

Internetrecht und Digitale Gesellschaft

Band 63

E-Privacy im Trilog

Privatheit im Spannungsfeld konfligierender Interessen

Von

Patrick Herget



Duncker & Humblot · Berlin

PATRICK HERGET

E-Privacy im Trilog

Internetrecht und Digitale Gesellschaft

Herausgegeben von

Dirk Heckmann

Band 63

E-Privacy im Trilog

Privatheit im Spannungsfeld
konfligierender Interessen

Von

Patrick Herget



Duncker & Humblot · Berlin

Die Juristische Fakultät der Universität Passau
hat diese Arbeit im Jahr 2023 als Dissertation angenommen.

Bibliografische Information der Deutschen Nationalbibliothek

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

Alle Rechte vorbehalten
© 2024 Duncker & Humblot GmbH, Berlin
Satz: L101 Mediengestaltung, Fürstenwalde
Druck: CPI books GmbH, Leck
Printed in Germany

ISSN 2363-5479
ISBN 978-3-428-19176-5 (Print)
ISBN 978-3-428-59176-3 (E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☺

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

Meinen Eltern

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2023/2024 von der Juristischen Fakultät der Universität Passau als Dissertationsschrift angenommen. Gesetzgebung, Literatur und Rechtsprechung wurden bis zur Einreichung im März 2023 berücksichtigt.

Mein besonderer Dank gilt meinem Betreuer, Herrn Prof. Dr. Meinhard Schröder. Er gewährte mir die Freiheit, das Thema meiner Dissertation selbst zu wählen und stand mir stets mit konstruktiven Anmerkungen und wertvollen Hinweisen zur Seite. Bei Herrn Prof. Dr. Moritz Hennemann bedanke ich mich für die zügige Erstellung des Zweitgutachtens. Überdies bedanke ich mich bei Herrn Prof. Dr. Kai von Lewinski für die Bereitschaft, den Vorsitz des Prüfungsausschusses zu übernehmen.

Darüber hinaus danke ich der Deutschen Forschungsgemeinschaft, welche mein Promotionsprojekt im Rahmen des DFG-Graduiertenkollegs 1681/2 „Privatheit und Digitalisierung“ umfangreich förderte. Mein Dank gilt außerdem Julia Gilde für das gründliche Korrekturlesen des Manuskripts.

Schließlich möchte ich meiner Familie danken, die mich stets bedingungslos unterstützt. Ohne sie wäre der erfolgreiche Abschluss dieser Arbeit nicht möglich gewesen.

Nüsttal, Februar 2024

Patrick Herget

Inhaltsverzeichnis

Kapitel 1

Thematische Einführung 15

A. Einleitung und Problemaufriss	15
I. Erkenntnisinteresse und Forschungsansatz	16
II. Aufbau der Arbeit	19
B. Privatheit im Kontext ubiquitärer Digitalisierung	21
I. Dimensionen nach Rössler	21
1. Lokale Privatheit	22
2. Dezisionale Privatheit	23
3. Informationelle Privatheit	24
II. Die politische und gesellschaftliche Dimension von Privatheit	25
1. Privatheitsverlust in der Überwachungsgesellschaft	28
2. Verbesserte Partizipationsmöglichkeiten durch digitale Privatheit	30
3. Post-Privacy	32
III. Zusammenfassung	33
C. Datenschutz als Privatheitsschutz	34
I. Individualistische Perspektive	36
II. Disposition über personenbezogene Daten	37
III. Zwischenergebnis	40
D. E-Privacy: Privatheit auf Distanz im Spannungsfeld ubiquitärer Digitalisierung	42
I. Gründe und Ziele der Reform	43
II. Unionsprimärrechtliche Grundlagen	45
1. Art. 7 GRCh	47
2. Art. 8 GRCh	50
3. Verhältnis von Art. 7 und Art. 8 GRCh	53
E. Zwischenergebnis	54

Kapitel 2

Kontroversen und Intransparenz im Rahmen der E-Privacy-Reform

57

A. Interessenlagen im Datenschutz	57
I. Divergierende Frames als Grundlage für Politikpositionen	58

II. Interessengefüge im Rahmen der E-Privacy-Reform	60
1. Verbraucherinteressen	62
a) Zentrale Akteure	62
b) Zentrale Forderungen und Ziele	68
aa) Privatheitsschutz	69
bb) Kostenfreie Inanspruchnahme internetbasierter Anwendungen	70
2. Wirtschaftsinteressen	73
a) Zentrale Akteure	74
b) Zentrale Forderungen und Ziele	78
aa) Datenbasierte Geschäftsmodelle	80
(1) Werbefinanzierung	82
(2) E-Commerce	84
(3) Big Data	85
bb) Geschäftsmodelle mit integriertem Datenschutz	88
3. Sicherheitsinteressen	90
a) Zentrale Akteure	92
b) Zentrale Forderungen und Ziele	94
aa) Cybercrime und -terrorismus	95
bb) Gesundheitsschutz	97
III. Zusammenfassung	98
B. Disproportionale Einflussnahmemöglichkeiten und Intransparenz	99
I. Gemeinwohl und Partikularismus vor dem Hintergrund unterschiedlicher Frames	101
1. Gesetzgebung im informellen Trilogverfahren	105
a) Erteilung der Verhandlungsmandate	107
b) Unterschiede zum formellen Trilog	108
c) Erschwerete Nachvollziehbarkeit	109
2. Lobbyismus	110
II. Recht als Indikator für politischen Einfluss	114
1. Positives Recht als geronnene Politik	116
2. Rechtsetzung als institutionalisierte Kompromissbildung	118
3. Erscheinungsformen von Kompromissen im positiven Recht	119
a) Quantitative und qualitative inhaltliche Lösungen	121
b) Verfahrenslösungen	121
c) Formelkompromisse	122
C. Zusammenfassung	124

Kapitel 3

Vergleichende Analyse der Entwürfe von Kommission und Parlament	126
A. Vorschlag der Europäischen Kommission vom 10.01.2017	126
I. Anwendungsbereich, Definitionen und Inkrafttreten	127
1. Persönlicher und sachlicher Anwendungsbereich	128
a) Elektronische Kommunikationsdienste	132
b) Elektronische Kommunikationsdaten	137
c) Endeinrichtungen der Endnutzer	139
2. Territorialer Anwendungsbereich	140
3. Verhältnis zur DS-GVO	142
4. Inkrafttreten	146
II. Vertraulichkeit und Verarbeitung elektronischer Kommunikationsdaten	148
1. Verarbeitung elektronischer Kommunikationsdaten	149
a) Verarbeitung im Rahmen des Erforderlichen	150
b) Verarbeitung aufgrund Einwilligung	152
aa) Zusätzliche Anforderungen	157
bb) Kopplungsverbot im Bereich elektronischer Kommunikation	159
2. Speicherung und Löschung elektronischer Kommunikationsdaten	163
a) Löschung von Kommunikationsinhalten	165
b) Löschung von Kommunikationsmetadaten	166
III. Schutz von Informationen in Bezug auf die Endeinrichtungen der Endnutzer	167
1. Online-Tracking	168
a) Verarbeitung im Rahmen des Erforderlichen	170
b) Verarbeitung aufgrund Einwilligung	175
aa) Internetzugangssoftware als Torwächter	178
bb) Vorgaben zu Tracking Walls	184
2. Offline-Tracking	186
IV. Öffentliche Sicherheit	191
B. Bericht des Europäischen Parlaments vom 20.10.2017	193
I. Anwendungsbereich, Definitionen und Inkrafttreten	195
1. Persönlicher und sachlicher Anwendungsbereich	195
a) Elektronische Kommunikationsdienste	196
b) Elektronische Kommunikationsdaten	196
c) Endeinrichtungen der Endnutzer	197
2. Territorialer Anwendungsbereich	197
3. Verhältnis zur DS-GVO	198
4. Inkrafttreten	198
II. Vertraulichkeit und Verarbeitung elektronischer Kommunikationsdaten	199
1. Verarbeitung elektronischer Kommunikationsdaten	200

a)	Verarbeitung im Rahmen des Erforderlichen	200
b)	Verarbeitung aufgrund Einwilligung	201
aa)	Zusätzliche Anforderungen	202
bb)	Kopplungsverbot im Bereich elektronischer Kommunikation	203
2.	Speicherung und Löschung elektronischer Kommunikationsdaten	204
a)	Löschung von Kommunikationsinhalten	204
b)	Löschung von Kommunikationsmetadaten	205
III.	Schutz von Informationen in Bezug auf die Endeinrichtungen der Endnutzer	205
1.	Online-Tracking	206
a)	Verarbeitung im Rahmen des Erforderlichen	206
b)	Verarbeitung aufgrund Einwilligung	210
aa)	Internetzugangsssoftware als Torwächter	211
bb)	Vorgaben zu Tracking Walls	216
2.	Offline-Tracking	219
IV.	Öffentliche Sicherheit	220
C.	Gegenüberstellung mit der regulatorischen Situation im Jahr 2017	222
I.	Anwendungsbereich und Definitionen	224
1.	Persönlicher und sachlicher Anwendungsbereich	224
a)	Elektronische Kommunikationsdienste	227
b)	Elektronische Kommunikationsdaten	231
c)	Endeinrichtungen der Endnutzer	233
2.	Territorialer Anwendungsbereich	236
3.	Zwischenergebnis	238
II.	Vertraulichkeit und Verarbeitung elektronischer Kommunikationsdaten	239
1.	Verarbeitung elektronischer Kommunikationsdaten	243
a)	Verarbeitung im Rahmen des Erforderlichen	245
b)	Verarbeitung aufgrund Einwilligung	248
aa)	Zusätzliche Anforderungen	253
bb)	Kopplungsverbot im Bereich elektronischer Kommunikation	254
2.	Speicherung und Löschung elektronischer Kommunikationsdaten	256
a)	Löschung von Kommunikationsinhalten	256
b)	Löschung von Kommunikationsmetadaten	258
3.	Zwischenergebnis	262
III.	Schutz von Informationen in Bezug auf die Endeinrichtungen der Endnutzer	264
1.	Online-Tracking	264
a)	Verarbeitung im Rahmen des Erforderlichen	268
b)	Verarbeitung aufgrund Einwilligung	270
aa)	Internetzugangsssoftware als Torwächter	276
bb)	Vorgaben zu Tracking Walls	277

Inhaltsverzeichnis	13
2. Offline-Tracking	279
3. Zwischenergebnis	280
IV. Öffentliche Sicherheit	283
D. Zusammenfassendes Zwischenergebnis	289
<i>Kapitel 4</i>	
Vergleichende Analyse des Verhandlungsmandats des Rates	293
A. Allgemeine Ausrichtung des Rates vom 10.02.2021	293
I. Anwendungsbereich, Definitionen und Inkrafttreten	296
1. Persönlicher und sachlicher Anwendungsbereich	296
a) Elektronische Kommunikationsdienste	296
b) Elektronische Kommunikationsdaten	297
c) Endeinrichtungen der Endnutzer	297
2. Territorialer Anwendungsbereich	297
3. Verhältnis zur DS-GVO	298
4. Inkrafttreten	299
II. Vertraulichkeit und Verarbeitung elektronischer Kommunikationsdaten	299
1. Verarbeitung elektronischer Kommunikationsdaten	300
a) Verarbeitung im Rahmen des Erforderlichen	301
b) Verarbeitung aufgrund Einwilligung	306
aa) Zusätzliche Anforderungen	310
bb) Kopplungsverbot im Bereich elektronischer Kommunikation .	311
2. Speicherung und Löschung elektronischer Kommunikationsdaten	311
a) Löschung von Kommunikationsinhalten	312
b) Löschung von Kommunikationsmetadaten	312
III. Schutz von Informationen in Bezug auf die Endeinrichtungen der Endnutzer	313
1. Online-Tracking	313
a) Verarbeitung im Rahmen des Erforderlichen	314
b) Verarbeitung aufgrund Einwilligung	319
aa) Internetzugangssoftware als Torwächter	320
bb) Vorgaben zu Tracking Walls	322
2. Offline-Tracking	324
IV. Öffentliche Sicherheit	326
B. Gegenüberstellung mit der regulatorischen Situation im Jahr 2021	329
I. Anwendungsbereich und Definitionen	330
1. Persönlicher und sachlicher Anwendungsbereich	331
a) Elektronische Kommunikationsdienste	333
b) Elektronische Kommunikationsdaten	335
c) Endeinrichtungen der Endnutzer	335

2. Territorialer Anwendungsbereich	336
3. Zwischenergebnis	337
II. Vertraulichkeit elektronischer Kommunikationsdaten	337
1. Verarbeitung elektronischer Kommunikationsdaten	338
a) Verarbeitung im Rahmen des Erforderlichen	343
b) Verarbeitung aufgrund Einwilligung	346
aa) Zusätzliche Anforderungen	349
bb) Kopplungsverbot im Bereich elektronischer Kommunikation	350
2. Speicherung und Löschung elektronischer Kommunikationsdaten	352
a) Löschung von Kommunikationsinhalten	352
b) Löschung von Kommunikationsmetadaten	355
3. Zwischenergebnis	356
III. Schutz von Informationen in Bezug auf die Endeinrichtungen der Endnutzer	358
1. Online-Tracking	358
a) Verarbeitung im Rahmen des Erforderlichen	361
b) Verarbeitung aufgrund Einwilligung	363
aa) Internetzugangssoftware als Torwächter	367
bb) Vorgaben zu Tracking Walls	369
2. Offline-Tracking	370
3. Zwischenergebnis	371
IV. Öffentliche Sicherheit	373
C. Zusammenfassendes Zwischenergebnis	378
 <i>Kapitel 5</i>	
Schlussbetrachtung	380
A. Zusammenfassende Darstellung der Ergebnisse	380
I. Sinnbildlichkeit der E-Privacy-Reform für aktuelle Privatheitsdiskurse	380
II. Notwendigkeit des interdisziplinären Forschungsansatzes	381
1. Interessengefüge im Bereich des Datenschutzes	381
2. Verordnungsentwürfe als statische Momentaufnahme	382
III. Entgegengesetzte Berücksichtigung divergenter Interessen	383
IV. Disproportionaler Einfluss durch intransparente Strukturen?	383
B. Ausblick und Schlussbemerkung	385
I. Aktueller Stand der Trilogverhandlungen	385
II. Privatheit zwischen Ungewissheit und Bedeutungsverlust?	387
III. Privatheitsschutz mit Unzulänglichkeiten	389
Literaturverzeichnis	392
Sachwortverzeichnis	428

Kapitel 1

Thematische Einführung

A. Einleitung und Problemaufriss

Menschen hinterlassen tagtäglich vielfältige Spuren, die Rückschlüsse auf ihre Person ermöglichen. Während die Zuordnung eines physischen Finger- oder Schuhabdrucks zu einer bestimmten Person nur mit erheblichem Aufwand möglich ist, lassen digitale Spuren im Netz einen schnellen und präzisen Rückschluss auf sehr sensible und persönliche Informationen eines bestimmten Nutzers¹ zu.² Wenngleich das Aufkommen neuer Medien schon immer auch von Bedenken begleitet wurde,³ führt die Ubiquität des Internets zu einer grundsätzlichen Transformation nahezu aller Lebensbereiche und gesellschaftlicher Praktiken.⁴ Digitale Daten sind wertvoll und können beliebig vervielfältigt und kombiniert werden. Vor allem die Kommerzialisierung des Internets sowie die Ausweitung staatlicher Zugriffsbefugnisse zur Kriminalitäts- und Terrorismusbekämpfung führen dabei zunehmend zu Konflikten mit dem Interesse des Individuums am Schutz seiner Privatheit. Obwohl die komplexen Verarbeitungsvorgänge für den Einzelnen oft nicht nachvollziehbar sind und die Vorbehalte vor staatlicher und kommerzieller Überwachung weiter verstärkt wurden, ist die Nutzung informationstechnischer Systeme zunehmend unerlässlich, damit Menschen am gesellschaftlichen Leben partizipieren können.⁵ Überdies werden persönliche Informationen oftmals durch die Nutzer selbst bereitwillig preisgegeben, um internetbasierte Angebote und Dienste ohne die Zahlung eines monetären Entgelts in Anspruch nehmen zu

¹ In der vorliegenden Forschungsarbeit wird aus Gründen der besseren Lesbarkeit die Form des generischen Maskulinums verwendet. Diese soll jedoch geschlechtsunabhängig verstanden werden.

² *Albrecht*, Finger weg von unseren Daten!, S. 53.

³ So befürchtete man bereits Ende des 19. Jahrhunderts das Eindringen fotografischer Momentaufnahmen und des Zeitungsgeschäfts in das Private. Siehe dazu *Warren/Brandeis*, The Right to Privacy, Harvard Law Review 1890, Vol. 4, No. 5, S. 193, 195 f.

⁴ *Becker/Seubert*, DuD 2016, S. 73, 78.

⁵ *Jandt*, Der Januskopf des Internet – Zur Ambivalenz von Selbst- und Fremdbe- stimmung, in: Hruschka/Joerden (Hrsg.), Jahrbuch für Recht und Ethik, Bd. 23, S. 53, 71; *Papier*, Die Warnung, S. 112.

können.⁶ Die tiefgreifenden Kontroversen im Bereich der Netzpolitik und die Regulierung der sich dynamisch fortentwickelnden, vielschichtigen Verarbeitungsmöglichkeiten und Geschäftsmodelle gestalten sich dabei insbesondere für politische Entscheidungsverfahren als Herausforderung.⁷

I. Erkenntnisinteresse und Forschungsansatz

Um die derzeitige Entwicklungsrichtung des gesellschaftlichen und politischen Wertes von Privatheit im Kontext allgegenwärtiger Digitalisierung zu beschreiben, nimmt die vorliegende Arbeit vor dem Hintergrund der genannten netzpolitischen Entwicklungen eine interdisziplinäre rechtspolitische bzw. gesetzgebungswissenschaftliche⁸ Perspektive ein. Indem widerstreitende Interessen in zunehmend netzwerkartigen Entscheidungsprozessen in Ausgleich gebracht werden müssen, werden die Grenzen des Privatheitsschutzes auch auf einer politischen Ebene verhandelt.⁹ In diesem Zusammenhang kommt insbesondere Rechtsetzungsprozessen im Bereich des Datenschutzes eine herausragende Bedeutung zu, da hier die gesellschaftlichen Interessendifferenzen und Spaltungen in Bezug auf Digitalisierungsdiskurse sichtbar werden.

Geradezu charakteristisch für die Konflikte um Privatheit innerhalb von Digitalisierungsdiskursen gestaltet sich dabei der Rechtsetzungsprozess zur E-Privacy Verordnung, in welchem die konfliktierenden Interessenlagen im Bereich des Datenschutzes konzentriert abgebildet werden.¹⁰ Die Reform im sektorspezifischen Telekommunikationsdatenschutzrecht soll die DS-GVO präzisieren und ergänzen sowie die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG¹¹ ersetzen. Im Kontext der Strategie für ei-

⁶ *Einspanner-Pflock*, Privatheit im Netz, S. 68; *Füllsack*, Die Regulierung von OTT-Kommunikationsdiensten, S. 57; *Seemann*, Das neue Spiel, S. 16.

⁷ Vgl. *Veddern*, Digitale Souveränität und europäische Öffentlichkeit ... oder warum es eines neuen Zeitalters der europäischen Aufklärung bedarf, in: *Friedrichsen/Bisa* (Hrsg.), *Digitale Souveränität, Vertrauen in der Netzwerkgesellschaft*, S. 333, 334.

⁸ Gesetzgebungswissenschaft analysiert Gesetze, wie sie sind und wie sie ein sollten. Die fehlende Festlegung als Wissenschaftsdisziplin könnte dabei weniger als Grenze, sondern als Chance begriffen werden. Siehe dazu *Schulze-Fielitz*, Theorie und Praxis parlamentarischer Gesetzgebung, S. 35.

⁹ Privatheit wird auf verschiedenen Ebenen reguliert, jedoch ist die Verhandlung von Privatheit als politische Aufgabe von besonderer Bedeutung. Vgl. *Becker/Seubert*, *DuD* 2016, S. 73, 78.

¹⁰ In diese Richtung auch *Hildebrandt/Arnold*, Wirtschaftliche Auswirkungen der Regelungen der ePrivacy-Verordnung auf die Online-Werbung und werbefinanzierte digitale Geschäftsmodelle, S. 27.

¹¹ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) vom

nen digitalen Binnenmarkt für Europa¹² verfolgt die Initiative einen zweifachen Zweck.¹³ So soll die Verordnung sowohl einen effektiveren Schutz der Vertraulichkeit der elektronischen Kommunikation sowie der enthaltenen Daten der Nutzer sicherstellen als auch zugleich einen freien Datenverkehr gewährleisten.¹⁴ Auch Aspekte öffentlicher Sicherheit wurden wiederholt im Rahmen der Verhandlungen thematisiert.¹⁵

Entgegen dem ursprünglichen Zeitplan der Kommission, der ein gemeinsames Inkrafttreten der Verordnung mit der DS-GVO am 25.05.2018 vorsah, verzögerte sich das ambitionierte rechtspolitische Vorhaben bis zuletzt. Nachdem bereits im Rechtsetzungsprozess zur DS-GVO eine zunehmende Lobbyarbeit, insbesondere durch Akteure der Digitalwirtschaft, beobachtet werden konnte,¹⁶ setzte sich diese Entwicklung im Rahmen der E-Privacy-Reform fort.¹⁷ Wenngleich dies einerseits die außerordentliche Bedeutung, die dem Politikfeld des Datenschutzes mittlerweile zukommt, veranschaulicht, wirft das strukturelle Ungleichgewicht im Rahmen der Interessenvertretung andererseits die Frage auf, ob eine überproportionale Repräsentation partikularer, nicht verallgemeinerungsfähiger Interessen zu einer Untergrabung des demo-

12. Juli 2002, ABl. L 201/37 vom 31.07.2002, zuletzt geändert durch Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universalien und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz vom 25. November 2009, ABl. L 337/11 vom 18.12.2009.

12 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa vom 06.05.2015, COM (2015) 192 final.

13 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.01.2017, COM (2017) 10 final, Begründung, S. 4.

14 Hoffmann/Eckhardt, cepAnalyse Nr. 16/2017, S. 1.

15 Siehe dazu etwa Engeler, PinG 2018, S. 141, 143 f.; Sippel, Für einen besseren Privatsphäre-Schutz im Internet – die ePrivacy-Verordnung, <https://birgitsippel.de/libe-ausschuss-fuer-buergerliche-freiheiten-justiz-und-inneres/eprivacy/>.

16 Schrems, Die DSGVO als Produkt von Lobbyismus und Tauschhandel, in: Knyrim (Hrsg.), Datenschutz-Grundverordnung, S. 33–37.

17 Vgl. Cáceres, Lobby-Einfluss auf neue EU-Verordnung, <https://www.sueddeutsche.de/digital/lobby-einfluss-auf-neue-eu-verordnung-internetkonzerne-schreiben-bei-datenschutzregeln-mit-1.1596560>; Dachwitz, ePrivacy: Die Lobby macht der Datenindustrie, <https://netzpolitik.org/2017/eprivacy-die-lobby-macht-der-datenindustrie/>.