auf informationelle Selbstbestimmung, der grundgesetzlichen Presse- und Meinungsfreiheit sowie des allgemeinen Persönlichkeitsrechts führen könnte: *Masing*, Ein Abschied von den Grundrechten, SZ v. 09.01.2012, S. 10; *Kühling*, Die Europäisierung des Datenschutzrechts, 2014, S. 12. Ob diese Konsequenz den an den Beratungen zur DS-GVO Beteiligten bewusst war, ist zweifelhaft. Die Anwendbarkeit von §§ 22, 23 KUG und von § 1004 BGB analog bzw. §§ 823 Abs. 1 jeweils i. V. m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG schrumpft erheblich zusammen. Für die nationalen Traditionen im Bereich des Persönlichkeitsrechts lässt die Öffnungsklausel gemäß Art. 85 Abs. 2 DS-GVO zugunsten von journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken einen kleinen Anwendungsbereich übrig. Unter Anwendung der Datenschutz-RL plädierte *Ohly* noch dafür, den Anwendungsbereich des Datenschutzrechts im Verhältnis zu den (sonstigen) Persönlichkeitsrechten einzuschränken: *ders.*, AfP 2011, 428 (438).

[14] *BVerfG*, Beschl. v. 06.11.2019, 1 BvR 16/13 = GRUR 2020, 74 (Rn. 39/74/91 f.) – *Recht auf Vergessen I.*

[15] Das Urteil des *BVerfG* ist insoweit nicht eindeutig. Während für eine Fortsetzung der deutschen Rechtsprechung zum äußerungsrechtlichen allgemeinen Persönlichkeitsrecht immerhin die Öffnungsklausel des Art. 85 Abs. 2 DS-GVO ins Feld geführt werden kann, scheint das *BVerfG* auch am allgemeinen Recht auf informationelle Selbstbestimmung festhalten zu wollen, Beschl. v. 06.11.2019, 1 BvR 16/13 = GRUR 2020, 74 (Rn. 83 ff.) – *Recht auf Vergessen I.* Tatsächlich kann das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG jedoch nur auf solche Sachverhalte angewendet werden, für die in der DS-GVO eine Öffnungsklausel besteht (beispielsweise im Arbeitsrecht oder für journalistische Zwecke). Im Anwendungsbereich der DS-GVO sind dagegen die europäischen Grundrechte der Beurteilungsmaßstab. Zur vorherigen Diskussion, wie sich das *BVerfG* wieder „ins Spiel bringen" könne: *Thym*, JZ 2015, 53 (61); *Bäcker*, EuR 2015, 389 (400 f.); *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 298 ff.

[16] Hierzu: *Dölemeyer/Klippel*, in: Beier u. a. (Hrsg.), FS 100 Jahre GRUR, 1991, 185 ff.

[17] *Hubmann*, Das Persönlichkeitsrecht, 2. Aufl., 1967; *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995; *Helle*, Besondere Persönlichkeitsrechte im Privatrecht, 1991, S. 37 ff.; sowie *Forkel,* in: ders./Kraft (Hrsg.), Beiträge zum Schutz der Persönlichkeit und ihrer schöpferischen Leistung, FS Hubmann, 1985, 93 (101 f.); Kritisch gegenüber einer zunehmenden Kommerzialisierung von Persönlichkeitsaspekten mittels translativer Übertragungen: *Schack*, JZ 2000, 1060 (1062); *Peifer*, Individualität im Zivilrecht, 2001, S. 291 ff.

haben Wissenschaft und Praxis die Persönlichkeitsrechte bislang weitgehend parallel zum Datenschutzrecht behandelt. Bisher war das Verhältnis zwischen Persönlichkeitsrechten und Datenschutzrecht – jedenfalls in Deutschland – durch freundliches Desinteresse geprägt.[18]

Spätestens seit dem 25.05.2018 kreuzen sich jedoch die Pfade des (nationalen) Persönlichkeitsrechts und des europäischen Datenschutzrechts. Umso verblüffender ist es, dass die Bedeutung der Persönlichkeitsrechte für das Datenschutzrecht während den Verhandlungen zur DS-GVO keine wesentliche Rolle spielten. Grund dafür könnte sein, dass das Datenschutzrecht die privatrechtliche Forschung kaum interessierte,[19] weil der Schutz von personenbezogenen Daten als Domain des Verfassungs- und (Wirtschafts-)Verwaltungsrechts wahrgenommen wurde, die mit persönlichkeitsrechtlichen Fragestellungen nur am Rande in Zusammenhang zu stehen schien.[20] Diese fehlende Synchronisierung von Persönlichkeitsrechten und Datenschutzrecht beruht auf einer jahrzehntealten Tradition und der weiten Auslegung der verfassungsrechtlichen Urteile durch den Gesetzgeber.

Seit dem *Volkszählungsurteil* des *BVerfG* von 1983 wird das deutsche Datenschutzrecht unmittelbar durch die Grundrechte geprägt (I). Zwar bemühten sich einige Privatrechtswissenschaftler im Anschluss an das Urteil darum, die unterschiedlichen Funktionen von Grundrechten als Abwehrrechte gegen staatliche Maßnahmen und als staatliche Gewährleistungspflichten im Privatrecht zu verdeutlichen. Dieser Versuch blieb aber weitgehend erfolglos (II).

I. Das RaiS als Grundlage des deutschen Datenschutzrechts

Diese Untersuchung leistet keine vollständige ideengeschichtliche Analyse von Privatheit als Ursprung des Datenschutzrechts. Inwieweit das Bedürfnis von Privatheit als soziologisches Massenphänomen eine Folge der Industrialisie-

---

[18] *Engert*, in: Grundmann/Möslein (Hrsg.), Innovation und Vertragsrecht, 2020, 153 (159). Als Ausnahme: *Ohly*, AfP 2011, 428 (438); sowie die Problematik andeutend: *Spindler*, GRUR-Beilage 2014, 101: „Auch wenn Datenschutz und (zivilrechtlicher) Schutz des Persönlichkeitsrechts im Grunde denselben verfassungsrechtlichen Wurzeln entspringen und zahlreiche Berührungspunkte aufweisen, beschränkt sich der nachfolgende Beitrag auf einige offene Fragen des Datenschutzes […] nur am Rande kann das Verhältnis zum zivilrechtlichen Persönlichkeitsschutz beleuchtet werden".

[19] Wichtige Ausnahmen: *Buchner*, Die informationelle Selbstbestimmung im Privatrecht, 2006; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012.

[20] *BVerfG*, Beschl. v. 14.02.1973, 1 BvR 112/65, NJW 1973, 1221 – *Soraya*; *BVerfG*, Urt. v. 13.02.2007, 1 BvR 421/05, NJW 2007, 753 – *Heimlicher Vaterschaftstest*; *BVerfG*, Beschl. v. 13.06.2007, 1 BvR 1783/05B, NJW 2008, 39 – *Esra*; *BVerfG*, Beschl. v. 08.12.2011, 1 BvR 927/08, NJW 2012, 756 – *Caroline von Hannover*; zuletzt: *BVerfG*, Beschl. v. 28.01.2019, 1 BvR 1738/16, NJW 2019, 1277 – *Kunstfreiheit*.

rung und der hiermit einhergehenden Urbanisierung ist, bleibt eine spannende Forschungsfrage.[21]

Für den Gegenstand dieser Untersuchung genügt es, vier wesentliche Einflussfaktoren herauszustellen, welche die Entstehung des deutschen Datenschutzrechts geprägt haben.[22] Diese *plausibilisieren*, warum dem Recht auf informationelle Selbstbestimmung (RaiS) sowohl im vertikalen Verhältnis zwischen Datensubjekt und Staat als auch im horizontalen Verhältnis zwischen Privatrechtsubjekten eine nahezu unterschiedslose Geltung zuerkannt wurde. Die wesentlichen Faktoren sind die Veränderung der Lebensverhältnisse infolge der Industrialisierung (1), der für die ersten Datenschutzgesetze prägende Einfluss der (Rechts-)Soziologie (2), die Erfahrungen in der nationalsozialistischen Diktatur (3) und die anschließende extensive Auslegung der Rechtsprechung des *BVerfG* durch den deutschen Gesetzgeber (4).

1. Industrialisierung und technischer Fortschritt

Als ganz wesentlicher Faktor verstärkte die Industrialisierung die Änderung der Lebensverhältnisse und begründete Forderungen nach einem rechtlichen Schutz von Privatheit.[23] Obwohl Privatheit keine Innovation des 18. und 19. Jahrhunderts ist, waren die Entstehung großer Städte und die Entwicklung eines städtischen Bürgertums Voraussetzungen für den modernen Individualismus.[24] Dem städtischen Bürgertum standen zunächst keine Instrumente zur Verfügung, um auf die wachsende Anzahl und die Reichweite der Berichterstattung zu reagieren, die aus der Gewährleistung von Presse- und Meinungsfreiheit und den technischen Entwicklungen von Medien, insbesondere zur Reproduktion von Text und Bild resultierten.[25]

Die Gerichte in den USA setzten dieser Entwicklung die Anerkennung eines *right to privacy* entgegen[26] und differenzierten es im Laufe der Zeit als *intru-*

---

[21] Hierzu im Verhältnis zwischen Bürger und Staat: *Nissenbaum*, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119 (2004). Zum Verhältnis zwischen Privatrechtsubjekten: *Posner*, 72 The American Economic Review, 405 ff.; grundlegend: *Warren/Brandeis* Harv. L. Rev. 1890, 193.

[22] Ausführlicher zur Entstehung des Datenschutzrechts: m. w. N. *Sattler*, in: Bakhoum u. a. (Hrsg.), 2018, Personal Data in Competition, Consumer Protection and Intellectual Property Law, 2018, 27 ff.

[23] *Shils*, 31 Law and Contemporary Problems (1966), 292, verfügbar unter: http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3109&context=lcp, zuletzt abgerufen am 19.05.2022.

[24] *Mallmann*, Zielfunktionen des Datenschutzes, 1977, S. 16 ff., 32; *Posner*, AEI Journal on Government and Society, 1978, 19 (20); *Shils*, 31 Law and Contemporary Problems, 1966, 292 ff. ("golden age of privacy"); *Westin*, 25 Washington and Lee Law Review 166, 1967, 22 ff.

[25] *Götting*, in: ders./Schertz/Seitz (Hrsg.), HdB Persönlichkeitsrecht, 2. Aufl. 2019, Teil 2, Rn. 1 ff. und 16.

[26] *Warren/Brandeis*, Harv. L. Rev. 1890, 193; rechtsvergleichende Übersicht bei: *Götting*, ebda, Teil 10. Allerdings hatte auch US-Amerikanische Gerichte immer wieder Schwierigkei-

sion, *public disclosure*, *false light* und *appropriation* weiter aus.[27] Das Reichsgericht zog zunächst noch das Hausrecht und das „natürliche Rechtsgefühl" heran,[28] um die Verwertung von Fotografien des toten *Otto von Bismarck* zu untersagen. Erst 1907 reagierte der deutsche Gesetzgeber mit der Einführung des Rechts am eigenen Bild in §§ 22 ff. KUG. Es war eine – im Vergleich zu den USA – späte rechtliche Antwort auf den reproduktionstechnischen Fortschritt, beispielweise die immer kompakteren und günstigeren Fotoapparate[29] und die infolgedessen veränderten Rahmenbedingungen für einen Schutz von Privatsphäre.

Auf Grundlage von zivilrechtlichen Generalklauseln, einer weiten Auslegung von § 22 KUG und mithilfe des Urheberrechts gelang es allmählich, den Schutz der Persönlichkeit auszubauen.[30] Ab 1954 setzte der *BGH* mit seiner *Leserbrief*-Entscheidung[31] diese Entwicklung fort und erweiterte den Schutz von Persönlichkeitsrechten kontinuierlich.[32] Erst infolge der flächenmäßigen Einführung von Computern in die Verwaltung entschied sich das Land Hessen im Jahr 1970 für die Verabschiedung eines ersten Datenschutzgesetzes.[33]

2. Prägender Einfluss der (Rechts-)Soziologie

Das Datenschutzrecht wurde als besonderer Bereich des Persönlichkeitsrechts wesentlich durch rollensoziologische Erkenntnisse geprägt.[34] *Niklas Luhmann* wird für das Jahr 1970 eine – aus heutiger Sicht – eklatante Fehleinschätzung anekdotisch zugeschrieben:

„Recht und Datenverarbeitung haben miteinander genauso viel zu tun wie Autos und Rehe: Meist gar nichts, nur manchmal stoßen sie zusammen".[35]

---

ten damit, neue Technologien in das bestehende Rechtssystem einzuordnen. Hierzu: *Richards/Smart*, in: Calo/Froomkin/Kerr (Hrsg.), Robot Law, 2016, 3 (13 ff.).

[27] *Prosser,* 48 Cal. L. Rev. 1960, 383 (389 ff.); *McCarthy*, The rights to Publicity and Privacy, 2008, § 1:19–24.

[28] *RG*, Urt. v. 28.12.1899 – VI 259/99, RGZ 45, 170 (173). Mit Kritik am Urteil: *Kohler* GRUR 1900, 208 ff.

[29] Zur Geschichte des Rechts am eigenen Bild: *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 12 ff.

[30] RGZ 69, 401 (403) – *Nietzsche-Briefe*; Grundlegende Analyse bei: *Hubmann*, Das Persönlichkeitsrecht, 2. Aufl. 1967.

[31] BGHZ 13, 334 = NJW 1954, 1404 – *Leserbrief*; *BGH*, I ZR 266/52 = GRUR 1955, 201, *Cosima Wagner Tagebücher.*

[32] *BGH*, GRUR 1956, 427 – *Paul Dahlke*; BGHZ 26, 349 = *BGH*, NJW 1958, 827 – *Herrenreiter*; *BGH*, GRUR 1965, 254 – *Soraya*; Überblick bei: *Götting*, in: ders./Schertz/Seitz (Hrsg.), Handbuch der Persönlichkeitsrechte, (2008), Teil 2, Rn. 15 ff.

[33] Hess. GVBl. II 1970, 300-10. Zur Begründung: *Osswald* (Hessicher Ministerpräsident), Der Spiegel (Heft 20/1971), S. 88.

[34] Hierzu bereits ein Überblick: *Sattler*, in: Ochs/Friedewald/Hess/Lamla (Hrsg.), Die Zukunft der Datenökonomie, 2019, S. 213 (222 ff.).

[35] Zurückgehend auf einen Vortrag von *Herbert Fiedler*, zitiert nach *Konzelmann*, JurPC

Diese Annahme hat sich in mehrfacher Hinsicht umgekehrt. Während die Wahrscheinlichkeit eines Zusammenstoßes von Kfz und Reh infolge der Fortschritte im Bereich des automatisierten Fahrens und damit aufgrund von automatischer Datenverarbeitung zurückgehen, ist die Kollision von Recht und Datenverarbeitung mittlerweile keine Ausnahme, sondern die Regel, insbesondere sofern personenbezogene Daten involviert sind. Mit Blick auf dieses Bonmot ist es paradox, dass gerade *Luhmanns* Forschung einen wesentlichen Anteil an der Zunahme der Kollisionen hatte.

Der Bericht „Grundfragen des Datenschutzes" von 1971, den mehrere Autoren um *Wilhelm Steinmüller* im Auftrag des Bundesministerium des Inneren ausgearbeitet hatten,[36] beruhte maßgeblich auf den soziologischen Forschungsarbeiten von *Niklas Luhmann* und *Jürgen Habermas*.[37] Dieser Bericht wiederum prägte nicht nur die Systematik des ersten BDSG von 1977, sondern beeinflusste unmittelbar die rechtwissenschaftliche Diskussion und – jedenfalls mittelbar – das *Volkszählungsurteil* des *BVerfG* von 1983.

Eine wesentliche Schlussfolgerung des Berichts von *Steinmüller u. a.* war die Einschätzung, dass die traditionelle Trennung zwischen öffentlicher und privater Sphäre nicht länger als regulatorischer Ausgangspunkt geeignet sei:

> „Der Dualismus Staat – Gesellschaft wird den Problemen unserer Zeit nicht mehr gerecht. Vielmehr sind beide Bereiche untrennbar zu einem Gemeinwesen verschmolzen. Sie bilden eine Wirkungseinheit".[38]

Folgt man dieser Annahme einer *faktischen* Verschmelzung, so ist es konsequent, auch einen einheitlichen *regulatorischen* Ansatz zu wählen, unabhängig davon, ob die Datenverarbeitung durch eine Behörde oder durch ein Unternehmen erfolgt.[39] Zwar schlossen sich *Steinmüller u. a.* der Theorie der unmittelbaren Drittwirkung der Grundrechte nicht an. In der Sache griffen sie aber stark auf die Ansätze von *Hans Carl Nipperdey* und *Walter Leisner* zurück[40] und

---

110/2003, Abs. 36. Eine ähnliche Fehleinschätzung wird *Thomas Watson* (IBM) zugeschrieben, der nach anekdotischer Überlieferung im Jahr 1943 den weltweiten Bedarf an Computern mit fünf Exemplaren beziffert haben soll: *Maney*, The Maverick and his machine, 2003, S. 355 f.; Sieg der Mikrosekunde, in: Der Spiegel, Nr. 22, 1965, S. 52 f.

[36] *Steinmüller/Lutterbeck/Malmann/Harbort/Kolb/Schneider*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, S. 84 ff.

[37] Der Bericht zitiert insbesondere: *Luhmann*, Grundrechte als Institution. Ein Beitrag zur politischen Soziologie, 1965; *ders.*, Recht und Automation in der öffentlichen Verwaltung, 1966; *Habermas*, Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft, 1962. Zur Kritik hieran, unten II.1.

[38] *Steinmüller u. a.*, Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, S. 35.

[39] So aktuell auch: *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), 2019, Art. 6 Rn. 2.

[40] In diesem Zusammenhang werden u. a. *Nipperdey* (Grundrechte und Privatrechte, ders. (Hrsg.), in: FS Molitor, 1962, 17 ff.), *Hesse* (Der Rechtsstaat im Verfassungssystem des Grund-

kamen infolgedessen zu einer sehr weitgehenden Anwendbarkeit von Verfassungsrecht im Privatrecht.[41]

Der Regierungsentwurf eines „Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung" von 1973 übernahm diesen nahezu einheitlichen, vorsorgenden Ansatz.[42] Immerhin unterschied das letztlich verabschiedete BDSG von 1977 noch ansatzweise zwischen der Datenverarbeitung durch öffentliche Stellen und – mit symptomatischer Wortwahl für diesen einseitig ausgerichteten Ansatz – der Datenverarbeitung durch „nichtöffentliche Stellen",[43] also durch (juristische) Personen des Privatrechts.

3. Prägung durch Erfahrungen der nationalsozialistischen Diktatur

Dass (West-)Deutschland ein Vorreiter im Bereich des Datenschutzrechts war,[44] ist nicht nur auf die Einführung erster Computer in der Verwaltung zurückzuführen.[45] Vielmehr wurde der einheitliche datenschutzrechtliche Regelungsansatz auch durch die Erfahrungen in der NS-Diktatur geprägt. Die seinerzeitige Auseinandersetzung mit der nationalsozialistischen Diktatur hatte grundlegenden Einfluss auf die Ausgestaltung des deutschen Datenschutzrechts. Dies wird am Bericht von *Steinmüller u. a.* deutlich. Darin erläutern die Autoren die Gefahren der Verarbeitung von personenbezogener Information anhand eines besonders wirkmächtigen – die historischen Bezüge gleichwohl noch verharmlosenden – Beispiels („*X ist Jude und auszuweisen*").[46]

Die Beispiele in der Studie – als weiteres Beispiel: „*Y ist Student und* [politisch] *links*" – sind im Kontext der historischen Erfahrung zulässig. Allerdings wähl-

---

gesetzes, in: Hesse u. a. (Hrsg.), FS Smend, 1962, 71 ff.), *Stein* (Lehrbuch des Staatsrechts, 1968) und *Leisner* (Grundrechte und Privatrecht, 1960) zitiert.

[41] So ausdrücklich *Walter Schmidt*: „Insofern ist das zwingende Privatrecht heute nichts anders als konkretisiertes Verfassungsrecht", *ders.*, JZ 1974, 241 (247).

[42] RegE BDSG, BT-Drs. 7/1027, S. 14: „Wir stehen zwar erst am Anfang dieser Entwicklung, dennoch ist der Gesetzgeber bereits jetzt aufgerufen, sie durch geeignete Maßnahmen so zu steuern, daß schwerwiegende und kaum reparable Schäden nicht erst eintreten und die Privatsphäre des einzelnen angesichts des technischen Fortschritts, den wir alle wünschen, unangetastet bleibt."

[43] Das Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (BDSG) vom 27.01.1977, BGBl. Teil I vom 01.02.1977, S. 201 ff. regelte im Abschnitt 2 die Datenverarbeitung durch Behörden und sonstige öffentliche Stellen. Die Abschnitte 3 und 4 regelten die Verarbeitung von personenbezogenen Daten durch „nicht-öffentliche Stellen", abhängig davon, ob die Verarbeitung zu eigenen Zwecken oder für fremde Zwecke erfolgte.

[44] *Simitis*, BDSG, 2014, Einleitung, Rn. 82. Zu den zeitgleichen Anfängen des Datenschutzes in den USA durch den Fair Credit Reporting Act (1970), 15 U.S.C. § 1681 und den Federal Privacy Act (1974), 5 U.S.C. § 552: *Buchner*, Die Informationelle Selbstbestimmung im Privatrecht, 2006, S. 6 ff.

[45] Der Hessische Ministerpräsident begründete das Hessische Datenschutzgesetz von 1970 (Hess. GVBl. II 1970, 300-10) mit der flächenmäßigen Einführung von Computern in die Verwaltung: *Osswald*, Der Spiegel (Heft 20/1971), S. 88.

[46] *Steinmüller* u. a. (Hrsg.), 1971, 55 ff., BT Drs. VI/3826.

ten die Autoren damit zugleich einen Ausgangspunkt, den man heute als ein, für ein wissenschaftliches Rechtsgutachten ungünstiges *Framing* beanstanden kann.

4. Extensive Auslegung der verfassungsgerichtlichen Urteile

Zuletzt wird rückblickend deutlich, dass das Urteil des *BVerfG* vom 15.12.1983[47] anschließend durch den Gesetzgeber sehr extensiv interpretiert wurde. Mit diesem Urteil hat das *BVerfG* das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung vom 25.03.1982[48] (Volkszählungsgesetz) für mit dem Grundgesetz unvereinbar erklärt. Bekanntlich leiteten die Verfassungsrichter in ihrem Urteil[49] ein Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht ab.[50] Nach Ansicht des *BVerfG* hatte sich das Gefährdungspotenzial für das Individuum aufgrund einer Verarbeitung von personenbezogenen Daten infolge des technischen Fortschritts erheblich verändert. Deshalb müsse die Entscheidung darüber, wer personenbezogene Daten erheben, verarbeiten und nutzen darf,[51] grundsätzlich bei der jeweiligen natürlichen Person liegen.[52] Um das Recht auf informationelle Selbstbestimmung gegen Beeinträchtigungen zu schützen, verpflichtete das *BVerfG* den Gesetzgeber, Verfahren zum Schutz der Datensubjekte („Betroffene") vorzusehen und zusätzlich organisatorische Schutzmaßnahmen einzuführen.[53]

Gegenstand der Verfassungsbeschwerden war die Eingriffsverwaltung gegenüber Bürgern auf Grundlage des Volkszählungsgesetzes.[54] Somit entschied das *BVerfG* nur

> „über die Tragweite dieses Rechts *für Eingriffe*, *durch* welche *der Staat* die Angaben personenbezogener Daten vom Bürger verlangt".[55]

Die Frage einer möglichen Drittwirkung im Privatrechtsverhältnis war nicht entscheidungserheblich und wurde auch nicht ausdrücklich angesprochen. Des-

---

[47] BVerfGE 65, 1 = NJW 1984, 419 – *Volkszählung*; bereits zuvor zu den Grenzen staatlicher Erhebung von personenbezogenen Daten als Schutz des engeren Lebensbereichs vor staatlicher Ausforschung: BVerfGE 27, 1 (7) – *Mikrozensus.*

[48] BGBl. I, S. 369.

[49] Laut *Hoffmann-Riem* die „Magna Charta" des Datenschutzrechts, *ders.*, AöR 123 (1998), 513 (515).

[50] Dabei handelt es sich nach Ansicht von *di Fabio* nicht um ein neues Grundrecht, sondern einen neuen Begriff, der die Selbstdarstellung als Bestandteil des Privatsphärenschutzes lediglich interpretatorische fortschreibt, *ders.*, in: Maunz/Dürig, GG, 2011, Art. 2 Rn. 173.

[51] Nach aktueller Terminologie gemäß Art. 4 Nr. 2 DS-GVO insgesamt: Verarbeitung.

[52] BVerfGE 65, 1 (43) – *Volkszählung.*

[53] Die vom *BVerfG* geforderten Maßnahmen umfassen die Pflicht, den Betroffenen zu informieren, die Art und Weise der Datenverarbeitung zu erläutern und die personenbezogenen Daten anschließend zu löschen: BVerfGE 65, 1 (48 ff.) – *Volkszählung.*

[54] Gesetz über eine Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung vom 25.03.1982 (BGBl. I S. 369).

[55] BVerfGE 65, 1 (44 f.) – *Volkszählung* [Hervorhebung durch den Verfasser].

halb lässt sich der Urteilsbegründung keine eindeutige Aussage entnehmen, ob und inwieweit das Recht auf informationelle Selbstbestimmung nach Ansicht des *BVerfG* auch Auswirkungen im Rechtsverhältnis zwischen Privatrechtsubjekten entfalten sollte.[56]

Allerdings enthielt das *Volkszählungsurteil* mehrere generalisierende Aussagen, die sich als umfassenden Regelungsauftrag interpretieren lassen. Bekannt und häufig zitiert ist die Aussage:

„[I]nsoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum mehr".[57]

Dieser Satz ließ sich aus Sicht der Legislative als Einladung dazu interpretieren, die Bedeutung des Rechts auf informationelle Selbstbestimmung auf den Bereich des Privatrechts auszudehnen.[58] Auch die Bezugnahme des Urteils auf die „soziale Umwelt",[59] bot einen Ansatzpunkt für ein derart weites Verständnis.[60]

Im Anschluss an das *Volkszählungsurteil* entwickelte das *BVerfG* das Recht auf informationelle Selbstbestimmung stetig fort, um die Bürger vor staatlichen Maßnahmen zu schützen, die in ihre Privatsphäre eingriffen.[61] Zudem leitete das *BVerfG* mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ein weiteres IT-Grundrecht[62] aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ab.[63] Überdies bestätigte das *BVerfG* diesen grundrechtlichen Abwehranspruch wiederholt gegen die Tendenz von Exe-

---

[56] Die Urteilsbegründung des BVerfG war hinsichtlich der Reichweite des Rechts auf informationelle Selbstbestimmung ambivalent BVerfGE 65, 1 = NJW 1984, 419 (422/Rn. 44 f.) – *Volkszählung*: „Die Verfassungsbeschwerden geben keinen Anlass zu erschöpfenden Erörterungen des Rechts auf informationelle Selbstbestimmung. Zu entscheiden ist nur über die Tragweite des Rechts für Eingriffe, durch welche der Staat die Angabe personenbezogener Daten vom Bürger verlangt." Diese salomonische Formulierung ließ unterschiedliche Interpretationen zu, je nachdem, ob man den ersten (nicht erschöpfend) oder den zweiten Satz („durch welche der Staat) betonte.

[57] BVerfGE 65, 1 (43) = NJW 1984, 419 (422) – *Volkszählung*.

[58] Hierfür plädierte: *Simitis*, NJW 1984, 398 (401).

[59] BVerfGE 65, 1 (42) = NJW 1984, 419 (422) – *Volkszählung*: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner *sozialen Umwelt* bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine *Gesellschaftsordnung* und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß". [Hervorhebungen durch den Verfasser].

[60] In diese Richtung weiterhin: *Brink*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, 30. Ed., Stand: 01.11.2017, Verfassungsrechtliche Grundlagen, Rn. 140; *Spiecker gen. Döhmann*, in: Vesting/Korioth (Hrsg.), Der Eigenwert des Verfassungsrechts, 2011, S. 263 (266).

[61] BVerfG 109, 279 = NJW 2004, 999 – *Lauschangriff*; BVerfGE 130, 151 = NJW 2012, 1419 – *Telekommunikationsdaten*; BVerfGE 133, 277 = NJW 2013, 1499 – *Antiterrordatei*.

[62] *Luch*, MMR 2011, 75 (78 f.)

[63] BVerfGE 120, 274 = NJW 2008, 822 – *Online Durchsuchung*; hierzu: *di Fabio*, NJW 2008, 424 ff.

kutive und Legislative, die Schranken der grundrechtlich gewährten Freiheiten im Interesse der Bekämpfung von Terrorismus und Straftaten auszudehnen.[64]

Retrospektiv fällt auf, dass das *BVerfG* den Begriff des *Rechts* auf informationelle Selbstbestimmung bis heute unverändert verwendet und dadurch sprachlich einen Unterschied zum deutlich jüngeren *Grundrecht* auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufrechterhält.[65] Bedeutender als die sprachliche Ambivalenz in den Urteilen des *BVerfG* ist jedoch der in der Folge des *Volkszählungsurteils* vom deutschen Gesetzgeber beibehaltene und – im Anschluss hieran – vom europäischen Gesetzgeber übernommene,[66] weitgehend einheitliche, grundrechtlich geprägte Ansatz zum Schutz personenbezogener Daten. Im Ergebnis beeinflussten die Entscheidungen des *BVerfG* auch den Datenschutz im Privatrecht direkt.

Die aus privatrechtlicher Perspektive frühzeitig geäußerte Warnung davor, aus den Grundrechten *unmittelbare* Folgen auch für das Privatrechtsverhältnis abzuleiten, verhallte ungehört.

II. Folgenlose Kritik am einheitlichen Schutzansatz

Im Ergebnis war das *Volkszählungsurteil* die Quintessenz einer langjährigen Diskussion in der (verfassungsrechtlichen) Wissenschaft. Es wurde deshalb von der Mehrheit der wissenschaftlichen „Vordenker" als Durchbruch gefeiert.[67] Dennoch wurde im Anschluss an das Urteil aus privatrechtlicher Perspektive eine stärkere Differenzierung zwischen staatlicher Eingriffsverwaltung und grundrechtlicher Gewährleistung in Form von Schutzpflichten im privatrechtlichen Bereich gefordert.

Die Kritik war grundlegend und knüpfte bereits an die maßgebliche Prägung des Berichts von *Steinmüller u. a.* durch die Arbeiten der Frankfurter Schule der Sozialwissenschaften an (1). Zudem wurde aus privatrechtlicher Perspektive die Umsetzung des Rechts auf informationelle Selbstbestimmung im Datenschutzrecht als überschießend kritisiert (2).

---

[64] Zur Unvereinbarkeit von Art. 2 Nr. 2 des sog. Gesetzes zur Vorratsdatenspeicherung (Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218 ff.) mit Art. 15 I der ePrivacy-RL (2002/58/EG): *EuGH*, C-203/15 und C-698/15. Im Anschluss hieran *OVG Münster*, Beschl. v. 22.06.2017, Az. 13 B 238/17. Zur einstweiligen Aussetzung der auf Art. 2 Nr. 2 Art. 2 Nr. 2 des sog. Gesetzes zur Vorratsdatenspeicherung beruhenden § 113b TKG geregelten Speicherverpflichtungen: Bundesnetzagentur, Mitteilung vom 28.06.2017.

[65] BVerfGE 120, 274 (Rn. 167 f./196/198 ff./309 f./314 ff.) = NJW 2008, 822 – *Online Durchsuchung*.

[66] Hierzu: *Marsch*, Das Europäische Datenschutzgrundrecht, 2018, S. 248 ff.

[67] *Steinmüller*, DuD 1984, 91 (92): „Manches liest sich wie ein Destillat aus 15 Jahren zunächst unbeachteter Vorarbeiten".

1. Kritik am rechtssoziologisch determinierten Zeitgeist

Insbesondere *Horst Ehmann* beanstandete, dass aus soziologischen Erkenntnissen unmittelbare rechtliche Konsequenzen gezogen wurden.[68] Nach seiner Ansicht hatten die Autoren um *Steinmüller* die Aussagen von *Luhmann* zudem missverstanden.[69] Aus *Luhmanns* Interaktionenlehre und Rollentheorie könnten eher Argumente gegen eine weite Auslegung des Rechts auf informationelle Selbstbestimmung und dessen Expansion ins Privatrecht abgeleitet werden.

Tatsächlich hatte *Luhmann* bereits mit Blick auf das Verwaltungsrecht selbst vor der Gefahr gewarnt, dass eine zu umfangreiche grundrechtliche Anerkennung der Entfaltungsmöglichkeiten von Individuen „die öffentlichen Interessen in die enger und enger geflochtenen Maschen des Verfassungsrechts treibt".[70] Danach münde eine zu umfassende „Verrechtlichung"[71] in die Sisyphusarbeit,

> „die von den Gipfeln der Grundrechte herabrollende Problematik aufzufangen und wieder nach oben zu wälzen, stets in Versuchung, schon auf halber Höhe ein Pathos anzuwenden, das nur Göttern ziemt".[72]

Die Kritik *Ehmanns* am Bericht von *Steinmüller u. a.* (1972) setzte sich in seiner Skepsis gegenüber dem *Volkszählungsurteil* fort, zumal die Vermutung nahelag, dass der Bericht nicht nur dem BDSG von 1977, sondern auch dem *Volkszählungsurteil* des *BVerfG* als Blaupause gedient hatte.[73]

Leider hielten es die Verfassungsrichter seinerzeit nicht für erforderlich, die rechtssoziologischen Ursprünge des Rechts auf informationelle Selbstbestimmung durch ein Zitat des Berichts von *Steinmüller u. a.* oder auch nur ihrer eigenen Vorarbeiten und die der anderen Verfahrensbeteiligten offenzulegen.[74] Insofern vermittelt bereits das *Volkszählungsurteil* teilweise den Eindruck, das Recht auf informationelle Selbstbestimmung sei – göttergleich – zur Erde gefallen.

---

[68] *Ehmann*, AcP 188 (1988), 230 (335).

[69] *Ehmann*, AcP 188 (1988), 230 (323/336 ff.).

[70] *Luhmann*, Grundrechte als Institution, 1965, S. 80.

[71] *Ehmann*, AcP 188 (1988), 230 (335). Ähnlich warnt *Hoffmann-Riem* im Zusammenhang mit dem Recht auf informationelle Selbstbestimmung davor, dass ohne eine „funktional-teleologische Interpretation" die „Verrechtlichung des Alltäglichen" droht, *ders.*, AöR 123 (1998), 513 (527 f.).

[72] *Luhmann*, Grundrechte als Institution, 1965, S. 59.

[73] Der vom BVerfG gewählte Begriff des Rechts auf informationelle Selbstbestimmung erinnert deutlich an das im Bericht vorgeschlagene „Recht auf Selbstbestimmung über Individualinformationen" bzw. „informationelle Selbstbestimmungsrecht" *Steinmüller u. a.* Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, 1971, BT Drs. VI/3826, 84 (93 und 139). Hierzu ausführlich: *Ehmann*, AcP 188 (1988), 230 (229 ff.).

[74] Hierzu ausführlich: *Ehmann*, AcP 188 (1988), 230 (330/Fn. 446).

2. Kritik an der überschießenden Umsetzung des RaiS

Die „Vordenker" des Rechts auf informationelle Selbstbestimmung waren zugleich die „Nachdenker" des *Volkszählungsurteils*. Sie interpretierten das Urteil extensiv und plädierten anlässlich der anschließenden Reformvorschläge dafür, die Anforderungen, die das *BVerfG* dem Gesetzgeber für staatliche Grundrechtseingriffe auferlegt hatte, auf den Bereich der Datenverarbeitung durch Private zu übertragen.[75]

Hiergegen wendeten sich mehrere Rechtswissenschaftler mit privatrechtlichem Hintergrund (insbesondere *Ehmann*, *Krause* und *Zöllner*). Ihrer Ansicht nach hatte das *BVerfG* das Recht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht für das Verhältnis zwischen Bürger und Staat und ausschließlich als Schranken-Schranke entwickelt, um dadurch den Gesetzgeber bei einer Konstitution von gesetzlichen Schranken des APR (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) – beispielweise durch das streitgegenständliche Volkszählungsgesetz – zu Normenklarheit zu zwingen.[76]

Eine unmittelbare Drittwirkung für das Privatrecht könne aus dem *Volkzählungsurteil* nicht abgeleitet werden. [77] Die Tendenz, einzelne Sätze aus dem Urteil auch zur Regulierung des privaten Informationsverkehrs unmittelbar anzuwenden, sei eine abzulehnende „Schmalspurjurisprudenz".[78] Anzuerkennen sei allenfalls eine mittelbare Drittwirkung im Rahmen der Auslegung von zivilrechtlichen Vorschriften, insbesondere der Generalklauseln zum Schutz des APR und innerhalb des BDSG. Eine solche mittelbare Drittwirkung sei

> „gar nicht zu vermeiden, sie findet kraft der Bewusstseinsänderungen, die das Volkszählungsurteil und die gesamte Datenschutzkampagne ausgelöst haben, nahezu unvermeidbar in allen juristischen Köpfen statt, die vom Pathos des [Rechts auf informationelle Selbstbestimmung] getroffen worden sind".[79]

Unverkennbar war das *Volkzählungsurteil* ein Kristallisationspunkt für unterschiedliche rechtspolitische und sogar ideologische Auffassungen darüber, welche Reichweite dem gesetzlichen Datenschutz künftig eingeräumt werden sollte. Diese Auseinandersetzung über die Reichweite des Schutzes ist damit zu-

---

[75] Vgl. Anhörungsverfahren zu den Entwürfen eines Gesetzes zur Änderung des BDSG, Kurzprotokoll des Innenausschusses des 10. Deutschen Bundestages, 110. Sitzung, BT-Drs. 10/1180, S. 125 (*Podlech*) und S. 104 (*Gallwas*: „jede Erhebung, jegliche Übermittlung, jegliche Nutzung von Daten [ist] zu einem Eingriff geworden").

[76] *Ehmann*, AcP 188 (1988), 230 (301 f.).

[77] *Ehmann*, AcP 188 (1988), 230 (303 ff.).

[78] *Zöllner*, RDV 1985, 3 (5).

[79] *Ehmann*, AcP 188 (1988), 230 (303). *Ehmann* unterschied zwischen dem Recht auf informationelle Selbstbestimmung (RaiS) und der erweiterten – und nach seiner Ansicht abzulehnenden – Interpretation als Grundrecht auf informationelle Selbstbestimmung (GRaiS).

gleich ein wichtiger Ausschnitt aus der umfangreichen, bis heute andauernden Diskussion über das Verhältnis zwischen Verfassungs- und Privatrecht.[80]

Wie tief die Gräben der Auseinandersetzung über die Ausgestaltung des Datenschutzrechts verliefen, verdeutlicht ein Vorwurf von *Horst Ehmann*. Er ist der Ansicht, dass die Drittwirkung des Rechts auf informationelle Selbstbestimmung den Befürwortern eines umfassenden Datenschutzrechts seinerzeit dazu diente, um

„die durch die starke Sozialbindung des Eigentums gebrochene Ideologie eines nur durch Klassenkampf zu überwindenden Interessengegensatzes zwischen Besitzenden und Nichtbesitzenden [zu] ersetzen durch den Interessengegensatz zwischen Wissenden und Unwissenden, zwischen Datenverarbeitern und davon Betroffenen, um daraus eine neue Rechtfertigung für die Fortführung des Klassenkampfes zur Herstellung einer klassen- und autoritätslosen Gesellschaft abzuleiten. […] Unter den Voraussetzungen dieser neuen Kampfziele ist eine vernünftige Interessenabwägung zwischen notwendigem Informationsschutz und erforderlicher Informationsfreiheit praktisch unmöglich".[81]

Ehmann wollte die „verfehlte These" begrenzen,[82] wonach jedes personenbezogene Datum an sich bereits schutzwürdig sei.[83] Nach seinem Verständnis hatte das *BVerfG* das Recht auf informationelle Selbstbestimmung auf die massenhafte automatisierte Verarbeitungen von Daten beschränkt.

Deshalb könne es nicht dazu dienen, auch die nicht automatisierte Datennutzung im Privatrechtsverkehr dem gleichen „Informationsverbot" zu unterwerfen.[84] Die verfassungsrechtliche Literatur habe insoweit einen über das Urteil hinausgehenden Prinzipienwechsel vollzogen, indem sie dem Recht auf informationelle Selbstbestimmung einen grundsätzlichen Vorrang vor den Grundrechten aus Art. 2, 5, 12 und 14 GG eingeräumt habe, obwohl letztere die Hand-

---

[80] Hierzu jeweils m.w.N.: *Schmidt-Rimpler*, AcP 147 (1941), 130ff.; *Nipperdey*, Grundrechte und Privatrecht, 1961; *M. Wolf*, Rechtsgeschäftliche Entscheidungsfreiheit und vertraglicher Interessenausgleich, 1970; *Raiser*, Die Zukunft des Privatrechts, 1971; *E.A. Kramer*, Die Krise des liberalen Vertragsdenkens, 1974; E. *v. Hippel*, Der Schutz des Schwächeren, 1982; *Hönn*, Kompensation gestörter Vertragsparität, 1982; *Canaris*, AcP 184 (1984), 201ff.; *Rittner*, AcP 188 (1988), 101ff.; *Hesse*, Verfassungsrecht und Privatrecht, 1988; *Dietlein*, Die Lehre von den grundrechtlichen Schutzpflichten, 1992; *Lerche*, in: Baur u.a. (Hrsg.), FS Steindorff, 1990, 897ff.; *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992; *Wiedemann*, JZ 1994, 411; *Hager*, JZ 1994, 373; *Zöllner*, AcP 196 (1996), 1; *Drexl*, Die wirtschaftliche Selbstbestimmung der Verbraucher, 1998; *Ruffert*, Vorrang der Verfassung und Eigenständigkeit des Privatrechts, 2011; sowie Teil 2, in: Möslein (Hrsg.), Private Macht, 2016; *Starke*; EU-Grundrechte und Vertragsrecht, 2016; *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 2014; *Hellgardt*, Regulierung und Privatrecht, 2016; *Lüttringhaus*, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, 2018. Für das 19. Jahrhundert: *Kaiser*, Zum Verhältnis von Vertragsfreiheit und Gesellschaftsordnung während des 19. Jahrhunderts, 1972.

[81] *Ehmann*, AcP 188 (1988), 230 (261/298f.).

[82] *Ehmann*, AcP 188 (1988), 230 (267).

[83] Dies findet aktuell in der Forderung einer restriktiven Auslegung der Anforderungen der DS-GVO Widerhall: *Leistner/Antoine/Sagstetter*, Big Data, 2021, S. 226/260.

[84] *Zöllner*, RDV 1985, 3 (15); *Krause*, JZ 1984, 656 (657); *Ehmann*, AcP 188 (1988), 230 (267).

lungs- und Informationsfreiheit der Bürger schützen. Dieser Prinzipienwechsel sei jedenfalls jenseits von einer automatischen Datenverarbeitung und für bloße Datenverwendungen nicht gerechtfertigt.[85] Während die Bindung einer Datenverarbeitung an den ursprünglichen Zweck im öffentlichen Bereich die bürgerliche Freiheit durch Einschränkung der Staatsmacht schütze, würden durch die Zweckbindung der Datennutzung im privaten Bereich mehr bürgerliche Freiheiten eingeschränkt als gewährleistet.[86] Insofern sei die Bindung der Datenverarbeitung an einen vorher bestimmten Zweck praktisch unbrauchbar und verfassungsrechtlich nicht zu rechtfertigen.[87]

3. Fazit: Fehlende privatrechtliche Unterfütterung des Datenschutzes

Rückblickend lässt sich denjenigen Privatrechtswissenschaftlern, welche die Konsequenzen des *Volkszählungsurteils* auf das Verfassungs- und Verwaltungsrecht beschränken oder allenfalls eine Schutzpflicht des Staates im Bereich der automatisierten Verarbeitung von Daten anerkennen wollten, vorwerfen, dass sie die Gefahren der Datenverarbeitung durch Private unterschätzt haben.

Zwar ist ihr Plädoyer konsequent, wonach die durch einen allwissenden und allmächtigen Staat drohenden Gefahren nicht mit denjenigen vergleichbar seien, die durch eine *nicht automatisierte* private Datensammlungen entstehen können. Auch die Verteidigung der Neugier[88] und des „Gebots der Lebensklugheit", möglichst viel über andere Menschen und deren Beziehungen zueinander wissen zu wollen,[89] sind im Grundsatz überzeugend.[90]

Allerdings gleicht diese Verteidigung der Privatautonomie für den Bereich der *nicht automatisierten* Datenverarbeitung aus heutiger Sicht einem Kampf gegen Windmühlen. Die Bereiche, in denen Daten nicht automatisiert verarbeitet werden, sind seitdem drastisch zurückgegangen. Insofern war die dem *Volkszählungsurteil* zugrunde gelegte tatsächliche Analyse der technischen Verarbeitungsmöglichkeiten zutreffend. Der seit Verkündung des *Volkszählungsurteils* eingetretene technische Fortschritt im Bereich der automatisierten Datenverarbeitung (sog. *ubiquitous computing*)[91] begünstigte den sich daran

---

[85] *Ehmann*, AcP 188 (1988), 230 (289).

[86] *Ehmann*, AcP 188 (1988), 230 (322).

[87] *Ehmann*, AcP 188 (1988), 230 (329); *Zöllner*, RDV 1985, 3 (13); *Krause*, Kurzprotokoll des Innenausschusses des 10. Deutschen Bundestages, 110. Sitzung, BT-Drs. 10/1180, S. 85. Zuletzt: *Giesen*, JZ 2007, 918 (927): „Der Gesetzgeber des BDSG hat die beiderseitigen Rechtspositionen der Datenverarbeiter und der Betroffenen unzureichend erkannt und ihren Konflikt in einer Schieflage zwischen Verstößen gegen das Übermaß- und das Untermaßverbot verfassungswidrig zu lösen versucht".

[88] *Ehmann*, AcP 188 (1988), 230 (287)

[89] *Ehmann*, AcP 188 (1988), 230 (326).

[90] Dies wieder aufgreifend: *Giesen*, JZ 2007, 817 (921).

[91] Hierzu *Roßnagel/Müller*, CR 2004, 625 ff.; *Kühling*, DV 40 (2007), 153 ff.

anschließenden, nahezu einheitlichen Ansatz des deutschen und im Anschluss hieran, unionsrechtlichen Datenschutzrechts.

Als Konsequenz der extensiven Interpretation des *Volkszählungsurteils* wurden die Anforderungen an eine rechtmäßige Datenverarbeitung zunehmend angeglichen, unabhängig davon, ob die Verarbeitung durch eine öffentliche oder eine „nicht-öffentliche Stelle" erfolgt. Die hieran aus privatrechtswissenschaftlicher Perspektive geäußerten Bedenken blieben folgenlos. Nach einer grundlegenden Kritik in den 1980er Jahren kehrten die Privatrechtswissenschaftler dem Datenschutzrecht den Rücken zu und überließen das Feld der öffentlich-rechtlichen und insbesondere – genährt durch weitere Urteile des *BVerfG* – der verfassungsrechtlichen Perspektive.[92] Diese Entwicklung wurde in zweifacher Hinsicht begünstigt:

Erstens wurden traditionelle Kommunikationsinfrastrukturen zunehmend privatisiert. Daraus erwuchsen dem Staat zusätzliche Gewährleistungspflichten in Form einer Privatisierungsfolgenverantwortung,[93] vgl. Art. 87f Abs. 1 GG. Soweit neue – insbesondere internetbasierte – Kommunikationstechniken aufkamen, wurden diese von Anfang an privatrechtlich bereitgestellt. Mit steigender Bedeutung der durch Privatrechtsubjekte bereitgestellten Kommunikations-Infrastruktur nahm auch das von privater Seite ausgehende Gefährdungspotenzial zu. Die „privatisierten Leviathane"[94] rückten ins Zentrum der rechts- und sozialstaatlichen Aufmerksamkeit. Zu den traditionellen Gefährdungen infolge des staatlichen Gewaltmonopols trat ein neues Gefahrenpotenzial infolge der ökonomischen Marktmacht von Unternehmen.[95] Diese technischen und wirtschaftlichen Entwicklungen begünstigen einen Regulierungsansatz, der jegliche Verarbeitung von personenbezogenen Daten unter den Anwendungsbereich des Datenschutzrechts bringt.[96] Er mündet in eine informationelle Prophylaxe oder – im datenschutzrechtlichen Jargon – in einen präventiven Vorfeldschutz.[97]

---

[92] Obwohl der führende Kommentar zum Datenschutzrecht von *Spiros Simitis* (Hessischer Datenschutzbeauftragter von 1975–1991) und damit von einem Privatrechtswissenschaftler bearbeitet wurde, wurde der Kommentar wegen seiner geringen privatrechtlichen Fundierung kritisiert: Hierzu: *Giesen*, JZ 2007, 918 (924 f./Fn. 43).

[93] *Bauer*, VVDStRL 54 (1995), 243 (278 f.).

[94] *Hoffmann-Riem*, 123 AöR (1998), 512 (525).

[95] *BVerfG*, Beschl. v. 22.05.2019, 1 BvQ 42/19 = NJW 2019, 1935 (Rn. 15) – *Nutzung sozialer Netzwerke*.

[96] Zur Videoüberwachung: *Bull*, JZ 2017, 797 (800): „basiert auf einer abstrakten Gefährlichkeitsvermutung, die das Datenschutzrecht in seiner herrschenden Interpretation charakterisiert – ein wesentlicher Grund für den verbreiteten freiheitsfeindlichen Datenpaternalismus. […] Datenschutz wird zum Selbstzweck."

[97] *Brink/Eckhardt*, ZD 2015, 205 (209): „Wesentliche Leistung der Volkszählungsentscheidung war nämlich, dem ‚Verletzungsdelikt APR' ein ‚Gefährdungsdelikt iSB' [zur Seite zu stellen]. Die Umkehr der Rechtfertigungslast für Datenverwendungen zielt gerade darauf ab, Vorfeldschutz schon gegen Rechtsgefährdungen zu leisten". *Marsch* führt diese Entwicklung