UniversitätsSchriften

Recht 929

Julia Stinner

Staatliche Schutzpflichten im Rahmen informationstechnischer Systeme

Nomos

Nomos Universitätsschriften

Recht

Band 929

Julia Stinner

Staatliche Schutzpflichten im Rahmen informationstechnischer Systeme

Nomos

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

Zugl.: Bonn, Univ., Diss., 2017

ISBN 978-3-8487-4664-4 (Print)

ISBN 978-3-8452-8891-8 (ePDF)

1. Auflage 2018
© Nomos Verlagsgesellschaft, Baden-Baden 2018. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Vorwort

Die vorliegende Bearbeitung wurde im Wintersemester 2016/2017 von der Rechtswissenschaftlichen Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn als Dissertation angenommen. Sie widmet sich der Fragestellung, inwiefern effektiver Persönlichkeitsschutz in einer digitalisierten Welt vom Staat verlangt und gewährleistet werden kann. Im Fokus der Überlegungen stehen das Recht auf informationelle Selbstbestimmung und insbesondere das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Ausprägungen des allgemeinen Persönlichkeitsrechts aus Artikel 2 I in Verbindung mit Artikel 1 I des Grundgesetzes. Am Beispiel sogenannter intelligenter Verkehrssysteme und des vernetzten und kommunikationsfähigen Fahrzeugs als einem der bisher letzten unüberwachten Rückzugsorte der individuellen Privatsphäre soll der Gedanke einer staatlichen Schutzpflicht untersucht werden.

Ich danke meinem Doktorvater und akademischen Lehrer Herrn Bundesverfassungsrichter a.D. Professor Dr. Dr. Udo Di Fabio sehr herzlich für seine stetige Inspiration und Hilfsbereitschaft. Die Zeit an seinem Lehrstuhl war für mich in persönlicher und beruflicher Hinsicht eine wertvolle Bereicherung und wird mir stets in bester Erinnerung bleiben. Damit verbunden ist ein Dank an alle Kolleginnen und Kollegen der staatsrechtlichen Abteilung des Instituts für Öffentliches Recht.

Für die rasche Erstattung des Zweitgutachtens gebührt Professor Dr. Dr. h.c. Matthias Herdegen Dank. Für ein großzügiges und vielfältiges Promotionsstipendium bin ich der Konrad-Adenauer-Stiftung dankbar, das mir mein Dissertationsvorhaben ermöglicht und erleichtert hat. Besonders danke ich Dr. Gernot Uhl, der als mein betreuender Referent immer ein offenes Ohr hatte und stets mit Rat und Tat zu Seite stand. Für seine Gesprächsbereitschaft danke ich des Weiteren MdEP Axel Voss. Auch dem Nomos Verlag, insbesondere Herrn Dr. Ganzhorn, möchte ich herzlich für die Unterstützung bei der Veröffentlichung meiner Arbeit danken.

Ein herzlicher Dank gilt Julia Polley, Anna Molinari und Ann-Kathrin Jungen für Ihre wertvolle Freundschaft. Ich danke ebenfalls sehr herzlich

Gisela Hütter, Tobias Polley, Claudia Mors, Dr. Corinna Bringmann und Sebastian Klein. Ein besonderer Dank gilt Sascha Becher.

Schließlich danke ich meiner Mutter, Ulrike Stinner, für ihre beständige Unterstützung, ihre Ermutigung und ihr immerwährendes Vertrauen in all meine Vorhaben.

Dafür danke ich auch Marliese und Rudolf Theis, die mir stets eine wichtige Stütze sind. Ein letzter Dank gilt Birgit und Hans-Joachim Utsch.

Bonn, im Dezember 2017 *Julia Stinner*

Inhaltsverzeichnis

Abkürzungsverzeichnis 15

A. Einführung 19

I. Fortschritt durch Digitalisierung 19
II. Gefährdungslage: Vernetztes Fahrzeug und intelligentes Verkehrssystem 22
III. Gang der Untersuchung 24

B. Charakteristika moderner Verkehrsinformationstechnologie 26

I. Begriffsbestimmungen 26
1. Digitalisierung 26
2. Daten und Informationen 27
3. „Informationstechnisches System“ 29
a) Informationstechnische Grundlagen 29
b) Rechtliche Grundlagen 30
aa) Bestimmung vor BVerfGE 120, 274 30
bb) Bestimmung im Kontext von Online-Durchsuchungen 31
c) Übertragung auf moderne Informationstechnologie 33
aa) Zugrundeliegendes Verständnis 33
bb) Vernetztes Fahrzeug als informationstechnisches System 34
II. Funktionsweise und Technik 35
1. Modelldifferenzierung und Definition 36
a) Das vernetzte Fahrzeug 36
b) Das intelligente Verkehrssystem 37
2. Technische Voraussetzungen 38
3. Quantität und Qualität der Datenverarbeitung 40
a) Kategorisierung und Informationsgehalt 40
b) Personenbezug der Daten 41
c) Gefährdungspotenzial 43
4. Telematik-Versicherungen 43

5. Das europaweite Notrufsystem eCall 45
a) Technische Realisierung 46
b) Gefährdungspotenzial 46

C. Verfassungsrechtliche Grundlagen 48

I. Entwicklung der Grundrechte ab dem 19. Jahrhundert 48
II. Grundrechtsfunktionen 50
1. Grundrechte als Abwehrrechte 51
2. Grundrechte als Leistungs-, Teilhabe- und Mitwirkungsrechte 52
3. Schutzfunktion der Grundrechte 54
III. Die grundrechtliche Schutzpflicht 54
1. Der Gedanke der grundrechtlichen Schutzpflicht 55
a) Die Legitimation des Staates nach Hobbes und Locke 56
b) Der Zusammenhang von Sicherheit und Freiheit 58
2. Voraussetzungen und Inhalt der Schutzpflicht 60
a) Der Tatbestand der Schutzpflicht 60
aa) Das grundrechtliche Schutzgut 60
bb) Der rechtswidrige Übergriff eines Privaten 61
b) Die Rechtsfolge der Schutzpflicht 64
3. Schutzpflichten nach dem Verfassungstext 66
a) Explizite Schutzpflichten im Grundrechtskatalog 66
b) Schutzpflichten als Schranken 67
c) Grundgesetzlicher Kompetenzkatalog und Landesverfassungen 68
d) Erweiterung durch objektiv-rechtliche Wertungsdimension 68
4. Die Rechtsprechung des Bundesverfassungsgerichts 69
a) Schwangerschaftsabbruch I und II 69
b) Die Schleyer-Entscheidung 70
c) Gefahrenquelle Technik 71
d) Datenschutz und allgemeines Persönlichkeitsrecht 73

D. Grundrechtlicher Persönlichkeitsschutz durch Datenschutz 76

I. Das allgemeine Persönlichkeitsrecht als Ausgangspunkt 76
II. Das Recht auf informationelle Selbstbestimmung 78
1. Das Volkszählungsurteil des Bundesverfassungsgerichts 79

2. Grundrechtliche Neuschöpfung 79
3. Konsequenzen des Urteils 82
4. Anlass zur umfassenden Verrechtlichung des Datenschutzes? 83
III. Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme 85
1. Die Entstehung des sogenannten IT-Grundrechts 85
2. Abgrenzung zur informationellen Selbstbestimmung 86
3. Vertraulichkeit und Integrität 87
a) Gewährleistung der Vertraulichkeit 88
b) Gewährleistung der Integrität 89
4. Einschränkbarkeit von Vertraulichkeit und Integrität 90
IV. Staatliche Schutzpflicht für informationstechnische Systeme 91
1. Tatbestand eines staatlichen Schutzauftrags 91
a) Die objektiv-rechtliche Dimension des Persönlichkeitsrechts 91
b) Bedeutung der informationellen Selbstbestimmung 93
c) Vertraulichkeit und Integrität informationstechnischer Systeme 96
aa) Entindividualisierung durch informationstechnische Systeme 97
bb) Das Angewiesensein auf informationstechnische Systeme 98
cc) Komplexität informationstechnischer Systeme 98
dd) Vertraulichkeits- und Integritätsschutz eigengenutzter Systeme 99
d) Tatbestandspräzision durch neue Schutzbereichsausprägung 100
e) Zwischenergebnis 101
2. Begründungsnotwendige Voraussetzungen 101
a) Erheblichkeit der Einwirkung 101
b) Begründung der Rechtswidrigkeit 103
aa) Die Verfassung als Rechtswidrigkeitsmaßstab 103
bb) Das allgemeine Persönlichkeitsrecht: Die freie Entfaltung der Persönlichkeit und die Würde des Menschen 104
cc) Differenzierung moderner Verkehrsinformationstechnologie 105

dd) Autonome Freiheitsausübung oder „gestörte Freiwilligkeit“? 107
(1) Inhalt und Reichweite der Privatautonomie 107
(2) „Plug and play-Falle“ 109
(3) Machtgefälle als Wirksamkeitshindernis 110
(4) „Gestörte Freiwilligkeit“ 111
(5) Digitale Emergenz 112
ee) Zwischenergebnis zur Rechtswidrigkeit des Übergriffs 112
(1) Notrufsystem eCall 113
(2) Sonstige fahrzeuginterne Informationstechnologie 115
(3) Vermeintliche Freiwilligkeit und faktischer Zwang 116
c) Praktikabilität der Einwilligung 118
d) Zwischenergebnis 122
3. Rechtsfolge für informationstechnische Systeme 123
a) Grundlegende Konturierung der Gewährleistungsverantwortung 123
b) Die Bedeutung multipolarer Rechtsverhältnisse 124
aa) Widerstreitende grundrechtliche Interessen 125
bb) Grundsätzliche Freiheit oder grundsätzliches Verbot 126
cc) Auswirkungen und Herausforderungen 127
c) Gesetzgeberischer Gestaltungsspielraum 128
d) Verfassungsgerichtlicher Kontrollmaßstab 130
V. Ergebnis auf Grundlage nationalen Verfassungsrechts 130

E. Bestandsaufnahme des nationalen Rechtsrahmens 132

I. Konkretisierung durch weitere Verfassungsnormen? 132
1. Sicherheitsanforderungen nach Art. 91 c GG 132
2. Gewährleistung nach Art. 87 f GG 133
II. Regelungen nach dem Bundesdatenschutzgesetz 133
1. Die Grundsätze des Datenschutzrechts 134
a) Datenvermeidung und Datensparsamkeit 134
b) Prinzip des Verbots mit Erlaubnisvorbehalt 135
c) Grundsatz der Zweckbindung 136
d) Grundsatz der Transparenz 137

2. Regelungen zum privaten Datenumgang 138
a) Allgemeine Bestimmungen nicht-öffentlicher Datenverarbeitung 138
b) § 6 a BDSG: Automatisierte Einzelentscheidung 139
c) § 9 BDSG: Technische und organisatorische Maßnahmen 142
d) § 9 a BDSG: Datenschutzaudit 145
e) Zulässigkeit der Datenverwendung im nicht-öffentlichen Bereich 146
aa) § 28 I BDSG: Datenverwendung für eigene Geschäftszwecke 147
(1) Rechtsgeschäftliches Schuldverhältnis 148
(2) Wahrung berechtigter Interessen 149
(3) Allgemein zugängliche Daten 150
bb) § 28 III BDSG: Adresshandel, Werbung und Koppelungsverbot 151
cc) § 28 b BDSG: Scoring 153
dd) § 29 BDSG: Geschäftsmäßige Datenverwendung 154
f) Sonstige Vorschriften 157
aa) § 33 BDSG: Benachrichtigung des Betroffenen 157
bb) § 34 BDSG: Auskunftsrecht des Betroffenen 157
cc) § 35 BDSG: Berichtigung, Löschung und Sperrung von Daten 158
3. Zwischenergebnis 159
III. Regelungen nach dem Telemediengesetz 162
1. Anwendungsbereich und Regelungsinhalte 163
2. Anlehnung an das allgemeine Datenschutzrecht 163
3. Konzeptioneller Selbst- und Systemdatenschutz 164
4. Zwischenergebnis 165
IV. Regelungen nach dem Telekommunikationsgesetz 165
1. Anwendungsbereich und Regelungsinhalte 166
2. Problemaufriss am Beispiel der Standortdaten 167
3. Zwischenergebnis 167
V. Gesetz über intelligente Verkehrssysteme 168
1. Regelungsinhalte 168
2. Europäische Richtlinie 2010/40/EU 169
3. Verordnungsermächtigung gemäß § 5 IVSG 169
4. Zwischenergebnis 169

VI. Bewertung des nationalen Rechtsrahmens 169

F. Persönlichkeitsschutz und Datenschutz nach europäischem Recht 172

I. Verhältnis von nationalem und europäischem Recht 172
1. Grundrechtsschutz und Ebenenpluralität 172
2. Einfluss und Entfaltung europäischen Rechts 174
3. Schnittstellen beider Rechtsordnungen 176
II. Europäische Schutzpflichtendimension 176
III. Überblick der europäischen Rechtslage 179
1. Primärrechtliche Bestandsaufnahme 179
a) Art. 16 AEUV 180
b) Art. 39 EUV 181
c) Charta der Grundrechte der Europäischen Union 181
aa) Art. 7 EU-GRCharta 181
bb) Art. 8 EU-GRCharta 182
d) Verfassungsüberlieferungen und allgemeine Rechtsgrundsätze 184
e) Zwischenergebnis 184
2. Sekundärrechtliche Bestandsaufnahme 185
a) Europäische Datenschutzgrundverordnung 186
aa) Amtliche Erwägungsgründe 186
bb) Allgemeine Bestimmungen 188
cc) Datenschutzgrundsätze 190
(1) Grundsätze für die Datenverarbeitung 190
(2) Rechtmäßigkeit der Datenverarbeitung 190
(3) Anforderungen an die Einwilligung 191
dd) Gewährung individuell-subjektiver Rechte 191
(1) Informationspflichten und Auskunftsrechte 191
(2) Automatisierte Einzelfallentscheidung und Profiling 192
(3) Das Recht auf Vergessenwerden 192
(4) Beschwerderecht gegenüber der Aufsichtsbehörde 194
ee) Datenschutz durch Technikgestaltung 194
ff) Kontrolle durch Aufsichtsbehörden 195
b) eCall-Verordnung 196
c) Richtlinienebene 197

d) Zwischenergebnis 199
3. Europäische Menschenrechtskonvention 202
a) Stellung auf europäischer Ebene 202
b) Innerstaatliche Wirkung 203
c) Gewährleistungen gemäß Art. 8 EMRK 204
4. Völkerrechtlicher Exkurs: Wiener Straßenverkehrskonvention 205
5. Europäische Rechtsprechung 206

G. Bewertung der Untersuchungsergebnisse 209

I. Die staatliche Infrastrukturgewährleistungsverantwortung 209
II. Inhalt und Umfang der Schutzpflicht 212
III. Würdigung der bisherigen Schutzmaßnahmen 213
IV. Ausblick 215

Literaturverzeichnis 221

Abkürzungsverzeichnis

aaO	am angegebenen Ort
ABl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGB	Allgemeine Geschäftsbedingungen
AfP	Archiv für Presserecht
AöR	Archiv des öffentlichen Rechts
Art.	Artikel
Aufl.	Auflage
BB	Betriebs-Berater
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Amtliche Entscheidungssammlung des Bundesgerichtshofs in Strafrecht
BGHZ	Amtliche Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT-Drucks.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Entscheidungssammlung des Bundesverfassungsgerichts
bzw.	beziehungsweise
CR	Computer und Recht
C’t	Magazin für Computertechnik
ders.	derselbe
dies.	dieselbe
DÖV	Die Öffentliche Verwaltung
DRIZ	Deutsche Richterzeitung
DSB	Datenschutz-Berater

DSG	Datenschutzgesetz
DuD	Datenschutz und Datensicherheit
DSGVO	Datenschutzgrundverordnung der Europäischen Union
DVBl	Das Deutsche Verwaltungsblatt
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EU-GRCharta	Charta der Grundrechte der Europäischen Union
EuR	Europarecht
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f./ff.	folgende
FAZ	Frankfurter Allgemeine Zeitung
Fn.	Fußnote
GASP	Gemeinsame Außen- und Sicherheitspolitik
GG	Grundgesetz
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GV NW	Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen
HGR	Handbuch der Grundrechte in Deutschland und Europa
Hrsg.	Herausgeber, herausgegeben von
HStR	Handbuch des Staatsrechts der Bundesrepublik Deutschland
i.B.a.	in Bezug auf
i.E.	im Ergebnis
insb.	insbesondere
i.S.v.	im Sinne von
ITRB	Der IT-Rechts-Berater
i.V.m.	in Verbindung mit
IVSG	Gesetz über intelligente Verkehrssysteme und deren Schnittstellen zu anderen Verkehrsträgern
Kfz	Kraftfahrzeug
KJ	Kritische Justiz
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
K&R	Kommunikation und Recht
LDSG	Landesdatenschutzgesetz
MMR	MultiMedia und Recht

m.w.N.	mit weiteren Nachweisen
NJW	Neue Juristische Wochenschrift
NW/NRW	Nordrhein-Westfalen
NZA	Neue Zeitschrift für Arbeitsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
RDV	Recht der Datenverarbeitung
RegE	Regierungsentwurf
Rn.	Randnummer
Rs.	Rechtssache
Rspr	Rechtsprechung
S.	Seite
sog.	sogenannte/r
st. Rspr.	ständige Rechtsprechung
StGB	Strafgesetzbuch
SVR	Straßenverkehrsrecht
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.a.	unter anderem
UN-ECE	United Nations Economic Commission for Europe
Vgl.	Vergleiche
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
VW	Versicherungswirtschaft
VSG	Verfassungsschutzgesetz
VZG	Volkszählungsgesetz
z.B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
ZfV	Zeitschrift für Versicherungswesen
ZNER	Zeitschrift für Neues Energierecht
ZSE	Zeitschrift für Staats- und Europawissenschaften

A. Einführung

I. Fortschritt durch Digitalisierung

Der moderne Mensch ist vernetzt, kommuniziert und präsentiert sich digital und entfaltet damit seine Persönlichkeit gänzlich konträr zu dem Menschen, wie ihn Rechtsprechung und Wissenschaft in einer scheinbar längst vergangenen Zeit zeichneten. Doch das Mehr an digitalen Möglichkeiten der Persönlichkeitsentfaltung bedeutet zugleich ein Mehr an Gefährdungspotenzial für den Persönlichkeitsschutz. Im Vergleich zu höchstrichterlichen Judikaten, die den Persönlichkeitsschutz prägten[1], hat sich die verfassungsrechtliche Problematik auf die Ebene privater Akteure verschoben. Denn es ist nicht (ausschließlich) der Staat, der im großen Stil die Daten der Nutzer sammelt und verwertet. Es sind Unternehmen wie *Facebook*, *Amazon* und *Google*, die uns Freunde und interessengerechte Produkte zum Kauf vorschlagen oder Recherchen im Internet mit meist erstaunlich treffsicheren Suchvorschlägen unterstützen. In einer Welt, die digital vernetzt ist und Daten auf der Grundlage von Algorithmen auswertet, können Menschen und deren Vorlieben, Eigenschaften und Neigungen gewissermaßen dechiffriert und lesbar gemacht werden.[2]

Die massenhafte Sammlung und Auswertung von Daten ist unter dem Schlagwort „Big Data“ zum Inbegriff einer Epoche der Informationsanalyse geworden, hat jedoch eine Achillesferse: den Persönlichkeitsschutz.[3] Big Data als disruptive Entwicklung, die immer größere, heterogene Datenmengen immer schneller und immer tiefgliedriger auswertbar macht und dadurch einen Paradigmenwechsel in der Datenverarbeitung einläutet: „Big Data ergänzt den Augenschein um Algorithmen, das Gedächtnis um Datenbanken und das Bauchgefühl um Statistik.“[4] Die wachsenden Möglichkeiten der Datenzusammenführungen und die Fähigkeit der Computersysteme Verfahrensweisen, Lage und Vorlieben der Nutzer zu analysieren

---

1 Als Beispiel seien hier genannt BVerfGE 65, 1; 120, 274; 120, 378.
2 Vgl. *Martini*, DVBl 2014, 1481 (1483) sowie *Brücher*, Rethink Big Data, S. 117 f.
3 Vgl. *Martini*, DVBl 2014, 1481 mit einem Plädoyer für ein Algorithmenkontrollrecht.
4 *Martini*, DVBl 2014, 1481 (1482).

und fruchtbar zu machen, lassen menschliches Handeln und Verhalten berechenbar werden.

Anschaulich wird dies etwa bei der sogenannten Autocomplete-Funktion von *Google*, wenn der Suchmaschinenbetreiber Benutzereingaben möglichst sinnvoll ergänzt. Dass Suchergänzungsvorschläge schnell in Widerspruch zu persönlichkeitsrechtlichen Interessen treten können, wurde in Deutschland in den letzten Jahren immer wieder deutlich.[5] Auch auf europäischer Ebene schärfte sich in der jüngeren Vergangenheit das Bewusstsein für den Datenschutz in Situationen mit digitalem Kontext. Der bereits genannte Suchmaschinenbetreiber muss in seinen Suchergebnissen personenbezogene Daten löschen, selbst wenn sie rechtmäßig erhoben wurden und weiterhin öffentlich zugänglich sind, denn das Recht auf Privatsphäre der EU-Bürger kann einen Anspruch auf Löschung aus den entsprechenden Suchergebnissen und Texten begründen, gar übergehen in das sogenannte Recht auf Vergessenwerden.[6]

Doch auch auf anderem Gebiet schreitet der Digitalisierungsprozess voran: Neue Technologien unterstützen die Krebsforschung und versetzen die Wissenschaft in die Lage Krebsregister zu erstellen, mobile Apps ermöglichen die permanente Kontrolle der eigenen Gesundheit und Versicherungen bieten vergünstigte Tarife an. Smartes Monitoring als Fernuntersuchung und -überwachung des Patienten, vorgenommen allerdings nicht vom Arzt, sondern durch einen Privatkonzern, an dessen Seite der Patient als Datenlieferant fungiert. Die gesellschaftlich zu beobachtende Tendenz ständiger Selbstoptimierung ermöglicht die digitale Erfassung von Körper- und Gesundheitsdaten im großen Stil. Da erscheint es nachvollziehbar, dass private Unternehmen wie Google Interesse daran haben in die Gesundheitssparte einzusteigen; im Oktober 2014 stellte das Internetdienstleistungsunternehmen ein Forschungsvorhaben vor, das mit Hilfe von Nanopartikeln im menschlichen Körper Herzkreislauferkrankungen und Krebs frühzeitig erkennen und damit die Heilungschancen erhöhen

---

5 Vgl. etwa BGHZ 197, 213, dort ging es um die Ergänzungsvorschläge „Scientology“ und „Betrug“; für eine rechtliche Analyse der Autocomplete-Funktion siehe *Kastl*, GRUR 2015, 136.

6 Vgl. EuGH, Urteil vom 13. Mai 2014, C-131/12, die Begrifflichkeit des Rechts auf Vergessenwerden wurde vor allem durch *Viktor Mayer-Schönberger* geprägt, siehe *ders*., Die Tugend des Vergessens in digitalen Zeiten, S. 6; siehe auch *Boehme-Neßler*, NVwZ 2014, 825.

will.[7] Eine Kontaktlinse, die den Blutzuckerspiegel des Trägers messen kann, ist ebenfalls in Planung.

Das „Internet der Dinge“[8] verfolgt eine umfassende Vernetzung von Alltagsgegenständen.[9] „Smart Home“ lautet ein weiteres wegweisendes Schlagwort und beschreibt die Vernetzung und Steuerung von Haushaltsgegenständen und Elektronik.[10] Mit diesem Modell lässt sich die komplexe Steuerung der eigenen vier Wände mit Hilfe modernster Technologie einfach und simpel handhaben. Für den Nutzer soll der Alltag an Komfort gewinnen, Sicherheit und Energieeinsparungen inklusive. Smart Home Systeme kontrollieren die Raumtemperatur, die Bewässerung des Gartens oder erkennen, ob ein Fenster oder eine Tür bei Abwesenheit im Haus geöffnet wurde. Diese Vorgänge können über das Smartphone oder jeden Computer via Internet gesteuert werden. Ein Bestandteil eines solchen hausinternen Netzwerkes können lernfähige Rauchmelder und Thermostate sein, wie sie etwa das kalifornische Unternehmen Nest Labs herstellt. Im Januar 2014 kaufte Google dieses Unternehmen. Die Raumthermostate, sogenannte „smart appliances“ für ein mitdenkendes Zuhause, werden über das Internet durch Algorithmen mit Sensoren gesteuert und regulieren die Wärme im Haus je nach Außentemperatur und Gewohnheiten der Hausbewohner. Dabei erlernt das Thermostat die Gewohnheiten des Nutzers und erstellt aus diesen und geographischen Grunddaten ein individuelles Anwenderprofil. Durch eine umfassende Vernetzung im Wohn- und Lebensbereich ist beispielsweise eine gezielte Suche nach Stromfressern oder gar das Erzwingen energieeinsparender Ziele denkbar.[11] Umfassende Kontrollmöglichkeiten der Umwelt sind mittlerweile nicht ausschließlich

---

7 Vgl. *Gropp*, Google sucht bald auch im menschlichen Körper, FAZ vom 30.10.2014, S. 22.

8 Zum Internet der Dinge i.B.a. die Vernetzung der Produktion und der Industrie siehe *Bräutigam/Klindt*, NJW 2015, 1137; zur Neuausrichtung von Versicherungsmodellen siehe *Naujoks/Matouschek*, VW 2015, 30; ferner *Forst*, BB 2014, 2293 im Kontext eines Rechts auf Vergessenwerden für Beschäftigte.

9 Die technische Grundlage der „zu erwartenden Durchdringung der Welt mit Informationstechnologie“ unter dem Schlagwort des Ubiquitous Computing skizziert *Mattern*, Die technische Basis für das Internet der Dinge, S. 39 ff.

10 Vgl. *Rüdiger*, RDV 2014, 253, der beschreibt, wie dieses Wohnsystem im Alltag aussehen kann.

11 Vgl. *Rüdiger*, RDV 2014, 253 (258).

Bestandteil belletristischer Zukunftsvisionen[12], sondern bereits Realität. Das Problem bei all diesen Beispielen: Zwischen der Bedeutung von Einschränkungen grundrechtlich gewährleisteter Freiheiten und dem Verständnis der Nutzer über Umfang und Auswirkungen dieser Einschränkungen existiert ein Ungleichgewicht.

II. Gefährdungslage: Vernetztes Fahrzeug und intelligentes Verkehrssystem

Die vorliegende Bearbeitung zieht ein Fallbeispiel aus dem alltäglichen Leben heran, das nicht zuletzt wegen des großen Identifikationspotenzials und der breiten Inanspruchnahme gerade in der deutschen Bevölkerung als Ausdruck der Persönlichkeitsgefährdung bewusst gewählt wurde: Das vernetzte Fahrzeug, oftmals auch unter dem englischen Schlagwort „Connected Car“ bekannt und das damit eng verbundene intelligente Verkehrssystem. In beiden Fällen agiert der Einzelne als Fahrer und Teilnehmer des Straßenverkehrs als Datenlieferant. Rechtlicher Ausgangspunkt der Untersuchung sollen zwei Ausformungen des allgemeinen Persönlichkeitsrechts sein: Das Recht auf informationelle Selbstbestimmung und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Fahrzeuge und Verkehrssysteme können im 21. Jahrhundert intelligent sein; das jedenfalls versprechen die Hersteller und die Automobilbranche. Denn das moderne Auto ist vernetzt, es kann mit der Umwelt, der Infrastruktur und dem Internet kommunizieren. Möglich wird dies durch im Kfz eingebaute Sensoren und andere Techniken, die ihrerseits mit technischen Einrichtungen in der Umgebung (z.B. Parkleitsystemen oder automatischen Wechselverkehrszeichen über Autobahnen) interaktionsfähig sind und somit eine Vielzahl sogenannter intelligenter Verkehrssysteme darstellen. Abhängig von Hersteller und Ausstattung des jeweiligen Fahrzeugs können beispielsweise Reifendrehzahl, Temperatur und Geschwindigkeit kontinuierlich gemessen werden, weitere Sensoren des Bremssystems und der elektronischen Stabilitätskontrolle kommen hinzu. Dank dieser Möglichkeiten existieren zahlreiche Assistenztechniken. Der Fahrer

12 Exemplarisch sei hier der Roman „Der Circle“ von *Dave Eggers* genannt (10. Aufl. 2015).

kann die Hilfe von Abstandswarnsystemen, Aufmerksamkeits-, Spurhalte- und Totwinkel-Assistenten sowie Brems- und Einpark-Assistenten beanspruchen; Autofahren wird sicherer und komfortabler.

Doch Sicherheit und Komfort haben ihren Preis, denn die Kommunikationssysteme nähren sich von personenbezogenen Daten. Schon heute kann man sich dieser generellen Kommunikationsfähigkeit auf vier Rädern kaum mehr entziehen. Mag beim Kauf eine bewusste Entscheidung gegen die modernen Technologien noch möglich sein, so wird nach jetzigem Stand diese Möglichkeit spätestens ab April 2018 durch die Einführung des verpflichtenden und europaweiten automatischen Notrufsystems eCall passé sein.[13] Dann müssen nach dem europäischen Vorhaben alle Neuwagen mit einer eigenen SIM-Karte ausgestattet werden, die sich bei einem Unfall automatisch über das Mobilfunknetz mit der nächstgelegenen Notrufstelle verbindet und dabei alle notwendigen Rettungsdaten übermittelt.[14] Gehört die Zeit, in der das Auto ein privater Rückzugsort, ein überwachungsfreier Lebensbereich der eigenen Privatsphäre war, also der Vergangenheit an – vorbei die Zeit, in der das Auto der Inbegriff von Freiheit und Ungebundenheit war?[15]

Zur Geburtsstunde des Rechts auf informationelle Selbstbestimmung (und auch in der Folgezeit der „Erfindung" des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme) beherrschte der Staat als Datensammler und Datenverwender das juristische und gesellschaftliche Denken. Die Verschiebung entsprechend des Orwell'schen Entwurfs auf die Ebene privater Akteure verlangt eine neue Betrachtung der grundrechtlichen Schutzidee – unter besonderer Berücksichtigung der Verflechtungen nationalstaatlicher und europäischer Rechts- und Kompetenzordnungen. Die vorliegende Untersuchung wird daher der Frage nachgehen, inwiefern dem Staat Schutzpflichten im Mehrebenensystem für informationstechnische Systeme, bzw. für deren Nutzer, erwachsen können. Dabei kann keine umfassende Lösung präsentiert, son-

---

13 Alle neuen Modelle von Pkw und leichten Nutzfahrzeugen müssen bis zum 31. März 2018 mit dem eCall-System ausgestattet sein, vgl. die Pressemitteilung des Europäischen Parlaments vom 28.04.2015, http://www.europarl.europa.eu/news/de/press-room/20150424IPR45714/ecall-automatisches-notrufsystem-in-allen-neuen-automodellen-ab-fruhling-2018 (zuletzt abgerufen am 27. November 2017).

14 Vgl. *Lüdemann/Sengstacken*, RDV 2014, 177 (178); innerhalb Deutschlands ergibt sich die nächstgelegene Notrufstelle aus §§ 2 a Nr. 2, 3 I NotrufV.

15 Vgl. *Lüdemann*, ZD 2015, 247; *Weichert*, SVR 2014, 201 (202); *Demuth*, DRiZ 2015, 158.