Schriften zum Öffentlichen Recht

Band 1304

Grundrechtlicher Schutz informationstechnischer Systeme

Unter besonderer Berücksichtigung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Von

Marcus Heinemann

Duncker & Humblot · Berlin

MARCUS HEINEMANN

Grundrechtlicher Schutz informationstechnischer Systeme

Schriften zum Öffentlichen Recht

Band 1304

Grundrechtlicher Schutz informationstechnischer Systeme

Unter besonderer Berücksichtigung
des Grundrechts auf Gewährleistung
der Vertraulichkeit und Integrität
informationstechnischer Systeme

Von

Marcus Heinemann

Duncker & Humblot · Berlin

Die Juristische Fakultät
der Universität Passau
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.

Fremddatenübernahme: Konrad Triltsch GmbH, Ochsenfurt
Druck: CPI buchbücher.de, Birkach
Printed in Germany

ISSN 0582-0200
ISBN 978-3-428-14485-3 (Print)
ISBN 978-3-428-54485-1 (E-Book)
ISBN 978-3-428-84485-2 (Print & E-Book)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier
entsprechend ISO 9706 ♾

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

Vorwort

Das vorliegende Werk trägt den zunächst möglicherweise irritierenden Titel „Grundrechtlicher Schutz informationstechnischer Systeme“. Der grundrechtliche Schutz kommt jedoch keinen Objekten zugute, sondern allein den grundrechtlich Berechtigten. Die Arbeit möchte demzufolge einen Beitrag zur Diskussion um die grundrechtliche Schutzbedürftigkeit der im Kontext der Nutzung informationstechnischer Systeme betroffenen Grundrechtsträger leisten.

Mittels zugriffsbezogener Analyse werden die zahlreichen tatsächlichen wie rechtlichen Gefährdungslagen bei der Verwendung informationstechnischer Systeme aufgezeigt und die damit einhergehenden grundrechtlichen Problemstellungen konkretisiert. Besondere Beachtung erfährt hierbei das vom BVerfG am 27. Februar 2008 entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Auch rund sieben Jahre nach dieser Entscheidung des BVerfG zum sog. „IT-Grundrecht“ hat diese Thematik nicht an Aktualität eingebüßt.

Die vorliegende Arbeit wurde im Herbst 2013 als Dissertation an der Juristischen Fakultät der Universität Passau eingereicht. Die Disputation fand am 5. August 2014 statt.

Mein herzlicher Dank gilt Herrn Prof. Dr. Urs Kramer für die menschlich wie fachlich vorbildliche Betreuung während des gesamten Promotionsverfahrens. Herrn Prof. Dr. Gerrit Hornung, LL.M. (Edinburgh), danke ich sehr für die zeitnahe Erstellung des Zweitgutachtens. Ausdrücklich bedanke ich mich auch bei meinen Eltern für ihre umfangreiche Förderung. Schließlich danke ich insbesondere Frau Ivonne Bauer, Frau Dipl.-Kffr. Aleksandra Gaus und Herrn Arian Nazari-Khanachayi, LL.M. Eur, für ihre fortwährende ermutigende Unterstützung.

Hamburg, im Frühjahr 2015 *Marcus Heinemann*

Inhaltsverzeichnis

A. Problemaufriss: Informationstechnische Gefährdungslagen 21

I. Informationstechnischer Fortschritt 21

II. Gefährdungslagen 22

III. Verfassungsrechtliche Herausforderungen 25
1. Neue Aufgaben 25
2. Neues Grundrecht 26

IV. Fortgang der Untersuchung 28

B. Charakteristika informationstechnischer Systeme 30

I. Grundbegriffe 30
1. Daten und Informationen 30
a) Definitionen 31
aa) Informationstechnische Definitionen 31
bb) Rechtliche Definitionen 31
b) Dimensionen 33
aa) Nachrichtentechnische Dimension 33
bb) Semiotische Dimension 33
cc) Zweckorientierte Dimension 34
dd) Rechtliche Dimension 35
2. Informationstechnik 36
3. Informations- und Kommunikationstechnik 37

II. Elemente und Funktionen informationstechnischer Systeme 37
1. Terminus „Informationstechnisches System“ 37
a) Informationstechnische Definitionen 38
b) Rechtliche Definitionen 39
2. Informationstechnische Bestandsaufnahme 41
a) Elemente 41
aa) Hard- und Software 41
bb) Entwicklungstendenzen 42
(1) Cloud Computing 43

(2) Ubiquitous Computing 43
b) Funktionen 45
3. Rechtliche Bestandsaufnahme 46
a) Elemente 46
aa) Anfallende Daten 46
(1) Inhaltsdaten 47
(2) Bestandsdaten 48
(3) Zugangsdaten 48
(4) Verkehrsdaten 48
(5) Nutzungsdaten 49
(6) Standortdaten 49
bb) Bezüge zur Persönlichkeit 49
(1) Personenbezogene Daten 50
(2) Personenbezug anfallender Daten 51
b) Funktionen 52

III. Kategorien informationstechnischer Systeme 53
1. Rechner 54
a) Personalcomputer 54
b) Mobile Speichermedien 55
2. Rechnerverbünde 55
a) Netzwerke 56
b) Internet 58
aa) World Wide Web 59
bb) Dateitransfer 59
cc) E-Mail-Kommunikation 60
dd) Newsgroups 61
ee) Chat-Kommunikation 61
ff) Voice over Internet Protocol-Kommunikation 62
gg) Soziale Netzwerke 63
hh) Streaming 63
ii) Remote Access 63
3. Mobile Kommunikationsgeräte 64
a) Mobiltelefone 64
b) Personal Digital Assistants 65
c) Smartphones 65
4. Mikrochip-Techniken 66
a) Radio Frequency Identification-Techniken 66
b) Medizinische Implantat-Techniken 67

5. Elektronische Smartcards 67
a) Elektronischer Personalausweis 67
b) Elektronische Gesundheitskarte 68
6. „Intelligente“ Wohnumgebungen 69
a) „Intelligente“ Hausanlagen 69
b) „Intelligente“ Haushaltsgeräte 69

IV. Anwendungsbezogene Interessen und Erwartungen 70
1. Terminus „Sicherheit in der Informationstechnik“ 71
2. Informationstechnische Bestandsaufnahme 73
a) Verlässlichkeit 73
aa) Verfügbarkeit 73
bb) Vertraulichkeit 74
cc) Integrität 75
b) Beherrschbarkeit 76
aa) Zurechenbarkeit 76
bb) Rechtsverbindlichkeit 77
3. Rechtliche Bestandsaufnahme 78
a) Verlässlichkeit 78
aa) Verfügbarkeit 78
bb) Vertraulichkeit 79
cc) Integrität 79
b) Beherrschbarkeit 80

C. Zugriffsmöglichkeiten auf informationstechnische Systeme 82

I. Tatsächliche und rechtliche Zugriffsmöglichkeiten 82
1. Lokaler Zugriff und lokaler Fernzugriff 82
a) Tatsächliche Zugriffsmöglichkeiten 82
b) Rechtliche Zugriffsmöglichkeiten 84
aa) Präventive Befugnisse 84
bb) Repressive Befugnisse 85
2. Online-Durchsuchung 85
a) Tatsächliche Zugriffsmöglichkeiten 85
aa) Infiltrationsphase 86
(1) Manuelle Installation 86
(2) „Man-In-The-Middle-Angriff“ 87
(3) Ausnutzen von Sicherheitslücken 87
(4) Installation durch Manipulation 88
bb) Durchsichts- bzw. Überwachungsphase 90
cc) De-Infiltrationsphase 91

dd) Exkurs: Messung physikalischer Abstrahlung 92
b) Rechtliche Zugriffsmöglichkeiten 93
aa) Präventive Befugnisse 93
(1) Landesrecht 93
(a) Bayern 93
(b) Rheinland-Pfalz 94
(2) Bundesrecht 94
bb) Repressive Befugnisse 95
(1) §§ 102 ff. StPO 95
(2) § 100a StPO 95
(3) § 100c StPO 96
(4) § 100h StPO, § 110a StPO oder §§ 161, 163 StPO 96
(5) §§ 102 ff. in Verbindung mit §§ 100a, 100c StPO 97
(6) § 100k StPO-E 97
3. Quellen-Telekommunikationsüberwachung 98
a) Tatsächliche Zugriffsmöglichkeiten 98
b) Rechtliche Zugriffsmöglichkeiten 98
aa) Präventive Befugnisse 98
(1) Landesrecht 98
(a) Bayern 98
(b) Rheinland-Pfalz 99
(c) Hessen 99
(d) Niedersachsen 100
(e) Thüringen 100
(2) Bundesrecht 100
bb) Repressive Befugnisse 101
4. Überwachung der E-Mail-Kommunikation 102
a) Tatsächliche Zugriffsmöglichkeiten 102
b) Rechtliche Zugriffsmöglichkeiten 102
aa) Präventive Befugnisse 102
(1) Landesrecht 102
(a) Bayern 102
(b) Rheinland-Pfalz 103
(c) Hessen 103
(d) Niedersachsen 103
(e) Thüringen 104
(2) Bundesrecht 104
bb) Repressive Befugnisse 104
5. Recherche in weiteren Internetdiensten 106
a) Tatsächliche Zugriffsmöglichkeiten 106

b) Rechtliche Zugriffsmöglichkeiten 107
aa) Präventive Befugnisse 107
bb) Repressive Befugnisse 109
6. Erhebung nicht-inhaltsbezogener Daten 109
a) Tatsächliche Zugriffsmöglichkeiten 109
b) Rechtliche Zugriffsmöglichkeiten 111
aa) Präventive Befugnisse 113
(1) Landesrecht 113
(2) Bundesrecht 114
bb) Repressive Befugnisse 114

II. Bedeutung des völkerrechtlichen Territorialgrundsatzes 115
1. Zugriffsmöglichkeiten auf gesicherte Quellen im Ausland 116
2. Zugriffsmöglichkeiten auf offene Quellen im Ausland 117
3. Konsequenzen für staatliche Zugriffsmöglichkeiten 118

D. Grundrechtsrelevanz staatlicher Zugriffsmöglichkeiten 119

I. Kein Grundrechtsverzicht durch Internetanschluss 119

II. Betroffene Grundrechte zum besonderen „Privatsphärenschutz“ 120
1. Unverletzlichkeit der Wohnung 121
a) Grundrechtlicher Schutzbereich 121
aa) Sachlicher Schutzbereich 121
bb) Personeller Schutzbereich 122
b) Staatliche Zugriffe als Grundrechtseingriffe 123
aa) Betreten und Durchsuchen von Räumen 123
bb) Lokaler Zugriff und lokaler Fernzugriff 124
cc) Online-Durchsuchung 125
dd) Verwendung erhobener Daten 126
c) Lücken der Unverletzlichkeit der Wohnung 127
2. Unverletzlichkeit des Fernmeldegeheimnisses 128
a) Grundrechtlicher Schutzbereich 128
aa) Sachlicher Schutzbereich 128
bb) Personeller Schutzbereich 128
b) Staatliche Zugriffe als Grundrechtseingriffe 129
aa) Zugriff auf laufende Kommunikationsinhalte 129
bb) Zugriff auf gespeicherte Kommunikationsinhalte 130
cc) Zugriff auf weitere Kommunikationsdaten 132
dd) Online-Durchsuchung 134
ee) Verwendung erhobener Daten 135
c) Lücken der Unverletzlichkeit des Fernmeldegeheimnisses 135

3. Ausprägungen des allgemeinen Persönlichkeitsrechts 136
a) Konkurrenzen zu den anderen Grundrechten 136
b) Schutz der Privatsphäre 137
c) Recht auf informationelle Selbstbestimmung 139
aa) Grundrechtlicher Schutzbereich 139
(1) Sachlicher Schutzbereich 139
(2) Personeller Schutzbereich 139
bb) Staatliche Zugriffe als Grundrechtseingriffe 140
(1) Mitschnitt von Raumgesprächen 140
(2) Datenerhebung aus gesicherten Quellen 141
(3) Datenerhebung aus offenen Quellen 143
(4) Online-Durchsuchung 145
(5) Verwendung erhobener Daten 146
cc) Lücken des Rechts auf informationelle Selbstbestimmung 146
d) IT-Grundrecht 147
aa) Erforderlichkeit des IT-Grundrechts 147
bb) Grundrechtlicher Schutzbereich 148
(1) Sachlicher Schutzbereich 148
(a) Vertraulichkeit 148
(b) Integrität 149
(c) Informationstechnische Systeme 151
(aa) Personenbezogene Daten 151
(bb) Verarbeitungskapazitäten 151
(2) Personeller Schutzbereich 153
(a) Nutzungsabhängigkeit 153
(b) Eigennutzung 154
(3) Kategorien informationstechnischer Systeme 156
(a) Rechner 156
(aa) Personalcomputer 156
(bb) Mobile Speichermedien 157
(b) Rechnerverbünde 158
(c) Mobile Kommunikationsgeräte 159
(d) Mikrochip-Techniken 161
(aa) Radio Frequency Identification-Techniken 161
(bb) Medizinische Implantat-Techniken 163
(e) Elektronische Smartcards 164
(aa) Elektronischer Personalausweis 164
(bb) Elektronische Gesundheitskarte 165
(f) „Intelligente“ Wohnumgebungen 166

cc) Staatliche Zugriffe als Grundrechtseingriffe 167
(1) Lokaler Zugriff und lokaler Fernzugriff 167
(2) Online-Durchsuchung 168
(3) Quellen-Telekommunikationsüberwachung 168
(4) Überwachung der E-Mail-Kommunikation 169
(5) Recherche in weiteren Internetdiensten 170
(6) Verwendung erhobener Daten 170

III. Betroffene Grundrechte außerhalb des besonderen „Privatsphärenschutzes“ 171
1. Recht auf körperliche Unversehrtheit 171
2. Glaubensfreiheit 171
3. Meinungsfreiheit 172
4. Informationsfreiheit 172
5. Pressefreiheit 173
6. Schutz von Ehe und Familie 173
7. Versammlungsfreiheit 174
8. Vereinigungsfreiheit 174
9. Recht auf Freizügigkeit 174
10. Berufsfreiheit 175
11. Eigentumsgarantie 177
12. Allgemeine Handlungsfreiheit 178

E. Rechtfertigung staatlicher Eingriffe in das IT-Grundrecht 179

I. Schranken des IT-Grundrechts 179
1. Schranken des allgemeinen Persönlichkeitsrechts 179
2. Bedeutung des Grundsatzes des Vorbehalts des Gesetzes 181

II. Schranken-Schranken des IT-Grundrechts 181
1. Bestimmtheitsgrundsatz 181
a) Inhalt des Bestimmtheitsgrundsatzes 181
b) Konsequenzen für das IT-Grundrecht 183
2. Zitiergebot 184
3. Grundsatz der Verhältnismäßigkeit 185
a) Legitimer Zweck 185
b) Geeignetheit 186
c) Erforderlichkeit 187
d) Angemessenheit 188
aa) Maßgebliche Eingriffsschwellen 189
(1) Präventive Eingriffsschwellen 190
(a) Verdeckte Zugriffe 190
(aa) Anforderungen des Bundesverfassungsgerichts 190

(bb) Bestehende gesetzliche Regelungen 193
(cc) Konsequenzen für verdeckte Zugriffe 193
(b) Offene Zugriffe 194
(aa) Bestehende gesetzliche Regelungen 194
(bb) Konsequenzen für offene Zugriffe 194
(2) Repressive Eingriffsschwellen 195
(a) Verdeckte Zugriffe 195
(aa) Bestehende gesetzliche Regelungen 195
(bb) Konsequenzen für verdeckte Zugriffe 196
(b) Offene Zugriffe 198
(aa) Bestehende gesetzliche Regelungen 198
(bb) Konsequenzen für offene Zugriffe 198
bb) Vorherige unabhängige Kontrolle 200
4. Unantastbarer Kernbereich privater Lebensgestaltung 202
a) Schutzgehalt des Kernbereichs privater Lebensgestaltung 202
aa) Garantie der Menschenwürde 202
bb) Wesensgehalt der Grundrechte 203
b) Ausgestaltung als zweistufiges Schutzkonzept 204
aa) Erhebungsphase 204
bb) Auswertungsphase 206
c) Hinreichende Effektivität des zweistufigen Schutzkonzepts 206

F. Objektiv-rechtliche Dimensionen des IT-Grundrechts 209

I. Schutzgehalte für grundrechtlich gesicherte Rechtsgüter 209
1. Förderung sicherer informationstechnischer Systeme 211
2. Normative Strategie der Sicherheit in der Informationstechnik 212

II. Ausstrahlungswirkungen auf die gesamte Rechtsordnung 214
1. Ausstrahlungswirkung auf § 823 Abs. 1 BGB 215
2. Ausstrahlungswirkung auf das Arbeitsrecht 215

III. Organisations- und Verfahrensgehalte 216
1. Gebot der Zweckbindung 217
2. Auskunfts- und Löschungspflichten 218
3. Garantie effektiven Rechtsschutzes 218

IV. Einrichtungsgarantien 220

G. Europarechtlicher Schutz informationstechnischer Systeme 222

I. Rechtshistorischer und -dogmatischer Hintergrund 222

II. Rechtserkenntnisquellen und europäische Grundrechtskodifikationen 224
1. Gemeinsame Verfassungsüberlieferungen 224
2. Art. 8 EMRK 225
3. Art. 7 EGRC und Art. 8 EGRC 226

III. Grundrechte nach der Rechtsprechung des Europäischen Gerichtshofs 227

IV. Geltungsabgrenzung zu den nationalen Grundrechten 228

H. Zusammenfassung der Untersuchungsergebnisse 230

Literatur- und Quellenverzeichnis 233

Sachwortverzeichnis 250

Abkürzungsverzeichnis

a. A.	andere Ansicht
a. F.	alte Fassung
ABl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AG	Amtsgericht
Anm.	Anmerkung
AnwBl	Anwaltsblatt
AöR	Archiv des öffentlichen Rechts
APuZ	Aus Politik und Zeitgeschichte
ARPANET	Advanced Research Projects Agency Network
Art.	Artikel
Aufl.	Auflage
AuR	Arbeit und Recht
Az.	Aktenzeichen
BayPAG	Gesetz über die Aufgaben und Befugnisse der bayerischen staatlichen Polizei
BayVBl.	Bayerische Verwaltungsblätter
BayVSG	Bayerisches Verfassungsschutzgesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BPolG	Gesetz über die Bundespolizei
BR	Bundesrat
BRAO	Bundesrechtsanwaltsordnung
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BV	Verfassung des Freistaates Bayern
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
bzw.	beziehungsweise
CD-ROM	Compact Disc Read-Only Memory
CERN	Organisation Européenne pour la Recherche Nucléaire
CIX	Commercial Internet Exchange

CR	Computer und Recht
DIN	Deutsches Institut für Normung
DNS	Domain Name System
DÖV	Die Öffentliche Verwaltung
DRiZ	Deutsche Richterzeitung
Drucks.	Drucksache
DStR	Deutsches Steuerrecht
DuD	Datenschutz und Datensicherheit
DVBl	Deutsches Verwaltungsblatt
DVD	Digital Video Disc
E	Electronic / Entwurf
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EGRC	Charta der Grundrechte der Europäischen Union
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EuGRZ	Europäische Grundrechte-Zeitschrift
EuR	Europarecht
Europol	Europäisches Polizeiamt
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
f. / ff.	folgend/e
FAZ	Frankfurter Allgemeine Zeitung
Fn.	Fußnote/n
FS	Festschrift
FTP	File Transfer Protocol
GA	Goltdammer's Archiv für Strafrecht
GG	Grundgesetz für die Bundesrepublik Deutschland
GPS	Global Positioning System
GRR	Grundrechte-Report
GSM	Global System for Mobile Communications
GVBl.	Gesetz- und Verordnungsblatt
HdbGR	Handbuch der Grundrechte in Deutschland und Europa
HdbStR	Handbuch des Staatsrechts der Bundesrepublik Deutschland
HFR	Humboldt Forum Recht
HRRS	Höchstrichterliche Rechtsprechung im Strafrecht
Hrsg.	Herausgeber
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IEC	International Elektrotechnical Commission
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
Interpol	Internationale kriminalpolizeiliche Organisation
IP	Internet Protocol

IRC	Internet Relay Chat
ISO	International Organization for Standardization
IT-Grundrecht	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
IT-Sicherheit	Sicherheit in der Informationstechnik
JA	Juristische Arbeitsblätter
JR	Juristische Rundschau
Jura	Juristische Ausbildung
jurisPR-ITR	juris PraxisReport IT-Recht
JuS	Juristische Schulung
JZ	Juristenzeitung
K&R	Kommunikation & Recht
KritV	Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft
LAN	Local Area Network
LG	Landgericht
lit.	Buchstabe
LKRZ	Zeitschrift für Landes- und Kommunalrecht Hessen, Rheinlad-Pfalz, Saarland
LKV	Landes- und Kommunalverwaltung
LT	Landtag
m. w. N.	mit weitere/m/n Nachweis/en
MAC	Media Access Control
MB	Megabyte
MMR	Multimedia und Recht
NdsSOG	Niedersächsisches Gesetzt über die öffentliche Sicherheit und Ordnung
NdsVBl.	Niedersächsische Verwaltungsblätter
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NNTP	Network News Transfer Protocol
Nr.	Nummer/n
NSA	National Security Agency
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Verwaltungszeitschrift
NVwZ-RR	NVwZ-Rechtsprechungs-Report Verwaltungsrecht
NWVBl.	Nordrhein-Westfälische Verwaltungsblätter
NZS	Neue Zeitschrift für Sozialrecht
OSI	Open Systems Interconnection
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
P&P	Poiesis & Praxis
PAuswG	Gesetz über Personalausweise und den elektronischen Identitätsnachweis
PIN	Personal Identity Number
POG RLP	Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz
POP	Post Office Protocol
Quellen-TKÜ	Quellen-Telekommunikationsüberwachung
RDP	Remote Desktop Protocol
RDV	Recht der Datenverarbeitung
RFID	Radio Frequency Identification
Rn.	Randnummer/n

RTCP	Real-Time Control Protocol
RTSP	Real-Time Streaming Protocol
RTTP	Real-Time Transport Protocol
RuP	Recht und Politik
RW	Rechtswissenschaft
S.	Seite/n
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
Slg.	Sammlung
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
sog.	sogenannte/n/r
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StraFo	Strafverteidiger-Forum
StV	Strafverteidiger
TCP	Transmission Control Protocol
Telnet	Telecommunication Network
ThürPAG	Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei
ThürVBl.	Thüringer Verwaltungsblätter
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UDP	User Datagram Protocol
UIG	Umweltinformationsgesetz
UMTS	Universal Mobile Telecommunications System
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte
URL	Uniform Resource Locator
USB	Universal Serial Bus
Usenet	User Network
Var.	Variante
VBlBW	Verwaltungsblätter für Baden-Württemberg
VDI	Verein Deutscher Ingenieure
VerwArch	Verwaltungsarchiv
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
vgl. / Vgl.	vergleiche / Vergleiche
VIG	Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformation
VO	Verordnung
VoIP	Voice over Internet Protocol
Vorb.	Vorbemerkung/en
VSG NRW	Gesetz über den Verfassungsschutz in Nordrhein-Westfalen
VVHSOG	Verwaltungsvorschrift zur Ausführung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung
WAN	Wide Area Network

WLAN	Wireless Local Area Network
WM	Zeitschrift für Wirtschafts- und Bankrecht
WWW	World Wide Web
z. B.	zum Beispiel
ZRP	Zeitschrift für Rechtspolitik
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft
ZUM	Zeitschrift für Urheber- und Medienrecht

A. Problemaufriss: Informationstechnische Gefährdungslagen

I. Informationstechnischer Fortschritt

Der informationstechnische Fortschritt mit seinen vielfältigen Informations- und Kommunikationsmöglichkeiten ist unaufhaltsam. Maßgebliche Bedeutung kommt hierbei dem Internet zu, dessen Ursprünge bis in das Jahr 1969 zurückreichen. Damals wurde mit dem Advanced Research Projects Agency Network (ARPANET) ein telefonleitungsgebundenes dezentrales Netzwerk für alle für das amerikanische Verteidigungsministerium forschenden Universitäten verwirklicht. Der Internetdienst World Wide Web (WWW) wurde erstmals im Jahr 1989 als Projekt der schweizerischen Organisation Européenne pour la Recherche Nucléaire (CERN) in Genf präsentiert und im Jahr 1991 weltweit zur allgemeinen Nutzung freigegeben.[1]

Im Jahr 2008 benutzten in der Bundesrepublik Deutschland bereits knapp zwei Drittel der Bevölkerung das Internet.[2] Infrastrukturelles Ziel der Bundesregierung bis zum Jahr 2014 war der Anschluss von drei Vierteln der Bevölkerung an schnelle Netze mit Datenübertragungsraten von über 50 Megabit pro Sekunde.[3] Flächendeckend soll dieses Ziel bis zum Jahr 2018 erreicht werden.[4]

Informationstechnik durchdringt derweil alle Lebensbereiche. Informationstechnische Systeme sind allgegenwärtig, und ihre Nutzung für die Lebensführung vieler Bürger ist von zentraler Bedeutung.[5] Neben im Internet veröffentlichten multimedialen Kommunikationsinhalten werden in zahlreichen Lebenslagen autarke wie vernetzte informationstechnische Systeme verwendet, vom multifunktionalen Smartphone bis zu Radio Frequency Identification (RFID)-Funketiketten auf der Milchtüte.[6] Wesentliche Charakteristika informationstechnischer Systeme sind ihr

---

[1] Zur geschichtlichen Entwicklung des Internets siehe etwa *Weichert*, DuD 2009, 7; *Böckenförde*, Die Ermittlung im Netz, S. 40.

[2] Vgl. *Worms*, RuP 2009, 138; *Finsterbusch*, FAZ vom 23.08.2008, S. 14.

[3] Vgl. *Leutheusser-Schnarrenberger*, K&R 2010, Nr. 1, Editorial; die Datenmenge von 50 Megabit entspricht umgerechnet 6,25 Megabyte (MB).

[4] Vgl. Bundesministerium für Wirtschaft und Energie, Digitale Agenda 2014-2017, S. 9.

[5] Vgl. BVerfGE 120, 274, 303.

[6] Vgl. *Bittner*, FAZ vom 04.03.2008, S. 13.

zunehmender Miniaturisierungs- und Vernetzungsgrad sowie die Allgegenwärtigkeit ihrer Dienste.[7]

II. Gefährdungslagen

Die mit dem informationstechnischen Fortschritt wachsende Abhängigkeit von der alltäglichen Verfügbarkeit informationstechnischer Systeme birgt zugleich neue Gefährdungslagen.

So führt die zunehmende informationstechnische Vernetzung zur enormen Erweiterung kritischer Infrastrukturen. Zu diesen kritischen Infrastrukturen zählen alle für das staatliche Gemeinwesen wichtigen Organisationen und Einrichtungen (z. B. die Telekommunikation, das Transportwesen und die Stromversorgung), deren Ausfall oder Beeinträchtigung zu nachhaltigen Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen dramatischen Folgen führen können.[8] Tatsächlich hat sich dieses Gefährdungspotenzial in den letzten Jahren bereits mehrfach gezeigt. Zu nennen sind etwa der Angriff auf das Flugkontrollsystem des Flughafens Worcester in Amerika im März 1997, die Einspeisung des Schadprogramms „Sasser" in das Internet ab dem Jahr 2004 oder großflächige „Denial-of-Service-Angriffe"[9] auf staatliche wie private vernetzte informationstechnische Systeme in Estland im Frühjahr 2007 und in Georgien im Herbst 2008.[10] Solche informationstechnischen Manipulationen bewirken schnell wirtschaftliche Störungsschäden in Millionenhöhe.

Im privaten Bereich sieht sich der Einzelne ebenso weitreichenden Gefährdungslagen ausgesetzt. So kann die bestimmungsgemäße Funktionsfähigkeit eingesetzter informationstechnischer Systeme durch unbemerkt oder leichtfertig mittels elektronischer Kommunikation eingeschleuste Trojaner bedroht werden. Diese als nützliche Dienste getarnten Schadprogramme können im Hintergrund und ohne Wissen des Nutzers andere Funktionen erfüllen, die bis zur heimlichen Steuerungsübernahme des informationstechnischen Systems samt der angeschlossenen Peripheriegeräte reichen können.[11]

---

[7] Zum informationstechnischen Fortschritt auch *Schaar*, in: Vieweg/Gerhäuser (Hrsg.), Digitale Daten in Geräten und Systemen, S. 61, 63.

[8] Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, S. 39 und 77; zum Begriff „Kritische Infrastrukturen" ausführlich auch *Möllers/Pflug*, in: Kloepfer (Hrsg.), Schutz kritischer Infrastrukturen, S. 47, 49 ff.

[9] Bei „Denial-of-Service-Angriffen" werden einzelne vernetzte informationstechnische Systeme derart mit externen Anfragen „bombardiert", dass es zur Störung der Verfügbarkeit der Angriffsobjekte kommt; vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2009, S. 76.

[10] Zu diesen Beispielen nur *Gercke/Brunst*, Praxishandbuch Internetstrafrecht, Rn. 3, m. w. N.

[11] Hierzu exemplarisch *Hermonies*, RuP 2011, 193 f.; *Eder*, Vorgänge 1/2009, 114, 117.

Ferner kommt es zu vielschichtigen neuartigen Bedrohungen für den Einzelnen durch die mit dem (freiwilligen) „Datenexhibitionismus“ einhergehenden Nutzungen sozialer Netzwerke (z. B. Facebook), deren Anwendungsrisiken für den Nutzer schon jetzt kaum überschaubar und regulierbar sind.[12] In der Presse finden sich eine Vielzahl weiterer kritischer Beispiele im Kontext der Nutzung sozialer Netzwerke, von zahlreichen online angekündigten Partyveranstaltungen, bei denen später eine unüberschaubare Anzahl von Partygästen erschien, über den „geposteten“ Aufruf zur Lynchjustiz gegen einen zunächst strafrechtlich Verdächtigen im April 2012 in der Stadt Emden bis hin zu einem Fall der außerordentlichen Kündigung einer Arbeitnehmerin, nachdem sich diese über ihren Zugang bei Facebook abträglich über einen Kunden des Arbeitgebers geäußert hatte.[13]

Aber auch der Bereich des Einzelnen, der bewusst nicht nach außen getragen wird, sieht sich neuen Gefährdungen ausgesetzt, denn nicht jedes Datum soll für die Allgemeinheit zugänglich sein. Gemeint sind vor allem solche Daten, die der Nutzer allein seinem informationstechnischen System anvertraut.[14] Gefährdungspotenzial entsteht zudem durch die nicht bewusst angelegten, sondern systemtätig aufgrund automatischer Datenverarbeitungsprozesse generierten Datenspuren, die der Einzelne bei der Nutzung informationstechnischer Systeme unvermeidbar hinterlässt und die dem Staat wie Dritten gleichermaßen Auskunft über dessen Nutzungsverhalten geben können.[15] Schon die unbefugte Kenntnis weniger Daten kann dabei Einblicke in wesentliche Teile der Lebensgestaltung einer Person zulassen oder gar ein aussagekräftiges Bild der Persönlichkeit abgeben.[16] So lässt sich etwa mit der punktuellen Auswertung automatisch generierter Standortdaten mobiler informationstechnischer Systeme ein detailliertes Bewegungsprofil erstellen. In den falschen Händen kann dies zu weitreichenden persönlichen Konsequenzen für den Betroffenen führen.[17]

Selbst der aufgeklärte Bürger hat aber gerade von automatisierten informationstechnischen Systemvorgängen kaum Kenntnis.[18] Vielmehr vertraut er allgemein darauf, dass das verwendete informationstechnische System sicher ist und nur solche Daten verarbeitet sowie nur solche Funktionen ausführt, die erwünscht und benötigt

---

[12] Vgl. *Peifer*, JZ 2013, 853, 855; *Volkmann*, FAZ vom 26. 02. 2009, S. 7; *Kutscha*, LKV 2008, 481.

[13] Zu einzelnen Beispielen *Kutscha*, in: Kutscha/Thomé, Grundrechtsschutz im Internet?, S. 13 f.; VGH München, MMR 2012, 422 ff.; zu weiteren Beispielen siehe auch *Peifer*, JZ 2013, 853, 856.

[14] Vgl. BVerfGE 120, 274, 312 f.; *Hoffmann-Riem*, JZ 2008, 1009, 1012, bezeichnet informationstechnische Systeme insoweit als „ausgelagertes Gehirn“ bzw. „ausgelagerte Psyche“ des Nutzers.

[15] Vgl. BVerfGE 120, 274, 305; *Hoffmann-Riem*, JZ 2008, 1009, 1016 f.

[16] Vgl. BVerfGE 120, 274, 314.

[17] Siehe schon *Sieber*, NJW 1989, 2569, 2570 f., zum Gefahrenpotenzial von Informationen.

[18] Vgl. *Kutscha*, LKV 2008, 481.