THOMAS WISCHMEYER

Informationssicherheit

Jus Publicum
317

Mohr Siebeck

JUS PUBLICUM

Beiträge zum Öffentlichen Recht

Band 317

Thomas Wischmeyer

Informationssicherheit

Mohr Siebeck

Thomas Wischmeyer, geboren 1983; Studium der Rechtswissenschaft in Freiburg i.Br., Lausanne und Krakau; 2014 Promotion; 2017 Juniorprofessor, seit 2020 Professor für Öffentliches Recht und Recht der Digitalisierung an der Universität Bielefeld; 2022 Habilitation.
orcid.org/0000-0001-6163-4056

Published with the support of the Open Access Publication Fund of Bielefeld University and the Deutsche Forschungsgemeinschaft (DFG).

ISBN 978-3-16-162059-1 / eISBN 978-3-16-162060-7
DOI 10.1628/978-3-16-162060-7

ISSN 0941-0503 / eISSN 2568-8480 (Jus Publicum)

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

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

Printed in Germany.

Vorwort

Die vorliegende Untersuchung wurde im Wintersemester 2022/2023 von der Rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg als Habilitationsschrift angenommen.

Ich hatte das große Glück, dass Andreas Voßkuhle die Entstehung dieser Arbeit betreut hat. Von ihm habe ich mehr als von jedem anderen über das Recht gelernt. Seine Zugewandtheit und sein Vertrauen haben mir den Weg in die Wissenschaft leicht gemacht. Hierfür kann ich mich nur bedanken. Herzlicher Dank gilt auch Jens-Peter Schneider für stete Anregungen, Ermutigung und für die Erstellung des Zweitgutachtens.

Beim Verfassen der Arbeit wurde ich durch verschiedene Institutionen und Personen gefördert, bei denen ich mich ebenfalls bedanke. Die Deutsche Forschungsgemeinschaft hat die Konzeption der Schrift durch die Finanzierung einer eigenen Stelle und ihre Veröffentlichung, gemeinsam mit der Universität Bielefeld, durch einen Zuschuss unterstützt. Der DAAD und das Jean Monnet Program der New York University, namentlich Gráinne de Búrca und Joseph Weiler, haben mir ermöglicht, als Emile Noël Fellow in einem frühen Stadium der Arbeit vom vibrierenden intellektuellen Klima der NYU Law School zu profitieren. Meine Bielefelder Kolleginnen und Kollegen und das Zentrum für interdisziplinäre Forschung (ZiF) haben mir Freiräume gewährt, um diese Arbeit auf einer (Junior-)Professur fertigzustellen. Bei der Endredaktion haben mich meine Mitarbeiterinnen und Mitarbeiter entlastet.

Zahlreiche weitere Personen haben mich in der Entstehungsphase der Arbeit in unterschiedlicher Form unterstützt. Hierzu zählen insbesondere Christian Bumke, Anna-Bettina Kaiser, Ann-Katrin Kaufhold und Angelika Siehr, ohne deren Zuspruch und Impulse diese Schrift so nicht entstanden wäre. Und ohne die Hilfe von Stephanie Höhne und Yonca Ruschinski hätte wichtige Zeit für ihre Fertigstellung gefehlt. Euch allen gilt mein besonderer Dank.

Gewidmet ist diese Arbeit Mareike, Simon und Lukas.

Berlin, im Dezember 2022 *Thomas Wischmeyer*

Inhaltsübersicht

Vorwort V
Inhaltsverzeichnis IX
Abkürzungsverzeichnis XVII

Einführung 1

§ 1 Die Vulnerabilität der digitalen Technik 3
§ 2 Recht der Informationssicherheit – Annäherungen an einen regulatorischen Diskurs 17

Erster Teil: Grundlagen des Informationssicherheitsrechts 47

§ 3 Informationssicherheitsrecht als Technikregulierung 49
§ 4 Informationssicherheitsrecht in der Sicherheitsgesellschaft 75

Zweiter Teil: Gewährleistung von Informationssicherheit durch Recht 119

§ 5 Unions- und verfassungsrechtliche Rahmenbedingungen des Informationssicherheitsrechts 121
§ 6 Gewährleistung von Informationssicherheit: Ein regulatorisches Schutzkonzept 183
§ 7 Sicherheitsgewährleistung durch Manipulation der Informationstechnik? 279

Schluss 319

§ 8 Ausblick 321
§ 9 Zusammenfassung in Leitsätzen 323

Bibliographie 333
Sachregister 407

Inhaltsverzeichnis

Vorwort V
Inhaltsübersicht VII
Abkürzungsverzeichnis XVII

Einführung

§ 1 Die Vulnerabilität der digitalen Technik 3

I. Informationssicherheit als Systemrisiko 3

II. Informationssicherheit auf der rechtspolitischen Agenda 5

III. Informationssicherheitsdiskurs zwischen Extremen: „Going dark" vs. „Versicherheitlichung" 10

IV. Informationssicherheit als Herausforderung für Recht und Rechtswissenschaft 12

§ 2 Recht der Informationssicherheit – Annäherungen an einen regulatorischen Diskurs 17

I. Bestandsaufnahme: Vier Schlaglichter 18

1. Informationssicherheit im Informationsverwaltungsrecht und im Recht des E-Government 18
2. Informationssicherheit im Datenschutzrecht 21
3. Informationssicherheit im Recht der kritischen Infrastrukturen . . . 22
4. Informationssicherheit im Völkerrecht 23
5. Zur Notwendigkeit einer integrativen Perspektive 25

II. Begriffliche Konturierung: Datensicherheit, Informationssicherheit, IT-Sicherheit, Cybersicherheit? 26

III. Gang der Untersuchung 29

IV. Zur Methode: Nach der Neuen Verwaltungsrechtswissenschaft . 31

1. Informationssicherheit als regulatorische Aufgabe 31
2. Methodische Implikationen 38
3. Alter Wein in neuen Schläuchen?! 42

Erster Teil

Grundlagen des Informationssicherheitsrechts

§ 3 Informationssicherheitsrecht als Technikregulierung 49

I. Zur Gestaltbarkeit der Technik 50
1. Technik als Schicksal? 50
2. Technik jenseits von Mittel und Zweck 53
3. Technik als soziales System und als Möglichkeitsraum 58

II. „Recht und Technik" revisited 59
1. Von der Technikignoranz der Rechtswissenschaft 60
2. ... über die Anerkennung der staatlichen Verantwortung für die Risiken der Technik 63
3. ... zur Technikregulierung als Strukturierung des Kommunikationsprozesses zwischen Recht und Technik 65

III. Exkurs: Der Sonderweg des Datenschutzrechts 68

§ 4 Informationssicherheitsrecht in der Sicherheitsgesellschaft . 75

I. Sicherheit: Auftrag, Perspektive oder Dispositiv? 77
1. Sicherheit als staatlicher Auftrag 77
2. Vom „alten" zum „neuen" Sicherheitsrecht: Sicherheit als Perspektive 79
a) Transformationen des Sicherheitsrechts 79
b) Sicherheitsrecht als Risikorecht 80
c) Ein „neuer" Sicherheitsbegriff 82
d) Erscheinungsformen des „neuen" Sicherheitsrechts 84
3. Kritik der „Versicherheitlichung": Sicherheit als Dispositiv 88
a) Diagnose der Diskursverschiebung 88
b) Folgen für das Rechtssystem: Identifikation von Aufmerksamkeitsfeldern I 91
aa) Grundrechte 92
bb) Gewaltenteilung 92
cc) Föderale Kompetenzverteilung 93
4. Zwischenfazit 96

II. Versicherheitlichungstendenzen im Cyberraum 97
1. Der Informationssicherheitsdiskurs als illiberale Diskursverschiebung? 97
a) Entgrenzter Begriff und entgrenzter Diskurs 97
b) Zur Rolle des Militärs und der Nachrichtendienste im Bereich der Informationssicherheitsgewährleistung 99
c) Digitale Technik als „Ideologie" 101
d) Kritische Würdigung 102

2. Zur Notwendigkeit eines „All-Gefahren-Ansatzes“ im Cyberraum 102
a) Komplexität der Problemlage 103
b) Attributionsproblem 104
c) Untauglichkeit der Unterscheidung von security und safety zur Erfassung von Informationssicherheitsrisiken 111
3. Folgen für das Rechtssystem: Identifikation von Aufmerksamkeitsfeldern II 112

III. Facetten der Informationssicherheit 115

Zweiter Teil

Gewährleistung von Informationssicherheit durch Recht

§ 5 Unions- und verfassungsrechtliche Rahmenbedingungen des Informationssicherheitsrechts 121

I. Grundrechte als Grenze staatlicher Informationssicherheitsregulierung 122
1. Grundrechte als Abwehrrechte gegen Maßnahmen zur Erhöhung des Informationssicherheitsniveaus 122
a) Schutz privater Betreiber informationstechnischer Systeme 122
aa) Systemische Natur und Kaskadeneffekte von IT-Sicherheitsrisiken 124
bb) Mangelnde IT-Sicherheit kein Ausdruck privater Macht . . . 125
cc) Informationssicherheitsregulierung kein Eingriff in den Kernbereich der Digitalwirtschaft 126
dd) Zwischenfazit 127
b) Schutz der Privatheitsinteressen Dritter 127
2. Abwehrrechte gegen Maßnahmen zur Senkung des Informationssicherheitsniveaus 129
a) Schutz der Vertraulichkeit und Integrität der Telekommunikation 130
b) Schutz des Zugangsbestimmungsrechts über die eigene Wohnung 134
c) Schutz des allgemeinen Persönlichkeitsrechts 140
aa) Recht auf informationelle Selbstbestimmung 140
bb) Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme 145
3. Informationssicherheit als übergreifendes Grundrechtsproblem . . . 152

II. Grundrechtliche Gewährleistungsverantwortung für die IT-Sicherheit 156
1. Maßstäbe: Grundrechtsschutz durch Informationssicherheit 157
2. Pflicht zur risikobasierten Regulierung 161

III. Zur Organisation hoheitlicher Interventionen in die Informationstechnik 163
1. Kompetenzrechtliche Determinanten für die Informationssicherheitsregulierung im Mehrebenensystem 163
a) Gesetzgebungskompetenzen 163
aa) Grundgesetz 164
bb) Unionsrecht 164
b) Verwaltungskompetenzen 167
aa) Grundgesetz 167
bb) Unionsrecht 170
2. Demokratische Legitimation der Informationssicherheitsverwaltung 172
a) Unabhängige Behörden? 173
b) Grenzen der Delegation 178
aa) Indienstnahme privaten Sachverstands 178
bb) Ermächtigung der Exekutive 180
IV. Folgerungen 181

§ 6 Gewährleistung von Informationssicherheit: Ein regulatorisches Schutzkonzept 183

I. Zur Ordnung komplexer Regulierungsregime 183
II. Strukturen des Informationssicherheitsrechts 188
1. Primat der Aufgabe: Ziele und sachlicher Umfang der Regulierung 188
a) Von den Schutzzielen zur Aufgabe Informationssicherheit 188
b) ... Aufgabe Informationssicherheit: Ein Schichtenmodell 191
aa) System- und Netzwerksicherheit 192
bb) Komponentensicherheit 196
cc) Internetsicherheit 198
c) ... von der Aufgabenbeschreibung zur rechtlichen Regulierung . 206
2. Territorialisierung des Informationssicherheitsproblems 209
a) Informationssicherheit als globales Problem 209
b) Expansive Jurisdiktionsregeln 212
c) Koordination und Kooperation 214
d) Lokalisierungspflichten 216
e) Zwischenfazit 217
3. Aufbau einer regulatorischen Kommunikations- und Wissensinfrastruktur 217
a) Informationssicherheit als Wissensproblem und als öffentliches Gut 217
b) Forschungs- und Innovationsförderung zwischen Staat und Markt 220

c) Aufbau spezialisierter Organisationseinheiten und administrativer Netzwerke zur Verarbeitung gesellschaftlich generierten Wissens . . . 221
d) Aufbau kooperativer Plattformen zum Informationsaustausch zwischen Staat und Gesellschaft . . . 224
e) Transparenzförderung durch Melde- und Informationspflichten . . . 226
f) Formen und Verfahren der Wissensdistribution . . . 230
g) Zwischenfazit . . . 231
4. Ausgestaltung der Verantwortungsarchitektur . . . 232
a) Akteure der Informationssicherheit . . . 232
b) Wandel der Verantwortlichkeitsstruktur: Von der Störerhaftung zur Inpflichtnahme privater Dritter für die Risiken der Informationstechnik . . . 233
c) Adressaten des Informationssicherheitsrechts . . . 237
aa) System- und Netzwerksicherheit . . . 237
bb) Komponenten- und Internetsicherheit . . . 241
d) Zwischenfazit . . . 244
5. Konkretisierung des Pflichtenprogramms für die Netzwerk- und Systemsicherheit . . . 244
a) Verpflichtung zu technischen und organisatorischen Maßnahmen . . . 244
b) Formen der Konkretisierung des Pflichtenprogramms („Stand der Technik“) . . . 247
c) Risikobasierter Ansatz . . . 253
d) Zwischenfazit . . . 255
6. Konkretisierung des Pflichtenprogramms für die Komponentensicherheit . . . 257
a) Komponentensicherheit als neues Aufmerksamkeitsfeld des Informationssicherheitsrechts . . . 257
b) Der EU Cybersecurity Act (CSA) als risikobasierte Rahmenregelung für Zertifizierungen . . . 258
c) Der CSA im Kontext weiterer Zertifizierungsregime . . . 262
d) Produktwarnungen, -empfehlungen und -untersuchungen . . . 264
e) Zwischenfazit . . . 266
7. Internetsicherheit als terra incognita des Informationssicherheitsrechts . . . 266
8. Durchsetzung und Kontrolle . . . 268
a) Allgemeine ordnungsrechtliche Durchsetzungs- und Kontrollbefugnisse . . . 268
b) Operative Tätigkeiten: CSIRT/CERT und MIRTs . . . 269
c) Haftung . . . 270
d) Strafrechtliche Sanktionen . . . 272

III. Fazit: Vom „patchwork of confusion“ zur integrativen Regulierung . . . 274

§ 7 Sicherheitsgewährleistung durch Manipulation der Informationstechnik? 279

I. Zur Doppelrolle des Staats als Garant und Gefährder der Informationssicherheit 279

II. Staatliche Governance von IT-Schwachstellen 281

1. Implikationen der Nicht-Offenlegung und Nutzung von Schwachstellen für die IT-Sicherheit: Kollisions-, Proliferations- und Einsatzrisiken 282
2. Zur staatlichen Nutzung von Schwachstellen am Beispiel der Quellen-TKÜ 285
   a) Unvollständige Würdigung der Einsatzrisiken 286
   b) Vernachlässigung der Kollisions- und Proliferationsrisiken . . . 289
3. Grundzüge einer staatlichen Schwachstellen-Governance 292
   a) Orientierungspunkte: Der Vulnerabilities Equities Process . . . 293
   b) Gestaltungselemente 295
      aa) Ziele und gesetzliche Grundlagen 295
      bb) Maßstäbe für die (Nicht-)Veröffentlichung 297
      cc) Informationssicherheit 300
      dd) Organisation und Verfahren der Schwachstellen-Governance 300
   c) Ausblick 307

III. Regulierung von Verschlüsselung 308

1. Ambivalenzen der Kryptopolitik: „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ 309
2. Ansätze staatlicher Verschlüsselungsregulierung für Online-Kommunikation 311
3. Ziele und Grenzen der staatlichen Regulierung von Verschlüsselungstechnologien 315
   a) Gewährleistungsverantwortung und Förderpflicht 315
   b) Beeinträchtigungen der Integrität von Verschlüsselungsmechanismen 315
   c) Grenzen der Verschlüsselungsregulierung 316

IV. Fazit 317

Schluss

§ 8 Ausblick 321

§ 9 Zusammenfassung in Leitsätzen 323

I. Ausgangsproblem, Gegenstand und Ziel der Untersuchung . . . 323

II. Grundlagen und Kontexte der Informationssicherheitsregulierung 324
III. Unions- und verfassungsrechtliche Rahmenbedingungen der Informationssicherheitsregulierung 326
IV. Grundzüge eines regulatorischen Schutzkonzepts 328
V. Grenzen für staatliche Manipulationen der Informationssicherheit 332

Bibliographie 333
Sachregister 407

Abkürzungsverzeichnis

a. A.	andere(r) Ansicht
a. a. O.	am angegebenen Ort
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a. F.	alte Fassung
Art.	Artikel
AS	Autonomes System
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Bd.	Band
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGP	Border Gateway Protocol
BK GG	Wolfgang Kahl/Christian Waldhoff/Christian Walter (Hrsg.), Bonner Kommentar zum Grundgesetz, 21 Bde., Hamburg 1950–1988, Heidelberg 1989 ff.; Stand: 216. Lieferung September 2022
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern und für Heimat
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft und Energie
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfG (K)	Kammerentscheidung des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BW	Baden-Württemberg
Calliess/Ruffert, EUV/AEUV	Christian Calliess/Matthias Ruffert (Hrsg.), EUV/AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta. Kommentar, 6. Aufl., München 2022
CEN	Comité Européen de Normalisation/Europäisches Komitee für Normung
CERT	Computer Emergency Response Team
CSA	Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikations-

	technik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)
CSG	Gesetz zur Verbesserung der Cybersicherheit
CSIRT	Computer Security Incident Response Teams
DDoS	Distributed Denial of Service
Denninger et al., AK-GG	Erhard Denninger/Wolfgang Hoffmann-Riem/Hans-Peter Schneider/Ekkehart Stein (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland (AK-GG), 3. Aufl., 3 Bde., Neuwied u. a. 2001 ff., Stand 2. Ergänzungslieferung August 2002
DNS	Domain Name System
DOC	United States Department of Commerce
DÖV	Die Öffentliche Verwaltung. Zeitschrift für öffentliches Recht und Verwaltungswissenschaft
DNSSEC	Domain Name System Security Extensions
Dreier	Dreier, Horst (Hrsg.), Grundgesetz-Kommentar, 3. Aufl., Bd. 1, Tübingen 2013; Bd. 2 Tübingen 2015; Bd. 3 Tübingen 2018; Brosius-Gersdorf, Frauke (Hrsg.), Grundgesetz-Kommentar, 4. Aufl., Bd. 1, i. E.
DSA	Verordnung des Europäischen Parlaments und des Rates über einen Binnenmarkt für digitale Dienste (Gesetz über digitale Dienste) und zur Änderung der Richtlinie 2000/31/EG
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder
DSRL-JI	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
Dürig/Herzog/Scholz, GG	Roman Herzog/Rupert Scholz/Matthias Herdegen/Hans H. Klein (Hrsg.), Grundgesetz. Kommentar, begründet von Theodor Maunz/Günter Dürig, Stand: 98. Ergänzungslieferung März 2022 (Loseblatt-Ausgabe: 7 Bde., München 1958 ff.)
EC3	Europäische Zentrum zur Bekämpfung der Cyber-Kriminalität
EDPB	European Data Protection Board
EGMR	Europäischer Gerichtshof für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
EKEK	Richtlinie (EU) 2018/1972 über den europäischen Kodex für die elektronische Kommunikation
ENISA	Agentur der Europäischen Union für Cybersicherheit
Epping/Hillgruber, BeckOK GG	Volker Epping/Christian Hillgruber (Hrsg.), Beck'scher Online-Kommentar Grundgesetz, Stand: 52. Edition August 2022
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EU CyCLONe	EU Cyber Crisis Liaison Organisation Network
EuGH	Gerichtshof der Europäischen Union
EU INTCEN	EU Zentrum für Informationsgewinnung und -analyse
Eurojust	Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen
eu-LISA	Europäische Agentur für IT-Großsysteme
Europol	Europäisches Polizeiamt

Fn.	Fußnote
Friauf/Höfling, GG	Karl-Heinrich Friauf (Begr.)/Wolfram Höfling/Steffen Augsberg/Stephan Rixen (Hrsg.), Berliner Kommentar zum Grundgesetz, 6 Bde., Berlin 2000 ff.; Stand: Januar 2022
GAL	Global Administrative Law
GCHQ	Government Communications Headquarters
Gersdorf/Paal, BeckOK Informations- und Medienrecht	Hubertus Gersdorf/Boris P. Paal (Hrsg.), Beck'scher Online-Kommentar, Informations- und Medienrecht, Stand: 37. Edition August 2022
GG	Grundgesetz
GRCh	Charta der Grundrechte der Europäischen Union
GTAZ	Gemeinsames Terrorismusabwehrzentrum
GVwR	Grundlagen des Verwaltungsrechts, Andreas Voßkuhle/Martin Eifert/Christoph Möllers (Hrsg.), 3 Bde., 3. Aufl., München 2022
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HTTP	Hypertext Transfer Protocol
Huber/Voßkuhle, GG	Grundgesetz-Kommentar, Peter M. Huber/Andreas Voßkuhle (Hrsg.), 3 Bde., 8. Aufl., i. E.
HVerfR	Matthias Herdegen/Johannes Masing/Ralf Poscher/Klaus F. Gärditz (Hrsg.), Handbuch des Verfassungsrechts, München 2021
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IEEEA	IEEE Annals of the History of Computing
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IJGLS	Indiana Journal of Global Legal Studies
IT-SiG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
IT-SiG 2.0	Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
Jarass, GRCh	Hans D. Jarass, Charta der Grundrechte der Europäischen Union, 4. Aufl., München 2021
J-CAT	Joint Cybercrime Action Taskforce
JSRR	Journal of Self-Regulation and Regulation
JZ	JuristenZeitung
Kahl/Ludwigs, HVwR	Wolfgang Kahl/Markus Ludwigs (Hrsg.), Handbuch des Verwaltungsrechts, 12 Bde., Heidelberg 2021 ff.
KRITIS	Kritische Infrastruktur(en)
L. J.	Law Journal
L. Rev.	Law Review
LAN	Local Area Networks
LIR	Local Internet Registries
Lisken/Denninger, HdbPolR	Matthias Bäcker/Erhard Denninger/Kurt Graulich (Hrsg.)/Hans Lisken (Begr.), Handbuch des Polizeirechts, 7. Aufl., München 2021
Meyer/Hölscheidt, Charta	Jürgen Meyer/Sven Hölscheidt (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019
MPEPIL	Max Planck Encyclopedia of Public International Law
v. Münch/Kunig, GG	Jörn-Axel Kämmerer/Markus Kotzur (Hrsg.), begründet von Ingo von Münch und Philip Kunig, 2 Bde., 7. Aufl., München 2021

NCAZ	Nationales Cyber-Abwehrzentrum
NIS-RL	Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
NIS 2-RL	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union
NIST	National Institute of Standards and Technology
NJW	Neue Juristische Wochenschrift
NSA	National Security Agency
NSC	National Security Council
OSI/ISO-Modell	Open Systems Interconnection Model
OTT	Over-the-Top
OZG	Onlinezugangsgesetz
Parl. Rat	Der Parlamentarische Rat 1948–1949. Akten und Protokolle, herausgegeben vom Deutschen Bundestag und vom Bundesarchiv, Boppard am Rhein, 1975 ff.
PESCO	Ständige Strukturierte Zusammenarbeit
PolG BW	Polizeigesetz Baden-Württemberg
POP	Post Office Protocol
PVS	Politische Vierteljahresschrift
RCE	Resilience of Critical Entities
RCE-RL	Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen
RFC	Request for Comment
RFSR	Raum der Freiheit, der Sicherheit und des Rechts
RIR	Regional Internet Registry
RL	Richtlinie
Sachs, GG	Michael Sachs (Hrsg.), Grundgesetz. Kommentar, 9. Aufl., München 2021
Schenke/Graulich/Ruthig	Wolf-Rüdiger Schenke/Kurt Graulich/Josef Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl., München 2019
Schmidt-Bleibtreu/Hofmann/Henneke, GG	Bruno Schmidt-Bleibtreu/Hans Hofmann/Hans-Günter Henneke (Hrsg.), Grundgesetz. Kommentar, 15. Aufl., Köln 2022
Schwarze, EU-Kommentar	Jürgen Schwarze/Ulrich Becker/Armin Hatje/Johann Schoo (Hrsg.), EU-Kommentar, 4. Aufl., Baden-Baden 2019
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
StPO	Strafprozessordnung
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TKÜV	Telekommunikations-Überwachungsverordnung
TLS	Transport Layer Security
TTDSG	Telekommunikations-Telemedien-Datenschutz-Gesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UN GGE	United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security
VEP	Vulnerabilities Equities Process

VEP 2017	Vulnerabilities Equities Policy and Process 2017
VO	Verordnung
VoIP	Voice-over-IP
VPN	Virtual Private Networks
VVDStRL	Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer
WCIT	World Conference on International Telecommunications
Wolff/Brink, BeckOK Datenschutzrecht	Heinrich Amadeus Wolff/Stefan Brink (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, Stand: 41. Edition August 2022
ZAC	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen
ZaöRV	Zeitschrift für ausländisches öffentliches Recht und Völkerrecht

Einführung

§ 1 Die Vulnerabilität der digitalen Technik

> „Societies today network first, and ask questions later."[1]

> „While ICTs and an increasingly digitalized and connected world provide immense opportunities for societies across the globe, the [United Nations Group of Governmental Experts] reaffirms that the serious ICT threats identified in previous reports persist. Incidents involving the malicious use of ICTs by States and non-State actors have increased in scope, scale, severity and sophistication. While ICT threats manifest themselves differently across regions, their effects can also be global."[2]

I. Informationssicherheit als Systemrisiko

Die Errungenschaften der Digitalisierung ruhen auf einem technischen Fundament, von dem unklar ist, ob es seine Last dauerhaft tragen kann. Ganze Sektoren wie die Energieversorgung, die Telekommunikation, die verarbeitende Industrie, der Finanzmarkt, das Gesundheitswesen aber auch staatliche Kernfunktionen wie Gesetzgebung und Verwaltung sind heute auf funktionierende Netze und Informationssysteme angewiesen. Gleichzeitig steigt die Zahl der Angriffe auf Netze und Systeme stetig an.[3] Die Lage gilt allgemein als fragil[4]

---

[1] *K. Eichensehr*, Giving Up On Cybersecurity, UCLA L. Rev. Discourse 64 (2016), S. 320.

[2] *United Nations General Assembly*, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 14.7.2021, A/76/135, Rn. 6.

[3] Das BSI dokumentiert die Gefährdungslage fortlaufend unter https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html. Analoge Erhebungen führen ENISA (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends), Europol (https://www.europol.europa.eu/iocta-report) und das BKA (https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html) durch.

[4] Das relative Gewicht der Bedrohung lässt sich diversen Risikobarometern entnehmen, die Cyberrisiken allgemein auf den vordersten Rängen der globalen Bedrohungslagen einordnen – mit lange Zeit stark steigender, seit 2022 allerdings leicht fallender Tendenz. Vgl. *World Economic Forum*, Global Risks Report, 2021, S. 11 und passim; *dass.*, Global Risks Report, 2022, S. 7, 45 ff. Aus Versicherungssicht siehe das Allianz Risk Barometer 2022 unter

und das individuelle Unsicherheitsgefühl ist hoch.[5] Die allenthalben mit großer Intensität vorangetriebene, durch die Covid-19-Pandemie nochmals beschleunigte[6] digitale Transformation von Staat, Wirtschaft und Gesellschaft verschärft das Problem stetig.[7] Effektives E-Government, moderne Telekommunikationstechnologien wie 5G,[8] verlässliche Online-Identitäten[9] und immer größere Teile der privaten Lebensführung[10] sind auf ein hohes Informationssicherheitsniveau angewiesen.

Gefährdet sind nicht nur die digitale Technik und die damit assoziierten Rechtsgüter, namentlich das Datenschutzgrundrecht und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Soweit vernetzte Software genutzt wird, um physische Komponenten zu steuern (sog. cyber-physische Systeme), schlagen Beeinträchtigungen der Informationssicherheit vielmehr auf alle möglichen Rechtsgüter durch.[11] Wenn aufgrund von Cyberattacken Stromversorger,[12] Krankenhäu-

---

https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html. Zurückhaltender die (älteren) Berechnungen bei *S. Romanosky*, Examining the costs and causes of cyber incidents, Journal of Cybersecurity 2:2 (2016), S. 121 ff. Siehe auch die Meta-Studie: *Cybersecurity and Infrastructure Security Agency*, Cost of a Cyber Incident: Systematic Review and Cross-Validation, 2020.

[5] Daten hierzu erhebt die Europäische Kommission in ihrem Digital Economy and Society Index (DESI) im Panel Cybersecurity, zuletzt https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67080. Siehe auch *M. Gross/D. Canetti/D. Vashdi*, Cyberterrorism, Journal of Cybersecurity 3:1 (2017), S. 49 ff. Zur rechtlichen Bedeutung des Sicherheitsgefühls allgemein nur *M. Kötter*, Subjektive Sicherheit, Autonomie und Kontrolle, Der Staat 43 (2004), S. 371 ff.; *C. Schewe*, Das Sicherheitsgefühl und die Polizei, 2009; *M. Bäcker*, Kriminalpräventionsrecht, 2015, S. 316 ff.; *E. Denninger*, Rechtsstaatliche und demokratische Grundlagen der Polizeiarbeit, in: Lisken/Denninger, HdbPolR, 7. Aufl. 2021, Kap. B I. Rn. 87 ff.

[6] Zu den messbaren Auswirkungen der Pandemie auf den globalen Datenverkehr vgl. die Statusberichte der Europäischen Kommission und des Body of European Regulators of Electronic Communications (BEREC) unter https://digital-strategy.ec.europa.eu/en/library/reports-status-internet-capacity-during-coronavirus-confinement-measures. Zum dadurch bedingten Anstieg an Cyber-Bedrohungen vgl. den Bericht des Joint Research Center der Europäischen Kommission: I. Nai Favino et al. (Hrsg.), Cybersecurity, our digital anchor, 2020, S. 71 ff.; sowie *H. Lallie/L. Shepherd et al.*, Cyber Security in the Age of COVID-19, Computers & Security 105 (2021), S. 102248.

[7] Zum Stand der Digitalisierung siehe *Kompetenzzentrum Öffentliche IT*, Deutschland-Index der Digitalisierung, 2021.

[8] Vgl. § 9b BSIG i.d.F. des IT-SiG 2.0. Siehe weiter die Nachweise unten § 1 Fn. 46.

[9] Vgl. aktuell den Vorschlag der Kommission zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität v. 3.6.2021, COM(2021) 281 final. Siehe bereits § 18 Abs. 2 S. 2 PAuswG.

[10] Im Überblick: *M. Hansen*, Private Haushalte, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 26.

[11] Vgl. die umfangreiche Darstellung bei *I. Agrafiotis/J. Nurse et al.*, A Taxonomy of Cyber-Harms, Journal of Cybersecurity 4:1 (2018), S. 1 ff.

[12] Zur dortigen Gefährdungslage siehe die Antwort der Bundesregierung auf die Kleine Anfrage „Sicherheit von Stromnetzen und anderer kritischer Infrastrukturen gegenüber Cyberangriffen" v. 30.3.2021, BT-Drs. 19/28113.

ser[13] oder Medienunternehmen[14] ihre Tätigkeit einstellen müssen, sind das Recht auf Leben, auf körperliche und geistige Unversehrtheit (Art. 2 Abs. 2 GG; Art. 2 und 3 GRCh) bzw. auf Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 GG; Art. 11 GRCh) jedenfalls in ihrer objektiv-rechtlichen Funktion betroffen. Wird, wie im Falle der U.S.-Präsidentschaftswahlen von 2016, die Integrität der Wahl beeinträchtigt, hat dies erhebliche Konsequenzen für die demokratische Ordnung.[15] Werden Produkte wie die Netzwerkmanagement-Software des Unternehmens SolarWinds kompromittiert, die tief in der IT-Lieferkette integriert sind, wird das Ausmaß des Schadens nur noch durch das Interesse und die Kapazitäten der Angreifer begrenzt.[16]

Die Sicherheit der Informationstechnik ist heute zur Bedingung der Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft geworden.[17] Sie entscheidet mit darüber, wie effektiv Grundrechte und Demokratie in Zeiten der Digitalisierung geschützt sind. Im speziellen Fall der Internetsicherheit stehen zudem die Gewährleistung der Menschenrechte sowie globale Entwicklungschancen auf dem Spiel.[18]

II. Informationssicherheit auf der rechtspolitischen Agenda

Die Einsicht in die Vulnerabilität der technischen Infrastrukturen hat mit dazu beigetragen, dass der Glaube an die Naturwüchsigkeit des Internets und der

[13] So kam es infolge des Ransomware-Angriffs auf die Universitätsklinik Düsseldorf im September 2020 zu Verzögerungen bei Notfallbehandlungen, die den Tod einer Patientin verursachten. Hier ermittelte die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC) zunächst wegen fahrlässiger Tötung. Letztlich konnte jedoch ein strafrechtlich relevanter Zusammenhang zwischen Angriff und Tod nicht mit hinreichender Gewissheit belegt werden, vgl. *W. Ralston*, The untold story of a cyberattack, Wired, 11.11.2020; *BSI*, Lage der IT-Sicherheit in Deutschland, 2021, S. 15. Großes Aufsehen erregte auch der Angriff auf das finnische Psychiatriezentrum *Vastaamo* im selben Jahr.

[14] Allein 2020 und 2021 waren die Mediengruppen *Funke* und *Madsack* betroffen. Vgl. *BSI*, Lage der IT-Sicherheit in Deutschland, 2021, S. 18.

[15] Zum Sachverhalt *U.S. Department of Justice*, *United States v. Viktor Borisovich Netyksho et al.*, Case No. 1:18-cr-00215-ABJ, Indictment, 13.7.2018; *U.S. Department of Justice*, Report on the Investigation into Russian Interference in the 2016 Presidential Election, Bd. I, 2019.

[16] Siehe zu dieser Attacke *National Security Agency/Cybersecurity and Infrastructure Security Agency/Federal Bureau of Investigation*, Russian SVR Targets U.S. and Allied Networks, 2021. In welchem Umfang durch die Angriffe auch deutsche Stellen betroffen waren, ergibt sich aus den defensiven Antworten der Bundesregierung auf die Schriftliche Frage 68 der Abgeordneten *P. Pau*, BT-Drs. 19/26646, und auf die Kleine Anfrage der Abgeordneten *K. von Notz et al.*, BT-Drs. 19/27487, nicht mit Sicherheit.

[17] Vgl. die entsprechende Priorisierung der Materie in den Sicherheitsstrategien der USA und der EU: *White House*, Renewing America's Advantages, 2021, S. 18; *Europäische Kommission*, EU-Strategie für eine Sicherheitsunion 2020–2025, COM(2020) 605 final, S. 1.

[18] Zur Verbindung von „Internet Integrity", Menschenrechten und „Human Development" ausführlich *M. Kettemann*, The Normative Order of the Internet, 2020, S. 36 ff.

digitalen Technik heute einer nüchternen Haltung gewichen ist.[19] Das hat Konsequenzen für den regulatorischen Zugriff, der nach einer langen Phase der Förderung und des Gewährenlassens in intensive Betriebsamkeit umgeschlagen ist. Nicht nur in Europa etabliert sich derzeit eine Digitalpolitik, für die die hoheitliche Intervention in den digitalen Code selbstverständlich geworden ist.[20] Das Recht soll die Exzesse und Nebenfolgen der Digitalisierung einhegen und die Resilienz der Systeme stärken.[21]

Auf der digitalen Agenda der Politik steht auch die Sicherheit der Informationstechnik.[22] Nachdem sich Staaten zum Schutz vor Cyberbedrohungen lange Zeit vorwiegend informeller und kooperativer Strategien bedient hatten, hat nunmehr ein Prozess der Institutionalisierung und Verrechtlichung eingesetzt. So lässt sich beobachten, wie staatliche Stellen gegenwärtig in einem von Versuch und Irrtum geprägten Verfahren versuchen, Steuerungsimpulse für das bisher weitgehend privat geordnete Feld zu setzen. Die Bundesregierung reformiert ihre Strukturen, um der Bedeutung der Aufgabe Rechnung zu tragen. Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Zentrale Stelle für Informationstechnik im Sicherheitsbereich

[19] Zu den kulturellen Wurzeln dieser Denkhaltung grundlegend *P. Flichy*, L'imaginaire d'internet, 2001; *F. Turner*, From counterculture to cyberculture, 2006; *D. Golumbia*, The cultural logic of computation, 2009. Zu den (netz-)politischen Auswirkungen dieser Denkhaltung vgl. nur *M. Feeley*, EU Internet Regulation Policy, Boston College Int'l & Comp. L. Rev. 22 (1999), S. 112 ff. Für die gänzlich andere Entwicklung, die die Entwicklung vernetzter IT-Systeme in der Sowjetunion mit ihren ebenfalls gänzlich anderen sozialen Strukturen nahm, siehe *B. Peters*, How Not to Network a Nation. The Uneasy History of the Soviet Internet, 2016.

[20] Zur Genese des Politikfelds Netz- bzw. Digitalpolitik *A. Reiberg*, Netzpolitik, 2018; *W. Schüneman*, E-Government und Netzpolitik, in: ders./Kneuer (Hrsg.), E-Government und Netzpolitik im europäischen Vergleich, 2. Aufl. 2019, S. 17 ff. *M. Hösl/F. Irgmaier/R. Kniep*, Diskurse der Digitalisierung, in: Klenk/Nullmeier/Wewer (Hrsg.), Handbuch Digitalisierung, 2020, S. 383 ff.

[21] Speziell zur Cyber-Resilienz *R. Dewar/M. Dunn Cavelty*, Die Cybersicherheitspolitik der Europäischen Union, in: Schüneman/Kneuer (Hrsg.), E-Government und Netzpolitik im europäischen Vergleich, 2. Aufl. 2019, S. 281 ff. Allgemein zum Verhältnis von Recht und Resilienz *T. Würtenberger*, Resilienz, in: Baumeister/Roth/Ruthig, FS W.-R. Schenke, 2011, S. 561 ff.; H.-H. Gander/W. Perron et al. (Hrsg.), Resilienz in der offenen Gesellschaft, 2012; *C. Gusy*, Resilient Societies, in: Heckmann/Schenke/Sydow (Hrsg.), FS T. Würtenberger, 2013, S. 995 ff.; *G. Riescher*, Resilienz. Demokratietheoretische Überlegungen, in: Heckmann/Schenke/Sydow (Hrsg.), FS T. Würtenberger, 2013, S. 1067 ff.; K. von Lewinski (Hrsg.), Resilienz des Rechts, 2016; *ders.*, Resilienz der Verwaltung, in: Hill/Schliesky (Hrsg.), Management von Unsicherheit und Nichtwissen, 2016, S. 239 ff. Umfassend jetzt aus sozial- und aus rechtswissenschaftlicher Sicht *A. Folkers*, Das Sicherheitsdispositiv der Resilienz, 2018; *T. Barczak*, Der nervöse Staat, 2. Aufl. 2021, insbes. S. 606 ff.

[22] Siehe für Deutschland *BMI*, Cyber-Sicherheitsstrategie für Deutschland, 2016; ersetzt durch *BMI*, Cybersicherheitsstrategie für Deutschland, 2021. Für die 20. Legislaturperiode aktualisiert durch *BMI*, Cybersicherheitsagenda, 2022.

(ZITiS) werden aus- bzw. aufgebaut.[23] Und der Gesetzgeber mustert seinen Instrumentenkasten durch: Einen ersten, in der Reichweite noch sehr begrenzten Anlauf unternahm der deutsche Gesetzgeber bereits 1990 mit dem Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSIG). Mit der Neufassung des BSIG im Jahr 2009, dem im Jahr 2015 beschlossenen IT-Sicherheitsgesetz (IT-SiG) und dem 2021 verabschiedeten IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) wurden die Vorgaben zur Informationssicherheit im verwaltungsinternen Bereich verschärft sowie Regelungen erlassen, die weit in den gesellschaftlichen Bereich hinein auf eine Verbesserung des Schutzniveaus für IT-Systeme und Netzwerke zielen.[24] Die Länder ziehen hier derzeit nach.[25]

In anderen Staaten lässt sich eine vergleichbare Wendung hin zum Staat als Akteur und zum Gesetz als Steuerungsinstrument im Umgang mit Informationssicherheitsrisiken beobachten.[26] Den Kräften des Marktes allein wird eine Lösung nicht mehr zugetraut. Insgesamt hat sich die Materie innerhalb des letzten Jahrzehnts von einem randständigen und stark technikgeprägten Feld zu einem der zentralen Gegenstände der Digitalpolitik, ja der allgemeinen innen- und außenpolitischen Debatte entwickelt.[27]

Mit dem wachsenden Bewusstsein für die Bedeutung der Materie verlagert sich der Schwerpunkt der regulatorischen Aktivitäten in Europa allmählich von den Mitgliedstaaten auf die Europäische Union.[28] Während sich die Union

---

[23] Im Überblick *R. Gitter*, Recht der IT-Sicherheitsbehörden, in: Hornung/Schallbruch (Hrsg.), 2021, § 15; *M. Schardt*, Öffentliche Verwaltung, in: Hornung/Schallbruch (Hrsg.), IT-Sicherheitsrecht, 2021, § 25 Rn. 21 ff. Vgl. dazu näher unten § 5 III. 1. b), insbesondere § 5 Fn. 249.

[24] BSI-Gesetz v. 14.8.2009, BGBl. I S. 2821 (zitiert als BSIG); Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) v. 17.7.2015, BGBl. I S. 1324 (zitiert als IT-SiG); Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme v. 18.5.2021, BGBl. I S. 1122 (zitiert als IT-SiG 2.0).

[25] Vgl. etwa für das Saarland das am 15.5.2019 in Kraft getretene Gesetz zur Abwehr von Gefahren für die Daten in der Informations- und Kommunikationsinfrastruktur des Landes (Amtsbl. I S. 653) und für Baden-Württemberg das am 17.2.2021 in Kraft getretene Gesetz zur Verbesserung der Cybersicherheit (GBl. 2021 S. 182).

[26] Siehe den hilfreichen Überblick bei S. Cordey/R. Dewar (Hrsg.), National Cybersecurity and Cyberdefense Policy Snapshots: Updated Collection 2, 2019. Siehe auch die aktuellen Darstellungen unter https://css.ethz.ch/en/publications/risk-and-resilience-reports. Die Schriftenreihe „SpringerBriefs in Cybersecurity" bündelt gleichfalls eine größere Zahl länderspezifischer Darstellungen.

[27] So auch *M. Dunn Cavelty/F. Egloff*, The Politics of Cybersecurity: Balancing Different Roles of the State, St Antony's Int'l Rev. 15 (2019), S. 37 (38).

[28] Zur Agenda: *Europäische Kommission/Hohe Vertreterin der Union für Außen- und Sicherheitspolitik*, Gemeinsame Mitteilung, Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen, JOIN(2017) 450 final; *Europäische Kommission/Hoher Vertreter der Union für Außen- und Sicherheitspolitik*, Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final. Zum politischen Rahmen dieser Strategie siehe unten § 1 Fn. 58. Zur Historie umfassend *R. Dewar*, Cyber security in the

zunächst auf koordinierende Vorgaben sowie auf Anpassungen des dem Binnenmarkt besonders nahen Produktsicherheitsrechts beschränkte, um anschließend auch den Schutz kritischer Infrastrukturen zu adressieren,[29] wird Informationssicherheit für die EU in jüngerer Zeit immer mehr zum Vehikel, um sich als eigenständiger Sicherheitsakteur zu etablieren und umfassende Zuständigkeiten zur Abwehr von Cybervorfällen zu beanspruchen.[30] Dement-

European Union, Diss. Glasgow 2017. In anderen Feldern der Digitalpolitik war die EU vergleichsweise früh aktiv, siehe nur *F. Mayer*, Europe and the Internet, EJIL 11 (2000), S. 149 ff.

[29] Grundlegende horizontale Vorgaben formulieren: Richtlinie (EU) 2016/1148 vom 6. 7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194, 19.7.2016, S. 1 (zitiert als NIS-RL); Verordnung (EU) 2019/881 vom 17.4.2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik, ABl. L 151, 7.6.2019, S. 15 (zitiert als Rechtsakt zur Cybersicherheit – CSA); Richtlinie (EU) 2019/770 vom 20.5.2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (EU) 2019/770 (Regelungen zu Software-Updates). Aus den sektoralen Rechtsakten siehe etwa die IT-bezogenen Vorgaben der Verordnung (EU) 2017/745 vom 5.4.2017 über Medizinprodukte und die Delegierte Verordnung (EU) 2022/30 der Kommission vom 29.10.2021 zur Funkanlagenrichtlinie.

[30] Siehe zur wachsenden Rolle der EU in diesem Feld auch *E. Fahey*, The EU's Cybercrime and Cyber-Security Rulemaking, Europ. J. of Risk Reg. 5:1 (2014), S. 46 ff.; *K. Sliwinski*, Moving beyond the European Union's Weakness as a Cyber-Security Agent, Contemporary Security Policy 35:3 (2014), S. 468 ff.; *R. Wessel*, Towards EU Cybersecurity Law: Regulating a New Policy Field, in: Tsagourias/Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2015, S. 403 ff.; *G. Christou*, Cybersecurity in the European Union, 2016; *R. Dewar*, The European Union and Cybersecurity, in: O'Neill/Swinton (Hrsg.), Challenges and Critiques of the EU Internal Security Strategy, 2017, S. 113 ff.; *H. Carrapico/A. Barrinha*, The EU as a Coherent (Cyber)Security Actor?, JCMS 55:6 (2017), S. 1254 ff.; *L. Kello*, Cyber Defence, in: Meijer/Wyss (Hrsg.), The Handbook of European Defence Policies and Armed Forces, 2018, S. 658 ff.; *J. Odermatt*, The European Union as a Cybersecurity Actor, in: Blockmans/Koutrakos (Hrsg.), Research Handbook on the EU's Common Foreign and Security Policy, 2018, S. 354 ff.; *M. Dunn Cavelty*, Europe's cyber-power, European Politics and Society 19:3 (2018), S. 304 ff.; *A. Bendiek/E. Pander Maat*, The EU's Regulatory Approach to Cybersecurity, SWP Working Paper, 2019; *Dewar/Dunn Cavelty*, Die Cybersicherheitspolitik der Europäischen Union, in: Schüneman/Kneuer (Hrsg.), E-Government und Netzpolitik im europäischen Vergleich, 2. Aufl. 2019, S. 281 ff.; *Europäischer Rechnungshof*, Herausforderungen für eine wirksame Cybersicherheitspolitik der EU, März 2019; *C. Calliess/A. Baumgarten*, Cybersecurity in the EU, German L. J. 21 (2020), S. 1149 ff.; *A. Bendiek/E. Pander Maat*, The EU's Cybersecurity Policy, in: Siboni/Ezioni (Hrsg.), Cybersecurity and Legal-Regulatory Aspects, 2021, S. 23 ff.; *R. Wessel*, European Law and Cyberspace, in: Tsagourias/Buchan (Hrsg.), Research Handbook on International Law and Cyberspace, 2. Aufl. 2021, S. 491 ff.; *Z. Bederna/Z. Rajnai*, Analysis of the cybersecurity ecosystem in the European Union, Int'l Cybersecurity L. Rev. 2022, S. 35 ff.; *Y. Miadzvetskaya/R. Wessel*, The Externalisation of the EU's Cybersecurity Regime, European Papers 7 (2022), S. 413 ff. Folgende weitere Unionsrechtsakte mit Implikationen für das Informationssicherheitsrecht wurden jüngst verabschiedet oder befinden sich derzeit (Dezember 2022) im fortgeschrittenen Gesetzgebungsverfahren: (i) die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau (NIS 2) vom 14.12.2022; (ii) die Richtlinie (EU) 2022/2557 über die Resilienz kritischer Ein-

sprechend kommt dem Aspekt Cybersicherheit in den Plänen der EU zur Stärkung der „Sicherheitsunion" (Art. 3 Abs. 2 EUV; Art. 67 ff. AEUV) eine herausragende Rolle zu.[31] Ausdruck hiervon ist die neu eingerichtete EU Joint Cyber Unit.[32] Und auch im Völkerrecht begegnen erste Normsetzungsprozesse – bislang jedoch mit begrenztem Erfolg.[33]

Die skizzierten hoheitlichen Interventionen zur Stärkung der Informationssicherheit holen auch nach, was beim ursprünglichen Design der vernetzen Informationstechnik versäumt wurde. Obwohl oder gerade weil staatliche Stellen intensiv an deren Entwicklung beteiligt waren, wurde dem Aspekt Informationssicherheit zunächst keine besonders bedeutende Rolle zuerkannt.[34] Da sich der praktische Betrieb digitaler Netze anfänglich auf eine kleine Gruppe von einander bekannten Nutzern beschränkte, die für informelle Sanktionen hinreichend empfänglich waren, erschienen technische oder gar rechtliche Sicherungsmechanismen verzichtbar.[35] Entsprechend überoptimistische und permissive Design-Entscheidungen erleichterten den Umgang mit

richtungen vom 14.12.2022; (iii) die Verordnung über die allgemeine Produktsicherheit (COM/2021/346 final); (iv) die Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors vom 14.12.2022; (v) die Verordnung über Maschinenprodukte (COM/2021/202); (vi) die Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) (COM/2021/206 final). In unterschiedlichen Stadien der Planung befinden sich weiterhin etwa (i) ein „Netzkodex" für die Cybersicherheit grenzüberschreitender Aktivitäten von Energiewirtschaftsunternehmen; (ii) Regelungen zum Aufbau eines unionsweiten „Cyberschutzschilds" aus Computer-Notfallteams (CSIRTs) und Sicherheitseinsatzzentren; (iii) der Erlass von Durchführungsrechtsakten auf der Grundlage des Rechtsakts zur Cybersicherheit; (iv) der EU Chips Act, der Regelungen zur Auditierung der Design- und Fertigungsprozesse relevanter Hardware enthalten soll (COM/2022/46 final); (v) ein Cyber Resilience Act (CRA), der eine horizontale Regelung für vernetzte Produkte schaffen soll (COM/2022/454 final); (vi) diverse sektorspezifische Sicherheitsvorgaben, etwa für Kraftfahrzeuge. Zur Europäisierung des Informationssicherheitsrechts zusammenfassend unten § 6 III.

[31] *Europäische Kommission*, EU-Strategie für eine Sicherheitsunion 2020–2025, COM(2020) 605 final. Auch der neue „Europäische Verteidigungsfonds" fördert in größerem Umfang Cybersicherheitsprojekte.

[32] Zu dieser näher unten § 5 III. 1. b) bb).

[33] Hierzu gleich bei § 2 I. 4.

[34] Allgemein zum staatlichen Beitrag zur Technikentwicklung aus historischer Sicht unten § 3 I. 1. Speziell zum Beitrag staatlicher Akteure zur Entwicklung der digitalen Technik unten § 4 II. 1. b).

[35] Hierzu und zum Wegfall dieser Voraussetzungen in der Folgezeit instruktiv *M. Blumenthal/D. Clark*, Design of the Internet, ACM Transactions on Internet Technology 1 (2001), S. 70 (93); *L. DeNardis*, The Internet Design Tension between Surveillance and Security, IEEEA 37:2 (2015), S. 72 (73); *N. Sivakumar*, Generative Security, AJIL Unbound 110 (2017), S. 358 f.; differenzierend *B. Fidler*, Cybersecurity Governance, Digital Policy, Regulation and Governance 19:6 (2017), S. 449 ff.; im Überblick auch *M. Dunn Cavelty/A. Wenger*, Cyber Security Meets Security Politics, Contemporary Security Policy 41:1 (2020), S. 5 (11).

der neuen Technologie und trugen zu ihrer Popularität bei.[36] Heute jedoch erweisen sie sich vielfach als Einfallstore für Bedrohungen, behindern dadurch ihrerseits Innovationen[37] und geben somit Anlass zur (Re-)Regulierung.

III. Informationssicherheitsdiskurs zwischen Extremen: „Going dark" vs. „Versicherheitlichung"

Gegenüber anderen technikgeprägten Materien weist der die Informationssicherheit betreffende Regulierungsdiskurs Besonderheiten auf. Grund dafür ist, dass im Cyberraum die Grenzen zwischen „technischer" und „allgemeiner" Sicherheit verschwimmen.[38] Unsichere digitale Produkte oder Systeme stellen nämlich nicht nur für die jeweiligen Betreiber, Hersteller und Nutzer ein technisches Risiko dar, sondern erleichtern auch aggressive Cyberaktivitäten jeder Art. Zugleich öffnen Schwachstellen Sicherheitsbehörden Tür und Tor zur Bekämpfung IT-spezifischer, vor allem aber auch sonstiger Gefahrenlagen. Informationssicherheitspolitik befindet sich insoweit stets in einem „double bind" und muss das Interesse an möglichst hohen IT-Sicherheitsstandards einerseits mit dem Interesse an einer effektiven, aber auch rechtsstaatlich eingehegten Gefahrenabwehr bzw. Strafverfolgung in Ausgleich bringen. Diese Spannungslage wird im Informationssicherheitsdiskurs häufig nicht in ihrer Komplexität anerkannt und bearbeitet. Stattdessen dominieren polarisierende Gegenüberstellungen und Katastrophenszenarien: Während Polizei und Nachrichtendienste den Verlust ihrer Aufklärungsfähigkeiten durch ein Übermaß an IT-Sicherheit befürchten – „going dark" –, wird von anderer Seite jede staatliche Intervention in Sachen IT-Sicherheit unter den Verdacht einer illiberalen „Versicherheitlichung" gestellt. Dieser „Daueralarm" erschwert rationale Politikgestaltung.[39]

Wie ambivalent die Rolle des Staates hier ist, zeigt beispielhaft der erfolgreiche Hacker-Angriff auf die U.S. National Security Agency (NSA) im Jahr 2016; die dabei erbeuteten Schwachstellen, die der Dienst für Zwecke der Terrorismusabwehr genutzt hatte, wurden anschließend von Cyberkriminellen als Grundlage für die WannaCry- und NotPetya-Ransomware genutzt.[40] Der-

[36] Hierzu am Beispiel der Netzwerkarchitektur *J. Kurose/K. Ross*, Computer Networking, 8. Aufl. 2020, S. 89 ff.

[37] Dazu *Expertenkommission Forschung und Innovation*, Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands, 2020, BT-Drs. 19/23070, S. 42 ff.

[38] Ausführlich zu diesem Aspekt unten § 4 II.

[39] Dazu *M. Dunn Cavelty*, Gesellschaft im Daueralarm, in: Daase/Engert/Junk (Hrsg.), Verunsicherte Gesellschaft – überforderter Staat, 2013, S. 133 ff.; *B. Frevel*, Dilemmata des Sicherheitsdiskurses, in: Sensburg (Hrsg.), Sicherheit in einer digitalen Welt, 2017, S. 167 ff.

[40] *L. Newman*, The Leaked NSA Spy Tool that Hacked the World, Wired, 7.3.2018.

Sach- und Personenregister

accusation 106, 109
Agentur für Innovation in der Cybersicherheit (Cyberagentur) 220
Agentur für Sprunginnovation (SPRIND) 220
air gap 195
Akkreditierung *siehe* New Legislative Framework; Zertifizierung
All-Gefahren-Ansatz 87, 93, 102–112, 115, 163, *siehe auch* Gefahr
Allgemeines Persönlichkeitsrecht 70, 140–152, 160, 284, 291, *siehe auch* Datenschutzrecht; Recht auf informationelle Selbstbestimmung
Allianz für Cyber-Sicherheit 225
Anlagenschutz 87 f., 198
Attribution 11, 104–110, 279, *siehe auch* Internet (Anonymität des Internets)
– Digitale Forensik 105
– Folgen des Attributionsproblems 234, 237, 273
– Funktionalität des Attributionsproblems 106
– Zurechnung 107
Arpanet 198
Aufgabe 30 f., 39–41, *siehe auch* Neue Verwaltungsrechtswissenschaft
– Informationssicherheit als Aufgabe 188, 191
– öffentliche Aufgabe 40
– Staatsaufgabenlehre 40, 80
– Verwaltungsaufgabe 40
Außenwirtschaftsrecht
– Direktinvestitionen 11
– Exportkontrolle 11, 309
– Sanktionen 109
Ausland-Ausland-Fernmeldeaufklärung 304
Ausnahmezustand 76, 91, 96, 116
Authentifizierung 207, 248
Authentizität (authenticity) 190, 204, 245, *siehe auch* Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme
Autonome Systeme 199, 205, 216

BBK 85 f., 88, 114, 168, 230, 275, *siehe auch* Katastrophenrecht; Zivilschutz
Berufsfreiheit 123–127, *siehe auch* Digitalwirtschaft
– Berufsausübungsregelung 124, 126
– Kernbereich 126
– Stufen-Lehre 124 f.
Bestimmtheitsgebot 93, 133, 143 f., 288, *siehe auch* Normenklarheit
Bevölkerungsschutzrecht 85, 89, 94, *siehe auch* Katastrophenrecht; Zivilschutz
Budapester Konvention gegen Datennetzkriminalität *siehe* Cybercrime Convention
Bundesamt für Sicherheit in der Informationstechnik (BSI) 6, 27 f., 41, 112, 114, 166, 173, 176, 194 f., 213, 222–230, 235, 248, 250–252, 260, 265, 268
– als CERT-Bund 100, 226, 269
– als Nationale Behörde für die Cybersicherheit 222, 277
– als „Ordnungsbehörde“ 275
– als Wissensakteur 224 f.
– als Zertifizierungsstelle 226, 277
– Befugnisse zur Produktwarnung, -empfehlung und -untersuchung 230, 264–266
– Durchsetzungs- und Kontrollbefugnisse 268 f.
– Geschichte des BSI 173, 236, 277
– Grundschutz 112 f., 248, 252
– Kompetenzgrundlage 167
– Koordinierungspflichten 223 f.
– Lageberichte des BSI 3
– operative Befugnisse 164, 167, 269
– Portscans 268
– Rolle des BSI beim Schwachstellenmanagement 292, 298, 302
– Sicherheitsaudits 268

– Unabhängigkeit und Weisungsfreiheit des BSI 173–177
Bundesdatenschutzbeauftragter 255, 303
Bundeskriminalamt (BKA) 3, 114, 153, 168
– Standardisierende Leistungsbeschreibung des BKA 288
– und „Pegasus“ 280
Bundesnetzagentur (BNetzA) 167, 255, 269
– IT-Sicherheitskatalog der BNetzA 223 f., 252
Bundessicherheitsrat (BSR) 301

Cloud Computing 196
Cloud-Speicherdienste 12, 150
– als digitale Dienste 213, 236
– und Grundrechte 150
Computer Emergency Response Team (CERT) 9, 128, 181, 228 f., 269
– CERT-Bund 226, 269
– CERT-EU 100, 171, 215
– Cyber-Feuerwehr 270
– Deutscher CERT-Verbund 226
– Mobile Incident Response Team (MIRT) 270, 274
Computer-Grundrecht *siehe* Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme
Computerkriminalität (Cybercrime) 194, *siehe auch* Cybercrime Convention; Strafrecht
– Begriff 110
– Erscheinungsformen 194
– Lagebild 3
Computerkultur 13
constitutional pluralism 121
Covid-19-Pandemie 4, 131
Cyberangriff 11, 97, 286, *siehe auch* Internet; Malware; Schwachstellen
– back door 193, 195, 197, 308
– BGP-Highjacking 205, 266 f., 280
– Botnetz 154, 272 f., 279
– Brute Force-Angriff 312
– cyber capacity building 97
– cyber doom 102
– Cyberkrieg/cyberwar 23, 29, 98, 100
– Cyberspionage 23, 97
– Cyberterrorismus 23
– Cyber-Verteidigungspolitik 97
– Cyberwaffen 23
– Desinformation 11
– Distributed Denial of Service (DDoS)-Angriff 194, 203
– Emotet 153 f., 160
– Hacking/Hacktivism 279
– NotPetya 10
– NSO-Group 280
– Ransomware 5, 10, 107, 153 f., 193
– Shadow Brokers 283
– Social Engineering 194 f.
– SolarWinds 197
– Spear-Phishing 191, 194
– Stuxnet 195
– WannaCry 10
Cybercrime Convention 109 f., 272, *siehe auch* Strafrecht
Cyberdomain *siehe* Cyberspace
cyber power 14, 29, 101
Cyberresilienz *siehe* Resilienz
cyber restraint 98
Cyberrisiken
– Arten von Cyberrisiken 3–5
– systemische Natur von Cyberrisiken 124, 207
– Third-Party Cyber Risks 198
– Versicherung von Cyberrisiken 3, 110
Cybersicherheitsstrategie(n) 5–10, 14, 97, 114, 224, 243, 260, 266 f.
Cyberspace 24, 210 f., 279
– Cyber- und Informationsraum 11, 110
– Normsetzung im Cyberspace 14
– Regulierbarkeit 210 f.

Daseinsvorsorge 22, 32, 84, 97
Daten
– Begriff 26 f.
– personenbezogene Daten 27, 71–74, 93, 128, 142 f., 238, *siehe auch* Datenschutz-Grundverordnung; Datenschutzrecht
Datenbank 69–74, 189, 192
Datenlokalisierung 216
Datenqualität 232
Datenschutz-Grundverordnung, *siehe auch* Datenschutzrecht
– Auftragsverarbeitung 238
– Datenschutz-Folgenabschätzung 74, 290 f.
– technische und organisatorische Maßnahmen 74, 123, 234, 244–246, 251
– Verantwortlichkeit 238, 257
– Zertifizierung nach Datenschutz-Grundverordnung 74, 123, 165, 262–264
Datenschutzkonferenz 252, 265

Datenschutzrecht *siehe auch* Allgemeines Persönlichkeitsrecht; Recht auf informationelle Selbstbestimmung
– Geschichte des Datenschutzrechts 68
– Kritik am Datenschutzrecht 141 f.
– Personenkennzeichen 69, 72
– Querschnittsnatur des Datenschutzrechts 277
– Risikogrundsatz im Datenschutzrecht 163
– Sonderweg des Datenschutzrechts 68–74.
– Staatliche Handlungspflichten im Datenschutzrecht 158
– Standard-Datenschutzmodell (SDM) 252
– Systemdatenschutz 235, 254
Datensicherheit *siehe auch* Datenschutz-Grundverordnung
– Begriff 26 f.
– Spannungsverhältnis von Datenschutz und Datensicherheit 128 f.
Datenwirtschaft *siehe* Digitalwirtschaft
DE-CIX *siehe* Internet-Infrastrukturdienste
De-Mail 20, 308
Demokratieprinzip 172–182, *siehe auch* unabhängige Behörden
Digitale Dienste 213, 239–241
– Cloud-Computing-Dienste 213
– Online-Marktplätze 213
– Online-Suchmaschinen 213
Digitale Forensik *siehe* Attribution
Digitale Souveränität 14, 216, 322
Digitalpolitik 6 f., 40
Digital Services Act 267
Digitalwirtschaft 124, 260, *siehe auch* Berufsfreiheit
Doppeltür-Modell 296

E-Government 4, 12, 18–21, *siehe auch* Informationsverwaltungsrecht
ENISA 3, 8, 165, 166, 170–172, 215 f., 222, 224–226, 229, 253, 260 f., 276, 278, 283, 293
Entnetzung 195
E-Privacy-Verordnung 238
Equation Group 197
EU Chips Act 9
EU-Cybersecurity Act (CSA) 165, 170, 172, 197, 225 f., 258, 260–264, 275, 277
Europäische Union (Allgemein)
– als Sicherheitsunion 9, 166 f., 170
– (digitaler) Binnenmarkt 8, 165, 258, 260
– Brussels Effect 209
– Cyber Diplomacy Toolbox 11
– gegenseitige Anerkennung 260
– Netzwerk-Konzept im europäischen Verwaltungsrecht 214
– Raum der Freiheit, der Sicherheit und des Rechts (RFSR) 171
– Rechtsangleichungskompetenz 170
– ReNEUAL-Musterentwurf für ein Europäisches Verwaltungsrecht 238
– Ständige strukturierte Zusammenarbeit (PESCO) 171
– Unabhängige Agenturen im Recht der Europäischen Union 170–177
– Warenverkehrsfreiheit 258
Europäische Union (Akteure)
– CERT-EU *siehe* Computer Emergency Response Team (CERT)
– Cyber Crisis Liaison Organisation Network (CyCLONe) 215, 276
– EU Joint Cyber Unit (JCU) 9, 171 f.
– eu-LISA 171
– Eurojust 171, 215
– Europäischer Verteidigungsfonds 9
– Europäisches Kompetenzzentrum für Cybersicherheit 170 f., 221, 276
– Europäisches Zentrum zur Bekämpfung von Cyberkriminalität (EC3) 170
– European Union Agency for Cybersecurity *siehe* ENISA
– Europol 1, 166, 170–172
– Frontex 166
– Netzwerk nationaler Koordinierungszentren 170, 215, 221, 276
– NIS-Kooperationsgruppe 171, 215
– Zentrum für Informationsgewinnung und -analyse (INTCEN EU) 171

Fernmeldegeheimnis *siehe* Telekommunikation
Forsthoff, Ernst 52, 61–64
Fragmentierung des Völkerrechts 217

Gefahr 79–88, *siehe auch* All-Gefahren-Ansatz
– dringende Gefahr 137 f.
– konkrete Gefahr 79
Gefährdungslage *siehe* Cyberrisiken
Gemeinsames Terrorismusabwehrzentrum (GTAZ) 114, 115, 168, *siehe auch* Nationales Cyber-Abwehrzentrum

Gesetz
– als Steuerungsinstrument 7, 183
– Gesetzesbegriff des Konstitutionalismus 61
Gesetzgebungskompetenzen 163–167
Gewaltenteilung 92, 177
Global Administrative Law 34–38
Globalisierung 13, 209–212
Going dark 10 f., 285, 308–312, *siehe auch* Verschlüsselung
Governance-Begriff 38
Grundrechte
– als Abwehrrechte 122–129
– als Schutzpflichten 78 f., 156–163, 289–291, 293, 296
– Kernbereichsschutz 133, 152, 177, 287, 306
– (un-)mittelbare Drittwirkung 125–127
– „neue" Grundrechte 65, 68 f.
– objektiv-rechtliche Funktion 156–163
Grundrecht auf Sicherheit *siehe* Sicherheit

Habermas, Jürgen 51 f.
Haftungsrecht (vertraglich, deliktisch) 233–237, 270–272
– Compliance 271
– Haftung des Nichtstörers 234 f.
– Update-Pflicht 272
– Verkehrssicherungspflicht 271
– verschuldensunabhängiges Produkthaftungsrecht 271
Hardware 12, 196–198, 277, *siehe auch* Software
Hassrede 132
Heartbleed 205, 293
Heidegger, Martin 52, 61

IETF 41, 180, 188, 192, 202–204, 206, 212, 244, 247, 249, *siehe auch* Internet-Protokolle; Normungsgremien
Industrial Control System 193
Information
– Begriff 26–29
– Informationelles Trennungsgebot 114
– Informationsgesellschaft 28, 44
– Informationsordnung *siehe* Informationsverwaltungsrecht
– Informationsverarbeitung(-szyklus) 114, 132
– Informationsvorsorge 80
Informationsverwaltungsrecht 18–21
– Informations(-management-)systeme 69–74, 230–232
– inneradministrativer Informationsaustausch 230
Innenrecht 34
Innere Sicherheit 77, 84, 94, *siehe auch* Sicherheit
Innovation 10, 65 f.
Instrument 184–188, *siehe auch* Regulierung
– Instrumentenmix 186
International Law Commission (ILC) 103, 107
– Articles on Responsibility of States for Internationally Wrongful Acts 103, 107
International Telecommunication Union (ITU) 98 f.
– Standardization Sector 247
– World Conference on International Telecommunications (WCIT) 99
Internet
– Anonymität im Internet *siehe* Attribution
– Dezentralität des Internets 9, 24, 198
– Domain Name System 216, 266 f.
– Fragmentierung des Internets 217, 266
– Geschichte des Internets 99
– Internet Assigned Numbers Authority (IANA) 201–204
– Internet Corporation for Assigned Names and Numbers (ICANN) 180, 201–204
– Internet der Dinge 260
– Internet Engineering Steering Group (IESG) 202
– Internet-Infrastrukturdienste 216, 244, 267
– Internet Integrity 5
– Internet Service Provider (ISP) 199, 244
– Konzentrationstendenzen 13
– Local Internet Registries (LIR) 201
– Regional Internet Registries (RIRs) 201
– Routing 205, 267
– Schichten-Modell der Internet-Regulierung 191
– Tier-1-Provider 201
– Top Level Domain (TLD)-Registrare 213, 216, 267
Internet-Protokolle 199–206, *siehe auch* Cyberangriff
– Border Gateway Protocol (BGP) 200, 202, 205 f.
– Domain Name System Protocol (DNS Protocol) 199, 202–206, 213

– Hypertext Transfer Protocol (HTTP) 199 f.
– Internet Protocol (IP) 200, 202 f.
– Internet Protocol Security (IPsec) 203
– Open Systems Interconnection Model (OSI/ISO-Modell) 200, 248
– Request for Comments (RFCs) 200–205, 247
– Secure Sockets Layer (SSL) 204
– TCP/IP-Referenzmodell 199 f., 204
– Transmission Control Protocol (TCP) 200
– Transport Layer Security (TLS) 204
Internetsicherheit 28, 198–206, 241, 266 ff., 276 f., *siehe auch* Cyberangriff; Internet-Protokolle
IT-Grundrecht *siehe* Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme
IT-Sicherheit 26, 28, 234
– Begriff 26–29
– IT-Sicherheit aus ökonomischer Sicht 219, 234
– Schutzgüter 189 f.
– – Authentizität (authenticity) 190, 204, 245
– – Integrität (integrity) 149, 189
– – Nichtabstreitbarkeit (non-repudiation) 190
– – Verfügbarkeit (availability) 189
– – Vertraulichkeit (confidentiality) 149, 189
IT-Sicherheitsforschung 220 f.
IT-Sicherheitskennzeichen 263, 275
IT-Sicherheitsverordnung Portalverbund 20

Jurisdiktion 212–214, 243, 267

Katastrophenrecht 85–88, *siehe auch* BBK; Zivilschutz
– Bevölkerungsschutzrecht 85
Kernenergie 63 f., *siehe auch* Technik
Kinderpornographie 132, 310
Kodifikationsidee 207 f.
Kollision *siehe* Schwachstelle
Komponentensicherheit 196, 198, 241, 257, 277
– Sicherheit der Lieferkette 197 f., 243, 277
Konformitätsbewertungen 258–263, *siehe auch* New Legislative Framework; Produktsicherheit
Kopenhagener Schule der internationalen Beziehungen 90
Kriminalpräventionsrecht 89
Kritikalität *siehe* Kritische Infrastrukturen (KRITIS)
Kritische Infrastrukturen (KRITIS) 8, 11, 22 f., 86–88, 115, 128, 164, 175, 212 f., 223–257, 262–269, 291 f., 298
– AG KRITIS 86
– Betreiber wesentlicher Einrichtungen 240, 245
– Betreiber wichtiger Einrichtungen 240, 245
– Einsatz von Systemen zur Angriffserkennung 250
– Kritikalität 87, 253
– kritische Komponenten 243, 255
– KRITIS-Strategie 86, 91
– KRITIS-Verordnung 88, 237, 240, 257, 267
– Recht der kritischen Infrastrukturen 22, 89, 94 f., 235, 242, 245, 252, 257, 268 f., 277
– Schwellenwerte 237, 240, 254
– Umsetzungsplan KRITIS 224 f., 235
– U.S. President's Commission on Critical Infrastructure Protection (PCCIP) 86
– Vitale Systeme 83
Kryptopolitik *siehe* Verschlüsselung
Kybernetik 51, 68, *siehe auch* Technik

Lex Huawei 4, 12, 243, *siehe auch* Kritische Infrastrukturen
Lieferkette 5, *siehe* auch Globalisierung; Komponentensicherheit
Luhmann, Niklas 53, 58, 75

Malware 193, 279, *siehe auch* Cyberangriff; Schwachstellen
– Rootkits 193
– trojanische Pferde 193
– Viren 193
– Würmer 193
Maschinelles Lernen 65
Marcuse, Herbert 52
Marktortprinzip *siehe* Jurisdiktion
Marktüberwachung *siehe* New Legislative Framework
Marktversagen 32, 34, *siehe auch* IT-Sicherheit als öffentliches Gut
Mayer, Otto 43
Meldepflichten 226–229, 298 f., *siehe auch* Schwachstellen-Management

Menschenwürde 143
Mobile Incident Response Teams *siehe* Computer Emergency Response Team

Nachrichtendienste 99–101, 280
– nachrichtendienstliche Kontrolle 306
Nationaler Cyber-Sicherheitsrat 225
Nationales Cyber-Abwehrzentrum (NCAZ) 114 f., 168–172
National Security Agency (NSA) 10, 203, 283, 293 f.
– Shadow Brokers 283, 284
National Security Council (NSC) 294, 300
Network and Information Security Directive *siehe* Europäische Union (Rechtsakte)
Netzpolitik *siehe* Digitalpolitik
Netzwerk- und Systemsicherheit 192–195, 244–257
Neue Verwaltungsrechtswissenschaft 31–45, *siehe auch* Aufgabe; Verwaltungsrecht
– Steuerung 31, 37
– und Governance 39
– und New Public Law 44
New Legislative Framework 259–264, *siehe auch* Produktsicherheit
– Funkanlagenrichtlinie 259, 263
– Maschinenrichtlinie 259, 263
– New Approach 258
– Niederspannungsrichtlinie 259
– Produktsicherheits-Richtlinie 263
– Produktsicherheits-VO 259
Nobody, but us 283
Normenklarheit 133, 143 f., 151, *siehe auch* Bestimmtheit
Normungsgremien *siehe auch* Standardsetzung; technische Normen; Zertifizierung
– Cenelec 259
– Deutsches Institut für Normung (DIN) 248
– Europäische Gruppe für die Cybersicherheitszertifizierung 260
– Europäische Normungsinfrastruktur 258
– Europäisches Komitee für Normung (CEN) 247, 259
– European Cybersecurity Certification Group 226
– European Telecommunications Standards Institute (ETSI) 259
– Gruppe hoher Beamter für die Sicherheit der Informationssysteme (SOG-IS) 260
– Institute of Electrical and Electronics Engineers (IEEE) 247
– International Electrotechnical Organization 41
– International Organization for Standardization 41, 247
– National Institute of Standards and Technology 248

Online-Durchsuchung 132, 139 f., 145 f., 148, 152, 154 f., 160, 280, 286 f., 288
Online-Identitäten 4
– eIDAS-Verordnung 20, 165
Over-the-top-Kommunikationsdienste (OTT-Dienste) 132, 311–317
OZG 20

Parlamentarischer Rat 63
Parlamentsvorbehalt 144
Präventionsparadigma 88
Präventionsstaat 80 f.
Predictive Policing 76
Presidential Policy Directive 293
Privatsphäre *siehe* Allgemeines Persönlichkeitsrecht; Recht auf Privatheit
Produktsicherheit 8, 22, 80, 111, 258–266, *siehe auch* New Legislative Framework; Zertifizierung
– behördliche Warnungen 264 f.
– CE-Kennzeichen 264
– Produktbegriff 271
– Produktempfehlungen 264
– Produktuntersuchungen 264, 298

Quellen-TKÜ 130, 132, 140, 147, 153, 155, 161, 280, 282, 284, 285–292, 296, 312, *siehe auch* Telekommunikation
– Exceptional (Lawful) Access 312, 317
– Quellen-TKÜ Plus 280

Realbereichsanalyse 41
Recht auf informationelle Selbstbestimmung 21, 69, 73, 128–130–134, 140–146, 148–155, 159, 169, 270, *siehe auch* Allgemeines Persönlichkeitsrecht; Datenschutzrecht
– (Europäisches) Grundrecht auf Datenschutz 4, 70, 123, 142, 151, 157, 159
– Informationelle Selbstbestimmung 22, 68, 71, 140–145, 151, 158
– Mikrozensus-Beschluss 70–72
– Volkszählungsurteil 68–72
– Verbot der Profilbildung 149

Recht auf Privatheit *siehe auch* Allgemeines Persönlichkeitsrecht; Fernmeldegeheimnis; Recht auf informationelle Selbstbestimmung
– im Unions- und Völkerrecht 158 f.
– Schutzgut 129
Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme 4, 129, 135, 140, 145 f. 148 f., 153–155, 287, 289, 296
Rechtsbegriff 34
– Privates Recht 36 f., *siehe auch* Standardsetzung
Rechtsdogmatik 42 f.
– Interdisziplinarität der Rechtsdogmatik 43
– und Neue Verwaltungsrechtswissenschaft 42–45
Rechtsgebiet 66, 76 f., 186
Rechtspluralismus 185
Recht und Technik *siehe* Technik
Regimekomplex 185, 209
Regulierung 32–44, 206–209, *siehe auch* Aufgabe; Neue Verwaltungsrechtswissenschaft
– Gemeinwohlorientierung von Regulierung 34
– integrative Regulierung 185, 274
– Krise regulativer Politik 14
– Regulatory capture 34
– Regulierte Selbstregulierung 187 f., 237
– Risikobasierte Regulierung 253, 278
– Selbstregulierung 35
Resilienz 6, 84, 90, 278
– Cyber Resilience Act 9
Risiko
– Begriff 82
– Dogmatisierung des Risikobegriffs 81
– Risikobasierte Regulierung 253, 278
– Risikobewusstsein 83
– Risikodiskurs 81
– Risikogesellschaft 81
– Risikorecht 80, *siehe auch* Sicherheitsrecht
– Risikosteuerung 81
Ropohl, Günter 52, 53, 55

safety 111 f., 263, *siehe auch* Sicherheit
Schichtenmodell *siehe* Internet
Schmitt, Carl 56
Schutz der Wohnung (Art. 13 GG) 134–140, *siehe auch* Recht auf Privatheit
– Betretungs- und Nachschaurechte 137 f., 140
– Durchsuchungen 137–140
– Lausch- und Spähangriffe 137
– verfassungsimmanente Schranken 138 f.
– Wohnraumüberwachung 148
– Wohnungsbegriff 148
Schwachstelle 278, 279–307, *siehe auch* Cyberangriff
– Assume-Breach-Paradigma 196
– back door 193, 195, 197, 308
– Begriff der Schwachstelle 193
– Common Vulnerabilities and Exposures System (CVE) 196
– Common Vulnerability Scoring System (CVSS) 196
– Drive-by-Infection 194, 204
– Exploit 196
– Klassifikation von Schwachstellen 196
– Kollision 185, 283
– N-day-Schwachstellen 284, 299
– Nutzung von Schwachstellen durch staatliche Stellen 279–288
– Risiken 282–285
– Schwachstellenregister 229
– Zero-day-Schwachstellen 194, 282, 284, 299
Schwachstellen-Governance 285, 292, 294, 300–307, 316
– gerichtliche Kontrolle 303 f.
– parlamentarische Kontrolle 305 f.
– VEP 2017 300
– Vulnerabilities Equitities Process (VEP) 292–295, 302
Schwachstellen-Management *siehe* Schwachstellen-Governance
Science and Technology Studies 55 f., *siehe auch* Technik
security 111 f., 263, *siehe auch* Sicherheit
security by default 260
security by design 241, 260
Security Studies 75, 90
Sicherheit *siehe auch* Versicherheitlichung
– als Dispositiv 88–97
– als Perspektive 82
– als staatliche Aufgabe 77–79
– Begriff 75, 82, 84, 93
– Grundrecht auf Sicherheit 78
– human security 79
– innere Sicherheit 77, 84, 94
– nationale Sicherheit 165
– öffentliche Sicherheit 79
– Sicherheitsarchitektur 80, 84, 94, 168

– Sicherheitsgefühl 4
– Sicherheitsgewährleistung 13 f., 40, 75
– zivile Sicherheit 83 f., 90, 168, *siehe auch* Zivilschutz
Sicherheitsgesellschaft 75 f., 89, *siehe auch* Ausnahmezustand
Sicherheitslücken *siehe* Schwachstellen
Sicherheitsrecht
– als Rechtsgebiet 22, 75–88
– „altes" Sicherheitsrecht 79 f.
– „neues" Sicherheitsrecht 77, 79 f., 102, 253
– Sicherheitsverfassung 76
Sicherheitsstrategien 5, 14, *siehe auch* Cybersicherheitsstrategien
Signaturgesetz 20
Smart Home 135, 148
Smart Meter 239
Software 12, 196, 199, *siehe auch* Hardware; Schwachstellen
– embedded Software 271
– Firmware 196 f., 271
– Netzwerkmanagement-Software 197
– Open-Source-Software 197
– Software-defined Everything 196
– stand alone Software 271
Souveränität 14, 108, *siehe auch* Digitale Souveränität
Standardsetzung 36, 99 f., 178–180, 212, 219 *siehe auch* Normungsgremien; Zertifizierung
– branchenspezifische Sicherheitsstandards (B3S) 252
– Delegation 180
– harmonisierte Normen 259
– „Normierung der Normung" 179
– „steuernde Rezeption" 178, 249
Stand der Technik 65, 178, 245–257, 250 f., 308, *siehe auch* Standardsetzung; Technik
Strafrecht *siehe auch* Computerkriminalität (Cybercrime); Cybercrime Convention
– Computerstrafrecht 272
– digitaler Hausfriedensbruch 272 f.
– Informationsstrafrecht 190

Tallinn Manual 23, 113, *siehe auch* Völkerrecht
Technik 49–74, *siehe auch* Technikrecht
– als „Geschick" 52, 55
– als „Möglichkeitsraum" 59
– als soziales System 50, 58, 67, 115
– Basis-Überbau-Modell 51
– nachtechnologische Technik 52
– nationalsozialistischer Technikdiskurs 61
– Recht und Technik 56, 65 ff., 256
– sozio-technisches System 55, 58
– Technikbegriff 53 f.
– Technikethik 57
– Technikfolgenforschung 45
– Technikgenese 58
– Technikkritik 63, 101
Technikrecht 22 f., 28, 49, 53, 60–66, 70, 7 f., 81, 116, 172, 178 f., 181, 184, 207, 210, 218, 236, 241, 244, 256, 258, 264, 274
– Funktionsbestimmung des Technikrechts 184
– Geschichte des Technikrechts 60
– Instrumente des Technikrechts 66
technische Normen 180, 188, *siehe auch* Standardsetzung
technische Sicherheit *siehe* Produktsicherheit; Sicherheit
technische und organisatorische Maßnahmen *siehe* Datenschutz-Grundverordnung
Technokratie 59
Telekommunikation 130, 147, 285, 287
– Telekommunikationsrecht 17, 255
– Telekommunikationsüberwachung 148, 287, *siehe auch* Quellen-TKÜ
Telekommunikationsgeheimnis 130, 144–151, 154, 159
Territorium *siehe* Globalisierung; Jurisdiktion
third party rule 307
transnationales Recht 36, 180, 210 f.
Transparenzregister 278

Überwachungskapitalismus 100
unabhängige Behörden 173–177, *siehe auch* demokratische Legitimation
Unabhängiger Kontrollrat 301, 304
United Nations (UN) *siehe* Völkerrecht
Unternehmen im besonderen öffentlichen Interesse 239–241, 268, *siehe auch* Kritische Infrastrukturen (KRITIS)

Verbot der Selbstbezichtigung 228
verdeckter Ermittler 138, 286
Verhältnismäßigkeit 288, 297
Verrechtlichung 6, 13, 107, 210 f., 225, 257, 307
Verschlüsselung 308–318
– „besonderer" Behördenzugang 313

– Client Side Scanning 314, 317
– Clipper Chip 309, 314
– crypto wars 308 f.
– Ende-zu-Ende-Verschlüsselung 132, 285, 308–317
– (Grund-)Recht auf Verschlüsselung 310, 315
– Hintertür 308
– Kryptopolitik 310, 315
– Transportverschlüsselung 317
– Verschlüsselungsalgorithmen 314
– Verschlüsselungspflichten 308
– Verschlüsselungsregulierung 133
Versicherheitlichung 10, 76, 88 f., 97, 176
– „desecuritization“ 90
Versorgungssicherheit *siehe* Daseinsvorsorge
Verteidigungsfall 85
Vertrauensdienstegesetz 20
Verwaltung
– als lernendes System 221
– Verwaltungsautomatisierung 68
– Verwaltungsrechtsverhältnis 18 f.
Verwaltungskompetenzen 167–172
Verwaltungsrecht
– Methoden der Verwaltungsrechtswissenschaft 39, *siehe auch* Neue Verwaltungsrechtswissenschaft
– Systemdenken im Verwaltungsrecht 185
Völkerrecht 23 f., 209–217, *siehe auch* Tallin Manual
– Anwendbarkeit auf den Cyberspace 107
– Staatenverantwortlichkeit 23, 107, *siehe auch* Attribution
– United Nations Group of Governmental Experts (UN GGE) 3, 107 f.
– Völkerrecht des Internets 24
Vorbehalt des Gesetzes 93, 289
Vorratsdatenspeicherung 100, 158, 165
Vorsorge 82, 87–91
– Vorsorgestaat 81

Weber, Max 54, 57, 61
Weltgesellschaft 210
Wissen 26, 40–45, 218–223
– Extrajuridisches Wissen 45
– organisationales Wissen 221
– Regulierungswissen 218
– Wissensdistribution 219, 230
– Wissensgenerierung 219
– Wissensordnung 219
– Wissenstransfer und Wissensdistribution 224

Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) 6 f., 115, 282
Zero-Day-Exploits *siehe* Cyberangriffe; Schwachstellen
Zertifizierung, *siehe auch* Datenschutz-Grundverordnung; Standards
– Cybersicherheitszertifizierung 219, 228, 258–266, 268, 275–278
– Zertifizierungs-Schemata 261 f.
– Fragmentierung der Zertifizierung 264
Zivilschutz 85, 94, 95, *siehe auch* Bevölkerungsschutz; Katastrophenrecht
Zweck im Recht 31
Zweck-Mittel-Schema 54, 57