

Schriften zum Öffentlichen Recht

Band 1301

Das IT-Grundrecht

Schnittfelder und Auswirkungen

Von

Markus Hauser



Duncker & Humblot · Berlin

MARKUS HAUSER

Das IT-Grundrecht

Schriften zum Öffentlichen Recht

Band 1301

Das IT-Grundrecht

Schnittfelder und Auswirkungen

Von

Markus Hauser



Duncker & Humblot · Berlin

Die Fakultät für Rechtswissenschaft
der Universität Hamburg
hat diese Arbeit im Jahr 2014
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
© 2015 Duncker & Humblot GmbH, Berlin
Fremddatenübernahme: L101 Mediengestaltung, Berlin
Druck: CPI buchbücher.de, Birkach
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-14643-7 (Print)
ISBN 978-3-428-54643-5 (E-Book)
ISBN 978-3-428-84643-6 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ☼

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

Vorwort

Die vorliegende Arbeit wurde im Sommersemester 2014 von der rechtswissenschaftlichen Fakultät der Universität Hamburg als Dissertation angenommen. Später erschienene Literatur konnte für die Drucklegung noch bis zum April 2015 berücksichtigt werden.

Mein Dank gilt Frau Prof. Dr. Marion Albers für die fachliche Betreuung der Arbeit über zwei Universitäten hinweg und wertvolle Anregungen. Herrn Prof. Dr. Wolfgang Schulz danke ich für die Anfertigung des Zweitgutachtens.

Persönlich möchte ich meinen Eltern, meinen Freunden und Kollegen für die Unterstützung in der Zeit der Entstehung dieser Arbeit und darüber hinaus danken.

Markus Hauser

Inhaltsverzeichnis

A. Einleitung	13
I. Ein neuer Ansatz für den Persönlichkeitsschutz	13
1. Einführung	13
2. Vertraulichkeit und Integrität informationstechnischer Systeme	14
II. Ziele der Untersuchung	16
III. Gang der Untersuchung	17
B. Grundlagen der Online-Durchsuchung	19
I. Zielsetzung	19
II. Nutzung und Missbrauch von Informationstechnologie	19
III. Bisherige Ermittlungsmöglichkeiten	22
1. Auskunft über Telekommunikationsverkehrsdaten	22
2. Telekommunikationüberwachung	25
3. Offene Durchsuchung, Sicherstellung	26
4. Akustische Wohnraumüberwachung	28
IV. Weitere Defizite der vorhandenen Ermittlungsmethoden	28
V. Online-Durchsuchung	29
1. Begriffsverständnis	30
2. Durchführung	31
a) Spähprogramm in den Händen staatlicher Behörden	31
b) Ablauf einer Online-Durchsuchung	34
3. Technische Herausforderungen	36
a) Installation	36
aa) Infiltration unter maßgeblicher Mitwirkung des Nutzers	37
bb) Infiltration unter geringer oder ohne Mitwirkung des Nutzers	38
b) Laufender Betrieb	41
c) Zwischenergebnis	42
VI. Bewältigung früherer Online-Durchsuchungen	43
C. Grundlegende Konzeption des IT-Grundrechts	46
I. Ein neues Grundrecht?	47
II. Schutzkonzept	49
1. Verwirklichung der Persönlichkeit bei der Nutzung informationstechnischer Systeme	50
2. Persönlichkeitsgefährdungen	54
3. Persönlichkeitsschutz in neuer Anknüpfung	55
a) Perspektivwechsel hin zu einem gegenständlichen Schutz	57

b) Vertraulichkeit und Integrität	60
c) Systemschutz ergänzt Systemdatenschutz	61
4. Virtuelle Wohnung?	66
III. Schutzbereich	70
1. Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	70
2. Das informationstechnische System	71
a) Grundlage	71
aa) Funktionseinheit	73
bb) Steuerung durch Verarbeitungslogik	74
cc) Technische Abgrenzung	75
dd) Zwischenergebnis	77
b) Bedeutung der Vernetzung	79
c) Beschränkung auf komplexe IT-Systeme	80
aa) Potentieller Einblick in wesentliche Teile der Lebensgestaltung	82
bb) Lediglich punktueller Bezug zu einem bestimmten Lebensbereich	83
cc) Beurteilung der Einschränkung	85
d) Einzelfälle	87
aa) Komponenten von IT-Systemen	87
bb) Mobiltelefone	88
cc) Lokale Netzwerke	90
dd) Von Hardware abstrahierte Systeme und Dienste	91
(1) Virtuelle IT-Systeme	91
(2) Cloud Computing	93
(3) Sonstige Online-Benutzerkonten	96
ee) Chipkarten mit Mikroprozessor, RFID	98
3. Nutzung als eigenes System	100
a) Einfachgesetzliche Zuordnungskriterien	101
b) Verfassungsrechtliches Verständnis	105
c) Einzelfälle	108
aa) Gemeinsame Nutzung	108
bb) Eigenes System über Systeme in der Verfügungsgewalt anderer	110
4. Vertraulichkeit und Integrität	112
a) Vertraulichkeit – Vertraulichkeitserwartung	112
b) Integrität – Integritätserwartung	116
5. Anvertrauen von Daten als weitere Anforderung?	119
6. Anwendbarkeit auf juristische Personen, Art. 19 Abs. 3 GG	120
7. Zwischenergebnis	124

D. Einordnung in das bestehende Grundrechtsgefüge	125
I. Fernmeldegeheimnis, Art. 10 GG	126
1. Relevante Entscheidungen zum Telekommunikationsschutz	127
2. Folgerungen für die neue Gewährleistung	130
a) Laufende Kommunikation, Quellen-TKÜ	135
b) Systeme in der Verfügungsgewalt Dritter	137
aa) Zugriff auf dem vorgesehenen Weg	137
bb) Abgrenzungskriterium Beherrschbarkeit	138
cc) Abgrenzungskriterium Kommunikation	141
dd) Abgrenzung von Kommunikationsinhalten und sonstigen Daten	143
ee) Autorisierungskriterium und Idealkonkurrenz	146
ff) Folgerungen	147
c) Lokale Netzwerke	150
d) Technische Kommunikationsvorgänge, IMSI-Catcher	152
3. Zwischenergebnis	154
II. Unverletzlichkeit der Wohnung, Art. 13 Abs. 1 GG	155
1. Schutzlücke des Wohnungsgrundrechts	158
2. Messung von Abstrahlungen	164
3. Konsequenzen für offene Maßnahmen	167
4. Zwischenergebnis	168
III. Schutz des Eigentums, Art. 14 GG	170
IV. Schutz der Privatsphäre	174
V. Recht auf informationelle Selbstbestimmung	178
1. Abgrenzung durch das Bundesverfassungsgericht	183
a) Gewährleistungsgehalt des IT-Grundrechts	183
b) Einzelne Datenerhebungen – punktuelle Eingriffe	190
c) Offene Maßnahmen	193
d) Komplexität	194
e) Integritätsschutz	195
f) Zwischenergebnis	196
2. Subsidiarität des IT-Grundrechts	197
3. Spezialität des IT-Grundrechts	198
a) Einordnung in das vorhandene Grundrechtsgefüge	200
b) Chance auf einheitlichen Beurteilungsmaßstab	201
4. Ergänzungsverhältnis der Gewährleistungen	203
VI. Sonstige Grundrechte	205
1. Pressefreiheit, Art. 5 Abs. 1 GG	205
2. Berufsfreiheit, Art. 12 Abs. 1 GG	206
E. Beschränkungen des IT-Grundrechts	209
I. Eingriff	209
1. Integrität	210

2. Vertraulichkeit	213
3. Besondere Fallkonstellationen	215
a) Online-Durchsuchung	215
b) Quellen-Telekommunikationsüberwachung	216
c) Offene, punktuelle Maßnahmen	219
d) Eingriffe in vernetzten Zusammenhängen	221
4. Nachwirkender Schutz	222
II. Rechtfertigung	223
1. Völkerrechtliche Belange	223
2. Legitimer Zweck	226
3. Geeignetheit	226
a) Einschätzungsprärogative des Gesetzgebers	227
b) Selbstschutz	228
c) Beweiswert von erlangten Daten	229
4. Erforderlichkeit einer Eingriffsbefugnis	231
5. Verhältnismäßigkeit im engeren Sinne	233
a) Gesteigerte Intensität des Eingriffs	233
aa) Ausforschungspotential	233
bb) Dauer des Eingriffs – Dauerüberwachung contra Momentaufnahme	235
cc) Heimlichkeit	235
dd) Beeinträchtigung der Integrität	237
ee) Streubreite	239
ff) Zwischenergebnis	240
b) Inhaltliche Anforderungen	241
aa) Präventive Online-Durchsuchung	241
(1) Übertugend wichtiges Rechtsgut	241
(2) Tatsächliche Anhaltspunkte einer konkreten Gefahr	243
bb) Repressive Online-Durchsuchung	246
c) Verfahrensrechtliche Rahmenbedingungen	248
aa) Richtervorbehalt	248
bb) Dokumentation	253
cc) Benachrichtigungspflicht	254
dd) Evaluierungspflicht	255
ee) Sonstige Vorkehrungen	259
d) Kernbereichsschutz	262
aa) Unantastbarer Kernbereich privater Lebensgestaltung	262
bb) Prozedurales Schutzkonzept	266
(1) Ausforschungseingriffe in den Kernbereich – „Tagebuch.txt“	266
(2) Auswertungsphase	271
6. Abweichender Maßstab für sonstige Eingriffe	274

a) Quellen-TKÜ	275
aa) Verfassungskonforme Gestaltung von Eingriffen	275
bb) Bisherige Ermächtigungsgrundlagen – insbesondere § 100a StPO	276
b) Offene, punktuelle Maßnahmen	283
c) Messung von Abstrahlungen	287
d) Isolierte Integritätsbeeinträchtigungen	289
F. Ausblick: Ausstrahlungswirkung und Schutzpflichten	290
I. Allgemeines	290
1. Ausstrahlungswirkung – mittelbare Drittwirkung	291
2. Schutzpflichten	292
II. Problemfelder bei der Nutzung von IT-Systemen	293
1. Grundlegende Herausforderungen	294
2. Gezielte (externe) Beeinträchtigungen	295
a) Hacking und Schadprogramme	295
b) Zugriff auf lokale Netzwerke	296
c) Missbrauch von Kommunikationsmitteln mit Auswirkung auf IT-Systeme	297
3. Immanente Beeinträchtigungen	297
a) Unerwünschte Funktionen von Hard- und Software	297
b) Sicherheitslücken	298
c) Exkurs: Entfernen von Nutzungsbeschränkungen – Jailbreaking, Rooting	299
4. Nutzung fremder IT-Infrastrukturen	300
a) Allgemeines	300
b) Arbeits- und Dienstverhältnisse	300
c) Cloud Computing	301
d) Sonstige Benutzerkonten, Soziale Netzwerke	303
III. Grundlegende Mechanismen der IT-Gewährleistung	304
1. Schwerpunkt bei der privatrechtlichen Ausgestaltung	305
2. Technisch-organisatorische Schutzkonzepte	306
3. Hilfe zur Selbsthilfe	309
IV. Einfachgesetzliche Ansatzpunkte für das IT-Grundrecht	310
1. Öffentliches Recht	310
a) Datenschutzrecht, BDSG	310
b) Weitere Regelungen	314
aa) Elektronischer Identitätsnachweis: § 27 Abs. 3 PAuswG	314
bb) De-Mail-Gesetz	315
2. Zivilrecht	316
a) Schuldrecht und insbesondere Vertragsrecht	316
b) Deliktsrecht	319
3. Strafrecht	323

a) Schutzgut Vertraulichkeit	324
aa) § 202a StGB – Ausspähen von Daten	324
bb) § 202b StGB – Abfangen von Daten	325
cc) § 202c StGB – Vorbereiten des Ausspähens und Abfangens von Daten	327
dd) Exkurs: § 201a StGB – Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen	328
b) Schutzgut Integrität	329
aa) § 303a StGB – Datenveränderung	329
bb) § 303b StGB – Computersabotage	331
c) Ergebnis	333
V. Besondere Fallgruppen	334
1. Arbeitsrecht	334
2. Vernetzte Systeme: Cloud Computing etc.	336
G. Ergebnis	340
I. Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme	340
1. Genese des IT-Grundrechts	340
2. Abwehrrecht	340
a) Schutzbereich	340
b) Einordnung in das bestehende Grundrechtsgefüge	341
c) Beschränkungen	342
3. Objektive Grundrechtsdimensionen	344
II. Ausblick	344
Literaturverzeichnis	346
Sachwortverzeichnis	373

A. Einleitung

I. Ein neuer Ansatz für den Persönlichkeitsschutz

1. Einführung

In nahezu jedem Lebensbereich kommen Bürger und Staat inzwischen mit elektronischer Datenverarbeitung in Berührung. Dabei fallen zwei Entwicklungen auf: Zum einen halten Datenverarbeitungssysteme mehr und mehr Einzug in das private Umfeld des Einzelnen. Wo früher Großrechenanlagen für unternehmerische oder staatliche Zwecke eingesetzt wurden, finden sich nun Personal Computer, Laptops, Smartphones und Tablets in den Haushalten und Jackentaschen der Bürger. Solche Systeme sind dabei nicht mehr nur isolierte Arbeits- oder Unterhaltungsgeräte. Sie werden vielmehr zunehmend mit der Lebensgestaltung selbst verflochten. Durch zahlreiche Erfassungsmöglichkeiten und die fortschreitende Vereinfachung ist eine zunehmende Digitalisierung verschiedenster Persönlichkeitsäußerungen zu beobachten.¹ Damit wachsen zunächst Datenbestände im – vermeintlichen – Einflussbereich des Einzelnen, denen bereits aus ihrer Quantität und Qualität heraus eine hohe Aussagekraft über die Persönlichkeit des Betroffenen zukommt. Parallel zu dieser Entwicklung schreitet auch die elektronische Vernetzung weiter voran. Das Internet hat als ubiquitäres Medium – ähnlich wie die Datenverarbeitungsanlagen – Einzug in die persönliche Lebensgestaltung der Bürger gehalten. Neben der Recherche von Daten zu eigenen Zwecken sind neue Möglichkeiten entstanden, Inhalte mit Dritten oder der Öffentlichkeit zu teilen.

Den Chancen dieser neuen Technologien stehen jedoch vielfältige Risiken für die Belange des Einzelnen gegenüber, die durch die Verzahnung von dezentraler Datenverarbeitung und elektronischer Kommunikation verstärkt werden. Die Begehrlichkeiten Dritter sind vielgestaltig. Sie richten sich zum einen auf die Erforschung der Teilnahme des Einzelnen an Kommunikationsvorgängen. Aber auch die Endgeräte selbst rücken verstärkt in den Fokus, versprechen sie doch tiefere Einblicke in die Persönlichkeit des Nutzers und Zugriff auf sonst kaum zu erlangende Daten. Eine zunehmend dauerhafte Vernetzung durch permanente Internetverbindungen und die Übersim-

¹ Vgl. *Schaar*, in: *Vieweg/Gerhäuser*, *Digitale Daten*, S. 64: „Automatisierung bereits in der Erhebungsphase“.

plifizierung eigentlich komplexer Zusammenhänge durch immer einfachere Benutzerschnittstellen erhöhen die Risiken von Persönlichkeitsbeeinträchtigungen weiter.

Das vorgefundene Grundrechtsgefüge schützt in vernetzten Zusammenhängen bereits Privatheitserwartungen²: Spezielle Gewährleistungen finden sich zunächst in Artt. 10 und 13 GG. Hinzu treten mit dem Recht auf Achtung der Privatsphäre und dem Recht auf informationelle Selbstbestimmung Ausprägungen des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V.m. Art. 1 Abs. 1 GG.

Personal Computer und ähnliche Geräte wurden dagegen bis vor Kurzem nicht als eigenständige Anknüpfungsobjekte für grundrechtliche Schutzmechanismen erkannt. Gleichwohl bündeln sich in ihnen spezifische Privatheitserwartungen. Sieht man von der grundsätzlichen Möglichkeit des Totalverzichts ab, ist der Einzelne zunehmend auf diese informationstechnischen Systeme in seinem Umfeld und auf deren Zuverlässigkeit angewiesen. Gleichzeitig sind gerade diese Systeme spezifischen Gefahren ausgesetzt.

2. Vertraulichkeit und Integrität informationstechnischer Systeme

Am 27. Februar 2008 hat der erste Senat des Bundesverfassungsgerichts anlässlich der Entscheidung zur sogenannten Online-Durchsuchung das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Fallgruppe des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V.m. Art. 1 Abs. 1 GG ausgeformt. Staatliche Ermittler haben aus der Verbreitung von (vernetzten) dezentralen Datenverarbeitungssystemen und damit verbundenen technischen Entwicklungen den Wunsch abgeleitet, wie bereits private Hacker viele Jahre zuvor Zugriff auf diese Systeme zu erlangen.

In seiner Genese unterscheidet sich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gerade dadurch vom Recht auf informationelle Selbstbestimmung, dass eine *spezifische Privatheitserwartung* ausgemacht wird, die eine konkrete thematische Anknüpfung ähnlich dem Wohnungsschutz aus Art. 13 GG ermöglicht. Das Bundesverfassungsgericht hat in seiner Entscheidung mit dem informationstechnischen System (IT-System) einen Topos hervorgehoben, der ohnehin bereits seit längerer Zeit ein wichtiger Faktor im Leben und für das Leben

² Vgl. *Albers*, DVBl. 2010, 1061 ff. zu den Dichotomien der Privatheit; *Benda*, in: *ders./Maihofer/Vogel*, Handbuch Verfassungsrecht, 2. Auflage, § 6 Rn. 27; *Heckmann*, K&R 2010, 770 (773) zur Bedeutung in vernetzten Zusammenhängen.

der Bürger ist. Deshalb kann auch ohne genaueren Blick auf die Ausführungen des Gerichts oder die Definitionsversuche der wissenschaftlichen Literatur zumindest eine Vorstellung von „informationstechnischen Systemen“ vorausgesetzt werden.

Dem IT-System als *Datenkontext* wird mit der Schaffung des IT-Grundrechts eine neue Bedeutung beigemessen. Das betrifft aus staatlicher Sicht die Art der Datengewinnung³ wie auch den Umgang mit den aus den Daten gewonnenen Informationen. Informationen sind durch ihre Datenbasis und durch deren Interpretation geprägt.⁴ Bestimmend für das neue Schutzkonzept ist die besondere Qualität der auf Seite des Bürgers zugrunde liegenden Verarbeitungsstrukturen und -prozesse. Dementsprechend muss jede Bewertung bei der Bestimmung des IT-Systems und seiner Bedeutung für den Einzelnen ansetzen. Die Interpretationsebene wird jedoch insbesondere dann relevant, wenn sich die Risiken systemspezifischer Eingriffe auf die Interpretation der erlangten Daten auswirken können. Das ist etwa der Fall, wenn erhebliche Risiken einer Manipulation durch Dritte bestehen, die sowohl die Interessen des Betroffenen als auch der Ermittler beeinträchtigen.

Angesichts der von einer marktwirtschaftlichen Dynamik geprägten Entwicklung der Informationstechnologie muss ein wirksamer Grundrechtsschutz bereits zwingend die Technikgestaltung einbeziehen. Die Abwehr von Informationseingriffen in IT-Systeme ist damit nur *ein* Bestandteil eines umfassenden und mehrere Grundrechte übergreifenden Schutzkonzepts. Wichtig ist schon eine grundrechtswahrende Gestaltung von Systemen und Abläufen. Selbst im Hinblick auf konkrete Beeinträchtigungen darf der *Kontext* des Eingriffs nicht außer Acht gelassen werden. (Staatliche) Methoden müssen in allen Phasen auf die besonderen Anforderungen der IT-Systeme ausgerichtet werden. Damit ist freilich eine weitere Verrechtlichung verbunden, die aber mit der fortschreitenden Technisierung korrespondiert.

Die Formulierung „Vertraulichkeit und Integrität informationstechnischer Systeme“ weist eine Reihe von Bedeutungsaspekten auf und vermittelt die trügerische Erwartung eines absoluten Schutzanspruchs. Schon grundlegende Erfahrungen mit dem Thema IT-Sicherheit lehren den durchschnittlichen Nutzer von Personal Computern, Smartphones und ähnlichen Geräten, dass

³ S. zum unscharfen Begriff des Informationseingriffs etwa BVerfGE 65, 1 (52); *Schwan*, VerwA 66 (1975), 120 (127 ff.). Unter diesem Begriff wird missverständlich auch die Informationstätigkeit des Staates zusammengefasst, vgl. *Bethge*, in: *Merten/Papier*, Handbuch der Grundrechte, Bd. III, § 58 Rn. 42. Besser geeignet erscheint im Zusammenhang mit (staatlichen) Warnungen der Begriff des „Informationshandelns“, vgl. BVerfGE 105, 252 (268).

⁴ Vgl. *Albers*, in: *Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle*, Grundlagen des Verwaltungsrechts, Bd. II, 2. Auflage, § 22 Rn. 12, die für den Kontext weiter zwischen Daten, Beobachtungen und Mitteilungen differenziert.